



SOFTWARE MANUAL



# Mellanox MLNX-OS®

## User Manual for Ethernet

---

Rev 4.80

Software Version 3.6.5000



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](http://www.mellanox.com)  
Tel: (408) 970-3400  
Fax: (408) 970-3403

© Copyright 2017. 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 CloudX™, 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

<b>Document Revision History .....</b>	<b>19</b>
<b>About this Manual .....</b>	<b>36</b>
<b>Chapter 1 Introduction .....</b>	<b>39</b>
1.1 System Features .....	39
1.2 Ethernet Features.....	40
<b>Chapter 2 Getting Started.....</b>	<b>42</b>
2.1 Configuring the Switch for the First Time.....	42
2.1.1 Configuring the Switch with ZTP .....	48
2.1.2 Rerunning the Wizard.....	49
2.2 Starting the Command Line (CLI).....	49
2.3 Starting the Web User Interface (WebUI) .....	49
2.4 Zero-touch Provisioning.....	53
2.4.1 Running DHCP-ZTP .....	53
2.4.2 ZTP on Director Switches .....	55
2.4.3 ZTP and MLNX-OS® Software Upgrade .....	55
2.4.4 DHCPv4 Configuration Example.....	56
2.4.5 DHCPv6 Configuration Example.....	56
2.4.6 Commands.....	57
2.5 Licenses .....	60
2.5.1 Installing MLNX-OS® License (CLI) .....	60
2.5.2 Installing MLNX-OS License (Web).....	60
2.5.3 Retrieving a Lost License Key .....	63
2.5.4 Commands.....	64
<b>Chapter 3 User Interfaces .....</b>	<b>69</b>
3.1 LED Indicators .....	69
3.2 Command Line Interface Overview.....	69
3.2.1 CLI Modes .....	69
3.2.2 Syntax Conventions.....	70
3.2.3 Getting Help.....	71
3.2.4 Prompt and Response Conventions.....	72
3.2.5 Using the “no” Form .....	72
3.2.6 Parameter Key.....	74
3.2.7 CLI Pipeline Operator Commands .....	75
3.2.7.1 “include” and “exclude” CLI Filtration Options.....	75
3.2.7.2 “watch” CLI Monitoring Option .....	76
3.2.7.3 “json-print” CLI Option .....	76

3.2.8 CLI Shortcuts .....	77
3.3 Web Interface Overview .....	78
3.3.1 Setup Menu .....	79
3.3.2 System Menu.....	80
3.3.3 Security Menu .....	81
3.3.4 Ports Menu .....	81
3.3.5 Status Menu.....	81
3.3.6 ETH Mgmt .....	82
3.3.7 IP Route .....	83
3.4 Secure Shell (SSH).....	83
3.4.1 Adding a Host and Providing an SSH Key.....	83
3.4.2 Retrieving Return Codes when Executing Remote Commands.....	84
3.5 Management Information Bases (MIBs).....	84
3.6 Commands .....	88
3.6.1 CLI Session .....	88
3.6.2 Banner .....	99
3.6.3 SSH .....	107
3.6.4 Remote Login.....	124
3.6.5 Web Interface .....	127
<b>Chapter 4 System Management.....</b>	<b>138</b>
4.1 Management Interface .....	138
4.1.1 Configuring Management Interfaces with Static IP Addresses .....	138
4.1.2 Configuring IPv6 Address on the Management Interface .....	138
4.1.3 Dynamic Host Configuration Protocol (DHCP) .....	139
4.1.4 Default Gateway .....	139
4.1.5 In-Band Management.....	139
4.1.6 Configuring Hostname via DHCP (DHCP Client Option 12) .....	140
4.1.7 Commands.....	141
4.1.7.1 Interface .....	141
4.1.7.2 Hostname Resolution .....	165
4.1.7.3 Routing .....	172
4.1.7.4 Network to Media Resolution (ARP & NDP) .....	176
4.1.7.5 DHCP.....	182
4.1.7.6 General IPv6 Commands.....	184
4.1.7.7 IP Diagnostic Tools.....	185
4.2 NTP, Clock & Time Zones .....	190
4.2.1 NTP Authenticate .....	190
4.2.2 NTP Authentication Key .....	190
4.2.3 Commands.....	191
4.3 PTP .....	209
4.3.1 Precision Time Protocol Principles.....	209

4.3.2 Clock Types and Operation Modes .....	210
4.3.3 PTP Domains .....	211
4.3.3.1 Boundary Clock .....	211
4.3.4 Commands.....	213
4.4 Software Management .....	226
4.4.1 Upgrading MLNX-OS Software.....	226
4.4.2 Upgrading MLNX-OS HA Groups .....	230
4.4.3 Deleting Unused Images.....	230
4.4.4 Downgrading MLNX-OS® Software .....	231
4.4.4.1 Downloading Image.....	232
4.4.4.2 Downgrading Image.....	232
4.4.4.3 Switching to Partition with Older Software Version.....	234
4.4.5 Upgrading System Firmware .....	234
4.4.5.1 After Updating MLNX-OS Software .....	234
4.4.5.2 Importing Firmware and Changing the Default Firmware .....	235
4.4.6 Image Maintenance via Mellanox ONIE .....	236
4.4.7 Commands.....	238
4.5 Configuration Management .....	249
4.5.1 Saving a Configuration File.....	249
4.5.2 Loading a Configuration File.....	249
4.5.3 Restoring Factory Default Configuration.....	249
4.5.4 Managing Configuration Files.....	249
4.5.4.1 BIN Configuration Files .....	250
4.5.4.2 Text Configuration Files.....	250
4.5.5 Commands.....	252
4.5.5.1 File System .....	252
4.5.5.2 Configuration Files.....	261
4.6 Logging.....	280
4.6.1 Monitor .....	280
4.6.2 Remote Logging.....	280
4.6.3 Commands.....	281
4.7 Debugging .....	302
4.7.1 Commands.....	303
4.8 Link Diagnostic Per Port .....	316
4.8.1 General.....	316
4.8.2 List of Possible Output Messages .....	316
4.8.3 Commands.....	317
4.9 Signal Degradation Monitoring .....	323
4.9.1 Effective-BER Monitoring .....	323
4.9.2 Configuring Signal Degradation Monitoring .....	323
4.9.3 Commands.....	324

4.10 Event Notifications . . . . .	326
4.10.1 Supported Events . . . . .	326
4.10.2 Terminal Notifications . . . . .	327
4.10.3 Email Notifications . . . . .	328
4.10.4 Commands . . . . .	330
4.10.4.1 Email Notification . . . . .	330
4.11 Telemetry . . . . .	349
4.11.1 Commands . . . . .	350
4.12 User Management and Security . . . . .	373
4.12.1 User Accounts . . . . .	373
4.12.2 Authentication, Authorization and Accounting (AAA) . . . . .	373
4.12.2.1 User Re-authentication . . . . .	374
4.12.2.2 RADIUS . . . . .	374
4.12.2.3 TACACS+ . . . . .	374
4.12.2.4 LDAP . . . . .	374
4.12.3 System Secure Mode . . . . .	375
4.12.4 Commands . . . . .	377
4.12.4.1 User Accounts . . . . .	377
4.12.4.2 AAA Methods . . . . .	382
4.12.4.3 RADIUS . . . . .	396
4.12.4.4 TACACS+ . . . . .	400
4.12.4.5 LDAP . . . . .	404
4.12.4.6 System Secure Mode . . . . .	420
4.13 Cryptographic (X.509, IPsec) and Encryption . . . . .	422
4.13.1 System File Encryption . . . . .	422
4.13.1.1 Commands . . . . .	423
4.14 Scheduled Jobs . . . . .	439
4.14.1 Commands . . . . .	439
4.15 Statistics and Alarms . . . . .	449
4.15.1 Commands . . . . .	449
4.16 Chassis Management . . . . .	469
4.16.1 System Health Monitor . . . . .	469
4.16.1.1 Re-Notification on Errors . . . . .	469
4.16.1.2 System Health Monitor Alerts Scenarios . . . . .	470
4.16.2 Power Management . . . . .	475
4.16.2.1 Width Reduction Power Saving . . . . .	475
4.16.3 Monitoring Environmental Conditions . . . . .	477
4.16.4 USB Access . . . . .	479
4.16.5 Unit Identification LED . . . . .	480
4.16.6 System Reboot . . . . .	480
4.16.6.1 Rebooting 1U Switches . . . . .	480
4.16.7 Commands . . . . .	481

4.16.7.1 Chassis Management.....	481
<b>4.17 Network Management Interfaces.....</b>	<b>509</b>
<b>4.17.1 SNMP .....</b>	<b>509</b>
4.17.1.1 Standard MIBs .....	509
4.17.1.2 Private MIB.....	511
4.17.1.3 Mellanox Private Traps .....	511
4.17.1.4 Configuring SNMP .....	512
4.17.1.5 Configuring an SNMPv3 User .....	512
4.17.1.6 Configuring an SNMP Notification .....	513
4.17.1.7 SNMP SET Operations .....	514
4.17.1.8 IF-MIB and Interface Information.....	518
<b>4.17.2 JSON API .....</b>	<b>519</b>
4.17.2.1 Authentication .....	519
4.17.2.2 Sending the Request .....	519
4.17.2.3 JSON Request Format .....	520
4.17.2.4 JSON Response Format.....	522
4.17.2.5 Supported Commands.....	524
4.17.2.6 JSON Examples.....	525
4.17.2.7 JSON Request Using WebUI .....	530
<b>4.17.3 XML API .....</b>	<b>532</b>
<b>4.17.4 Commands .....</b>	<b>533</b>
4.17.4.1 SNMP Commands .....	533
4.17.4.2 XML API Commands .....	553
4.17.4.3 JSON API Commands .....	555
<b>4.18 Puppet Agent .....</b>	<b>558</b>
4.18.1 Setting the Puppet Server .....	558
4.18.2 Accepting the Switch Request.....	558
4.18.3 Installing Modules on the Puppet Server .....	559
4.18.4 Writing Configuration Classes .....	559
4.18.5 Supported Configuration Capabilities.....	562
4.18.5.1 Ethernet, InfiniBand, and Port-Channel Interface Capabilities .....	562
4.18.5.2 VLAN Capabilities.....	562
4.18.5.3 Layer 2 Ethernet Interface Capabilities .....	562
4.18.5.4 LAG (Port-Channel) Capabilities .....	563
4.18.5.5 Layer 3 Interface Capabilities .....	563
4.18.5.6 OSPF Interface Capabilities.....	563
4.18.5.7 OSPF Area Capabilities .....	564
4.18.5.8 Router OSPF Capabilities.....	564
4.18.5.9 Protocol LLDP, SNMP, IP Routing and Spanning Tree Capabilities .....	564
4.18.5.10 Fetched Image Capabilities .....	564
4.18.5.11 Installed Image Capabilities .....	565
4.18.6 Supported Resources for Each Type .....	565
4.18.7 Troubleshooting .....	566

4.18.7.1 Switch and Server Clocks are not Synchronized .....	566
4.18.7.2 Outdated or Invalid SSL Certificates Either on the Switch or the Server	566
4.18.7.3 Communications Issue .....	567
4.18.8 Commands .....	568
4.19 Control Plain Policing .....	575
4.19.1 IP Table Filtering .....	575
4.19.1.1 Configuring IP Table Filtering .....	575
4.19.1.2 Modifying IP Table Filtering .....	577
4.19.1.3 Rate-limit Rule Configuration .....	577
4.19.2 Commands .....	578
4.20 Resource Scale .....	583
4.20.1 Ethernet Resources .....	583
4.20.1.1 Strict Mode.....	583
4.20.1.2 Loose Mode – SwitchX® .....	584
4.20.1.3 Loose Mode – Spectrum™ .....	584
4.20.2 Commands .....	585
4.21 Linux Dockers .....	587
4.21.1 Commands .....	588
<b>Chapter 5 Ethernet Switching.....</b>	<b>604</b>
5.1 Interface .....	604
5.1.1 Break-Out Cables.....	604
5.1.1.1 Changing the Module Type to a Split Mode .....	605
5.1.1.2 Unsplitting a Split Port.....	606
5.1.2 56GbE Link Speed .....	606
5.1.3 Transceiver Information .....	607
5.1.4 High Power Transceivers .....	608
5.1.5 Forward Error Correction .....	608
5.1.6 Commands.....	610
5.2 Interface Isolation.....	637
5.2.1 Configuring Isolated Interfaces .....	637
5.2.2 Commands.....	639
5.3 Link Aggregation Group (LAG).....	645
5.3.1 Configuring Static Link Aggregation Group (LAG).....	645
5.3.2 Configuring Link Aggregation Control Protocol (LACP) .....	645
5.3.3 Commands.....	647
5.4 Link Layer Discovery Protocol (LLDP) .....	667
5.4.1 Configuring LLDP .....	667
5.4.2 DCBX.....	668
5.4.3 Commands.....	669
5.5 VLANs.....	686
5.5.1 Configuring Access Mode and Assigning Port VLAN ID (PVID) .....	686

5.5.2 Configuring Hybrid Mode and Assigning Port VLAN ID (PVID) . . . . .	687
5.5.3 Configuring Trunk Mode VLAN Membership . . . . .	687
5.5.4 Configuring Hybrid Mode VLAN Membership . . . . .	688
5.5.5 Commands. . . . .	689
5.6 Spanning Tree . . . . .	700
5.6.1 Port Priority and Cost . . . . .	700
5.6.2 Port Type . . . . .	700
5.6.3 BPDU Filter. . . . .	701
5.6.4 BPDU Guard. . . . .	701
5.6.5 Loop Guard . . . . .	701
5.6.6 Root Guard. . . . .	702
5.6.7 MSTP . . . . .	702
5.6.8 RPVST . . . . .	702
5.6.8.1 RPVST and VLAN Limitations. . . . .	703
5.6.8.2 RPVST and RSTP Interoperability . . . . .	704
5.6.9 Commands. . . . .	705
5.7 MAC Address Table. . . . .	737
5.7.1 Configuring Unicast Static MAC Address. . . . .	737
5.7.2 MAC Learning Considerations . . . . .	737
5.7.3 Commands. . . . .	738
5.8 MLAG . . . . .	746
5.8.1 MLAG Keepalive and Failover. . . . .	748
5.8.2 Unicast and Multicast Sync. . . . .	748
5.8.3 MLAG Port Sync. . . . .	748
5.8.4 MLAG Virtual System-MAC. . . . .	749
5.8.5 Upgrading MLAG Pair . . . . .	749
5.8.6 Configuring MLAG . . . . .	749
5.8.7 Commands. . . . .	754
5.9 QinQ. . . . .	774
5.9.1 QinQ Operation Modes . . . . .	774
5.9.2 Configuring QinQ. . . . .	774
5.9.3 Commands. . . . .	776
5.10 Access Control List . . . . .	777
5.10.1 Configuring Access Control List . . . . .	777
5.10.2 ACL Actions . . . . .	777
5.10.3 ACL Logging . . . . .	778
5.10.4 ACL Capability Summary . . . . .	779
5.10.5 Commands . . . . .	781
5.11 OpenFlow . . . . .	827
5.11.1 Flow Table . . . . .	827
5.11.2 OpenFlow 1.3 Support . . . . .	828

5.11.2.1 ACL Rule Tables (0-249) . . . . .	829
5.11.2.2 FDB Table (250) . . . . .	832
5.11.2.3 Router Table (251) . . . . .	832
5.11.3 Configuring OpenFlow . . . . .	833
5.11.4 Configuring Secure Connection to OpenFlow . . . . .	834
5.11.5 Commands . . . . .	838
<b>5.12 VXLAN . . . . .</b>	<b>871</b>
5.12.1 Configuring VXLAN . . . . .	871
5.12.2 VMware Network Virtualization and Security Platform (NSX) Configuration . . . . .	873
5.12.2.1 Hardware Topology . . . . .	873
5.12.2.2 Switch Configuration . . . . .	874
5.12.2.3 Adding the Mellanox Switch to NSX . . . . .	876
5.12.3 Mapping a Logical Switch to a Physical Switch Port . . . . .	876
5.12.4 Commands . . . . .	878
<b>5.13 IGMP Snooping . . . . .</b>	<b>897</b>
5.13.1 Configuring IGMP Snooping . . . . .	897
5.13.2 Defining a Multicast Router Port on a VLAN . . . . .	897
5.13.3 IGMP Snooping Querier . . . . .	899
5.13.4 Commands . . . . .	900
<b>5.14 Priority Flow Control . . . . .</b>	<b>919</b>
5.14.1 Flow Control Threshold Configuration for Spectrum . . . . .	920
5.14.2 Commands . . . . .	922
<b>5.15 Quality of Service (QoS) . . . . .</b>	<b>926</b>
5.15.1 QoS Classification . . . . .	926
5.15.1.1 Trust Levels . . . . .	926
5.15.1.2 Switch Priority to IEEE Priority Mapping . . . . .	927
5.15.1.3 Default QoS Configuration . . . . .	927
5.15.2 QoS Rewrite . . . . .	928
5.15.2.1 Switch-priority to PCP,DEI Re-marking Mapping . . . . .	928
5.15.2.2 Switch-priority to DSCP Re-marking Mapping . . . . .	928
5.15.2.3 DSCP to Switch-priority in Router . . . . .	928
5.15.2.4 Default Configuration . . . . .	928
5.15.3 Queuing and Scheduling (ETS) for SwitchX . . . . .	928
5.15.4 Queuing and Scheduling (ETS) for Spectrum . . . . .	930
5.15.4.1 Traffic Class . . . . .	931
5.15.4.2 Traffic Shapers . . . . .	931
5.15.4.3 Default Shaper Configuration . . . . .	931
5.15.5 RED and ECN . . . . .	932
5.15.6 Commands . . . . .	933
5.15.6.1 QoS Classification . . . . .	933
5.15.6.2 QoS Rewrite . . . . .	950
5.15.6.3 Queuing and Scheduling (ETS) . . . . .	955

5.15.6.4 RED & ECN .....	964
5.15.6.5 RED & ECN .....	972
5.16 Shared Buffers .....	975
5.16.1 Traffic Pool Configuration .....	975
5.16.2 Lossless Traffic .....	976
5.16.3 Advanced Buffer Configuration .....	976
5.16.3.1 Packet Buffering Classification .....	976
5.16.3.2 Buffer Allocation .....	977
5.16.3.3 Pools .....	978
5.16.3.4 Usage Counting .....	978
5.16.3.5 Control Traffic Buffering .....	978
5.16.3.6 Default Configuration .....	979
5.16.3.7 Configuration Example .....	979
5.16.4 Commands .....	982
5.17 Storm Control .....	1009
5.17.1 Commands .....	1010
5.18 Head-of-Queue Lifetime Limit .....	1012
5.18.1 Commands .....	1013
5.19 User Defined Keys .....	1014
5.19.1 Commands .....	1015
5.20 Port Mirroring .....	1020
5.20.1 Mirroring Sessions .....	1020
5.20.1.1 Source Interface .....	1021
5.20.1.2 Destination Interface .....	1021
5.20.1.3 Header Format .....	1022
5.20.1.4 Congestion Control .....	1023
5.20.1.5 Truncation .....	1023
5.20.2 Configuring Mirroring Sessions .....	1023
5.20.3 Verifying Mirroring Sessions .....	1025
5.20.4 Commands .....	1026
5.20.4.1 Config .....	1026
5.20.4.2 Config Monitor Session .....	1027
5.20.4.3 Show .....	1033
5.21 sFlow .....	1035
5.21.1 Flow Samples .....	1035
5.21.2 Statistical Samples .....	1036
5.21.3 sFlow Datagrams .....	1036
5.21.4 Sampled Interfaces .....	1036
5.21.5 Configuring sFlow .....	1036
5.21.6 Verifying sFlow .....	1037
5.21.7 Commands .....	1038
5.21.7.1 Config .....	1038

5.21.7.2 Config sFlow.....	1041
5.21.7.3 Show .....	1049
<b>5.22 Transport Applications .....</b>	<b>1050</b>
5.22.1 RDMA over Converged Ethernet (RoCE).....	1050
5.22.1.1 RoCE Overview.....	1050
5.22.1.2 RoCE Configuration .....	1051
5.22.1.3 Configuring Switch Systems .....	1052
5.22.1.4 Configuring Router (PFC only) .....	1052
5.22.1.5 Configuring the RoCE Mode .....	1052
<b>5.23 802.1x Protocol.....</b>	<b>1054</b>
5.23.1 802.1x Operating Modes .....	1055
5.23.2 Configuring 802.1x .....	1055
5.23.3 Commands .....	1057
<b>5.24 Voice VLAN .....</b>	<b>1073</b>
5.24.1 Configuring Voice VLAN .....	1073
5.24.2 Limitations.....	1076
<b>5.25 Store-and-Forward .....</b>	<b>1077</b>
5.25.1 General .....	1077
5.25.2 Commands .....	1078
<b>Chapter 6 IP Routing .....</b>	<b>1079</b>
6.1 General .....	1079
6.1.1 IP Interfaces.....	1079
6.1.1.1 Configuring a VLAN Interface .....	1080
6.1.1.2 Configuring a Loopback Interface.....	1080
6.1.1.3 Configuring a Router Port Interface.....	1081
6.1.2 Equal Cost Multi-Path Routing (ECMP) .....	1082
6.1.2.1 Hash Functions.....	1083
6.1.3 Virtual Routing and Forwarding.....	1084
6.1.4 Commands.....	1085
6.1.4.1 General.....	1085
6.1.4.2 IP Interfaces .....	1095
6.1.4.3 Interface VLAN.....	1097
6.1.4.4 Loopback Interface .....	1109
6.1.4.5 Routing and ECMP .....	1113
6.1.4.6 Network to Media Resolution (ARP) .....	1119
6.1.4.7 IP Diagnostic Tools.....	1123
6.1.4.8 QoS .....	1127
6.2 IPv6 .....	1128
6.2.1 Neighbor Discovery Protocol .....	1128
6.2.2 Configuring IPv6 .....	1129
6.2.3 Commands.....	1131
6.3 OSPF.....	1161

6.3.1 Router ID .....	1161
6.3.2 ECMP .....	1161
6.3.3 Configuring OSPF.....	1162
6.3.4 Verifying OSPF.....	1164
6.3.5 Commands.....	1166
6.3.5.1 Config .....	1166
6.3.5.2 Config Router.....	1168
6.3.5.3 Interface .....	1180
6.3.5.4 Show .....	1193
6.4 BGP .....	1203
6.4.1 State Machine .....	1203
6.4.2 Default Address Family.....	1203
6.4.3 Default Route Originate .....	1204
6.4.4 Peer Groups and Update Groups.....	1204
6.4.5 Configuring BGP .....	1204
6.4.6 Verifying BGP.....	1205
6.4.7 Commands.....	1207
6.4.7.1 Config .....	1207
6.4.7.2 Config Router.....	1210
6.4.7.3 Show .....	1261
6.4.8 IP AS-Path Access-List.....	1275
6.4.8.1 Commands .....	1275
6.4.9 IP Community-List.....	1277
6.4.9.1 Commands .....	1277
6.5 BFD Infrastructure .....	1280
6.5.1 Session Establishment .....	1280
6.5.2 Interaction with Protocols .....	1280
6.5.3 Config Commands .....	1282
6.5.4 Interface Commands.....	1284
6.6 Policy Rules .....	1290
6.6.1 Route Map .....	1290
6.6.1.1 Commands .....	1291
6.6.2 IP Prefix-List .....	1321
6.6.2.1 Commands .....	1322
6.7 Multicast (IGMP and PIM) .....	1324
6.7.1 Basic PIM-SM.....	1324
6.7.2 Source-Specific Multicast (SSM).....	1325
6.7.3 Bootstrap Router.....	1325
6.7.4 Configuring Multicast .....	1326
6.7.4.1 Configuring IGMP.....	1326
6.7.4.2 Verifying IGMP.....	1327
6.7.4.3 Configuring PIM .....	1328

6.7.5 Commands .....	1329
6.7.5.1 PIM .....	1329
6.7.5.2 Multicast .....	1353
6.7.5.3 IGMP .....	1357
6.8 VRRP .....	1370
6.8.1 Load Balancing .....	1370
6.8.2 Configuring VRRP .....	1371
6.8.3 Verifying VRRP .....	1373
6.8.4 Commands .....	1374
6.9 MAGP .....	1385
6.9.1 Configuring MAGP .....	1385
6.9.2 Commands .....	1387
6.10 DHCP Relay .....	1394
6.10.1 DHCP-R Virtual Routing and Forwarding (VRF) Auto-Helper .....	1394
6.10.2 Commands .....	1395
6.10.2.1 Interface Commands .....	1404
6.10.2.2 Show Commands .....	1405
6.10.3 DHCPv6 Relay .....	1407
6.10.3.1 Commands .....	1407

## **Appendix A Enhancing System Security According to NIST SP 800-131A . 1419**

A.1 Overview .....	1419
A.2 Web Certificate .....	1419
A.3 SNMP .....	1420
A.4 SSH .....	1420
A.5 HTTPS .....	1421
A.6 LDAP .....	1422

## **Appendix B Show Commands Supported by JSON API . 1424**

## **Appendix C Splunk Integration with Mellanox Products . 1433**

C.1 Getting Started with Splunk .....	1433
C.2 Switch Configuration .....	1433
C.3 Adding a Task .....	1434
C.4 Retrieving Data from TCP and UDP Ports .....	1436
C.5 SNMP Input to Poll Attribute Values and Catch Traps .....	1438
C.6 Getting Started .....	1438
C.7 Configuration .....	1438

## List of Tables

Table 1:	Reference Documents .....	36
Table 2:	Glossary .....	36
Table 3:	General System Features .....	39
Table 4:	Ethernet Features .....	40
Table 5:	Serial Terminal Program Configuration for PPC Based Systems .....	43
Table 6:	Serial Terminal Program Configuration for x86 Based Systems.....	43
Table 7:	Configuration Wizard Session - IP Configuration by DHCP.....	44
Table 8:	Configuration Wizard Session - IP Zeroconf Configuration .....	46
Table 9:	Configuration Wizard Session - Static IP Configuration .....	47
Table 10:	LED Behavior Details .....	69
Table 11:	CLI Modes and Config Context .....	69
Table 12:	Syntax Conventions .....	70
Table 13:	Angled Brackets Parameter Description .....	74
Table 14:	CLI Keyboard Shortcuts .....	77
Table 15:	WebUI Setup Submenus .....	79
Table 16:	WebUI System Submenus .....	80
Table 17:	WebUI Security Submenus .....	81
Table 18:	WebUI Ports Submenus.....	81
Table 19:	WebUI Status Submenus.....	81
Table 20:	WebUI ETH Mgmt Submenus .....	82
Table 21:	WebUI IP Route Submenus .....	83
Table 22:	Module Type .....	85
Table 23:	Device Type .....	85
Table 24:	Sensor Type .....	86
Table 25:	PTP Message Formats .....	210
Table 26:	Default PTP Profile Attributes.....	212
Table 27:	Supported Event Notifications and MIB Mapping.....	326
Table 28:	User Roles (Accounts) and Default Passwords .....	373
Table 29:	Chassis Manager Information .....	469
Table 30:	System Health Monitor Alerts Scenarios .....	470
Table 31:	LWR Configuration Behavior.....	475
Table 32:	Standard MIBs – Textual Conventions and Conformance MIBs.....	509

Table 33: Standard MIBs – Chassis and Switch .....	509
Table 34: Private MIBs Supported.....	511
Table 35: SNMP Traps .....	511
Table 36: Supported SET OIDs.....	515
Table 37: Ethernet and Port-Channel Interface Capabilities .....	562
Table 38: VLAN Capabilities.....	562
Table 39: L2 Ethernet and Port-Channel Interface Capabilities .....	562
Table 40: LAG Capabilities .....	563
Table 41: L3 Interface Capabilities .....	563
Table 42: OSPF Interface Capabilities .....	563
Table 43: OSPF Area Capabilities.....	564
Table 44: Router OSPF Capabilities.....	564
Table 45: Protocol Enable/Disable Capabilities .....	564
Table 46: Fetched Image Capabilities .....	564
Table 47: Installed Image Capabilities .....	565
Table 48: Fetched Image Capabilities .....	565
Table 49: Number of Resources per Node in Strict Mode .....	583
Table 50: Number of Resources per Node in Strict Mode for SwitchX Based Systems ..	584
Table 51: Number of Resources per Node in Strict Mode for Spectrum Based Systems ..	584
Table 52: LR4/ER4 Switch and Port Support .....	608
Table 53: Supported VLANs by RPVST per Switch System .....	703
Table 54: Summary of ACL Capability .....	779
Table 55: OpenFlow 1.3 Pipeline Capabilities Summary Table .....	829
Table 56: Packet Classification Rules .....	926
Table 57: Default QoS Configuration .....	927
Table 58: Default Shaper Configuration .....	931
Table 59: Single Packet Usage Counting.....	978
Table 60: Mirroring Parameters .....	1021
Table 61: List of Statistical Counters.....	1036
Table 62: JSON API Show Commands.....	1424

## List of Figures

Figure 1:	Managing an Ethernet Fabric Using MLNX-OS® .....	41
Figure 2:	Console Ports SX10xx Systems .....	42
Figure 3:	MLNX-OS Login Window .....	50
Figure 4:	EULA Prompt .....	51
Figure 5:	Welcome Popup .....	52
Figure 6:	Display After Login .....	52
Figure 7:	No Licenses Installed .....	61
Figure 8:	Enter License Key(s) in Text Box .....	62
Figure 9:	Installed License .....	62
Figure 10:	WebUI .....	79
Figure 11:	Index Scheme .....	84
Figure 12:	PTP Clock Synchronization Example .....	210
Figure 13:	Boundary Clock Master/Slave Functionality .....	212
Figure 14:	JSON API WebUI Example .....	531
Figure 15:	JSON API WebUI Example .....	532
Figure 16:	Accepting an Agent Request through the Console .....	559
Figure 17:	Break-Out Cable .....	604
Figure 18:	Interface Isolation Example .....	637
Figure 19:	RPVST Network Config .....	703
Figure 20:	RPVST and RSTP Cluster .....	704
Figure 21:	MAC Learning Disable Example Case .....	737
Figure 22:	Basic MLAG Setup .....	746
Figure 23:	Basic MLAG Topology .....	749
Figure 24:	MLNX-OS and OpenFlow Pipeline .....	828
Figure 25:	Xon/Xoff Configuration .....	921
Figure 26:	RED/ECN Drop Profiles .....	932
Figure 27:	Overview of Mirroring Functionality .....	1020
Figure 28:	Mirror to Analyzer Mapping .....	1020
Figure 29:	Header Format Options .....	1023
Figure 30:	Mirroring Session .....	1024
Figure 31:	sFlow Functionality Overview .....	1035
Figure 32:	RoCEv2 and RoCE Frame Format Differences .....	1050
Figure 33:	RoCEv2 Protocol Stack .....	1051
Figure 34:	Tagging Voice Packets with a Different VLAN ID .....	1073

Figure 35: ECMP .....	1082
Figure 36: Multiple Hash Functions .....	1083
Figure 37: IPv6 Network .....	1129
Figure 38: OSPF Basic Topology .....	1162
Figure 39: Basic BGP Configuration .....	1204
Figure 40: Common VRRP Configuration with Load Balancing .....	1371
Figure 41: Add Data Option .....	1434
Figure 42: Monitor Icon .....	1435
Figure 43: TCP/UDP .....	1436
Figure 44: TCP/UDP Fields .....	1436
Figure 45: Input Settings .....	1437
Figure 46: Start Searching .....	1438
Figure 47: SNMP .....	1439
Figure 48: SNMP Attributes Polling Settings .....	1439
Figure 49: SNMP Attributes Polling Settings .....	1440
Figure 50: Mellanox-Switch .....	1440
Figure 51: Add to Search .....	1441
Figure 52: Search Options .....	1441

## Document Revision History

### Rev 4.80 - November 05, 2017

Added:

- Section 2.1.1, “Configuring the Switch with ZTP,” on page 48
- Section 2.4, “Zero-touch Provisioning,” on page 53
- the command “logging level” on page 294
- the command “show log” on page 300
- Section 4.9.2, “Configuring Signal Degradation Monitoring,” on page 323
- the command “telemetry threshold” on page 355
- the command “telemetry threshold level” on page 356
- the command “clear telemetry” on page 357
- the command “show telemetry threshold” on page 362
- Section 4.19, “Control Plain Policing,” on page 575
- Section 5.10.3, “ACL Logging,” on page 778
- Section 5.10.4, “ACL Capability Summary,” on page 779
- the command “bind-point rif” on page 782
- the command “remark” on page 783
- the command “shared-counter” on page 784
- the command “clear shared-counters” on page 785
- the command “clear counters” on page 786
- the command “{ipv4/ipv6/mac/ipv4-udk/mac-udk} access-list clear counters” on page 787
- the command “deny/permit (IPv6 ACL rule)” on page 799
- the command “deny/permit (IPv6 TCP ACL rule)” on page 800
- the command “deny/permit (IPv6 TCP-UDP/UDP ACL rule)” on page 802
- the command “deny/permit (IPv6 ICMPv6 ACL rule)” on page 804
- the command “deny/permit (MAC UDK ACL rule)” on page 805
- the command “deny/permit (IPv4 UDK ACL rule)” on page 807
- the command “deny/permit (IPv4 TCP UDK ACL rule)” on page 809
- the command “deny/permit (IPv4 TCP-UDP/UDP UDK ACL rule)” on page 811
- the command “deny/permit (IPv4 ICMP UDK ACL rule)” on page 813
- the command “port access-group (IPv4/IPv4 UDK/IPv6/MAC/MAC UDK)” on page 815
- the command “access-list log” on page 817
- the command “show access-lists (ipv4/ipv4-udk/ipv6/mac/mac-udk)” on page 821

- the command “show access-lists shared-counters (ipv4/ipv4-udk/ipv6/mac/mac-udk)” on page 823
- the command “show access-lists log” on page 825
- the command “show access-lists log config” on page 826
- the command “traffic pool” on page 982
- the command “type” on page 983
- the command “map switch-priority” on page 984
- the command “type map switch-priority” on page 985
- the command “memory percent” on page 986
- the command “advanced buffer management” on page 987
- the command “reserved shared size” on page 990
- the command “pool size type” on page 991
- the command “cable-length” on page 998
- the command “show buffers mode” on page 999
- the command “show buffers pools” on page 1005
- the command “show buffers pools mc-buffers” on page 1006
- the command “show qos interface” on page 944
- the command “show qos interface l2-mapping” on page 945
- the command “show qos interface l3-mapping” on page 946
- the command “show qos interface rewrite-mapping” on page 947
- the command “show qos interface tc-mapping” on page 948
- the command “show qos mapping ingress interface egress interface” on page 949
- the command “show traffic pool” on page 1007
- the command “show traffic pool interface ethernet” on page 1008
- Section 5.18, “Head-of-Queue Lifetime Limit,” on page 1012
- Section 5.19, “User Defined Keys,” on page 1014
- Section 6.2, “IPv6,” on page 1128
- the command “clear ip dhcp relay counters” on page 1403
- the command “clear ipv6 dhcp relay counters” on page 1415
- the command “show magp interface vlan” on page 1393
- Appendix C, “Splunk Integration with Mellanox Products” on page 1433

Deleted:

- the command “mc-unaware tc binding”

Updated:

- Table 21, “WebUI IP Route Submenus,” on page 83
- the command “cli max-sessions” on page 91
- the command “show ip dhcp” on page 183

- the command “show interfaces ethernet” on page 623
- the command “show interfaces counters” on page 625
- the command “show isolation-group” on page 644
- the command “show interfaces port-channel” on page 661
- the command “show spanning-tree detail” on page 729
- the command “show spanning-tree vlan” on page 733
- the command “show interfaces mlag-port-channel” on page 769
- the command “{ipv4/ipv6/mac/ipv4-udk/mac-udk} access-list” on page 781
- the command “deny/permit (IPv4 ACL rule)” on page 791
- the command “show access-lists (ipv4/ipv4-udk/ipv6/mac/mac-udk)” on page 821
- the command “show access-lists summary” on page 824
- the command “show dcb ets (Spectrum)” on page 963
- the command “map pool type reserved” on page 993
- the command “pool mc-buffer” on page 996
- the command “pool description” on page 997
- the command “show buffers status” on page 1000
- the command “show buffers details” on page 1002
- the command “destination interface” on page 1027
- the command “show monitor session summary” on page 1034
- the command “show ip interface” on page 1107
- the command “show ip route” on page 1115
- the command “show ip route interface” on page 1117
- the command “show vrrp detail” on page 1383
- the command “show vrrp statistics” on page 1384
- the command “show magp” on page 1392
- the command “show ip dhcp relay counters” on page 1406
- the command “show ipv6 dhcp relay” on page 1416
- Appendix B, “Show Commands Supported by JSON API” on page 1424

## Rev 4.70

### Software Ver. 3.6.4114, August 20, 2017

- No changes

### Software Ver. 3.6.4112, August 7, 2017

Added the following sections:

- Section 4.9, “Signal Degradation Monitoring,” on page 323

- Section 6.7.1, “Basic PIM-SM,” on page 1324
- Section 6.7.2, “Source-Specific Multicast (SSM),” on page 1325

Updated the following sections:

- Section 3.3, “Web Interface Overview,” on page 78
- Section 5.8, “MLAG,” on page 746
- Section 5.17, “Storm Control,” on page 1009
- Section 5.25, “Store-and-Forward,” on page 1077
- Section 6.2, “IPv6,” on page 1128

Added the following commands:

- “protocol ptp” on page 213
- “ptp domain” on page 214
- “ptp priority” on page 215
- “ptp enable” on page 216
- “ptp announce interval” on page 217
- “ptp announce timeout” on page 218
- “ptp delay-req interval” on page 219
- “ptp sync interval” on page 220
- “show ptp” on page 221
- “show ptp clock” on page 222
- “show ptp clock parent” on page 223
- “show ptp interface ethernet” on page 224
- “show ptp interface ethernet counters” on page 225
- “interface ethernet signal-degrade” on page 324
- “show interfaces ethernet signal-degrade” on page 325
- “docker label” on page 599
- “docker copy-sdk” on page 600
- “show docker labels” on page 603
- “show spanning-tree vlan topo-change-history” on page 734
- “show spanning-tree mst topo-change-history” on page 735
- “show spanning-tree topo-change-history” on page 736
- “bgp default” on page 1260
- “show ip bgp update-group” on page 1274

Updated the following commands:

- “show interfaces ethernet link-diagnostics” on page 321
- “start” on page 596
- “show interfaces ethernet” on page 623

- “show spanning-tree detail” on page 729
- “storm-control level” on page 1010
- “show storm-control” on page 1011
- “switchmode store-and-forward” on page 1078
- “ipv6 enable” on page 1131
- “ipv6 address” on page 1132
- “ipv6 nd managed-config-flag” on page 1133
- “ipv6 nd prefix” on page 1136
- “ipv6 nd ra dns-servers lifetime” on page 1137
- “ipv6 nd ra dns-suffixes lifetime” on page 1139
- “ipv6 nd ra dns-server” on page 1138
- “ipv6 nd ra dns-suffix” on page 1140
- “ipv6 nd ra hop-limit” on page 1141
- “ipv6 nd ra interval max-period” on page 1142
- “ipv6 nd ra lifetime” on page 1143
- “clear ipv6 neighbors” on page 1152
- “ipv6 route” on page 1153
- “show ipv6 interface” on page 1156
- “show ipv6 route” on page 1159
- “neighbor activate” on page 1253
- “neighbor default-originate” on page 1254
- “show ip bgp paths” on page 1269

Removed the following sections:

- Bidirectional PIM
- PIM Load-Sharing

Removed the following commands:

- ip pim bidir shutdown
- ip pim multipath rp
- ip pim border

## **Software Ver. 3.6.4071, July 17, 2017**

Added:

- Section 6.5, “BFD Infrastructure,” on page 1280
- Section 6.10.3, “DHCPv6 Relay,” on page 1407
- Section 6.4.2, “Default Address Family,” on page 1203
- Section 6.4.3, “Default Route Originate,” on page 1204
- Section 6.4.4, “Peer Groups and Update Groups,” on page 1204

Updated:

- Commands in Section 6.4, “BGP,” on page 1203

## Software Ver. 3.6.4050, June 30, 2017

Added:

- Section 4.3, “PTP,” on page 209
- Section 4.8, “Link Diagnostic Per Port,” on page 316
- the command “show interfaces ethernet link-diagnostics” on page 321
- the command “telemetry threshold” on page 368
- the command “telemetry threshold log” on page 369
- the command “telemetry threshold syslog” on page 370
- the command “telemetry threshold level” on page 371
- the command “clear telemetry” on page 409
- the command “show telemetry” on page 372
- MELLANOX-QOS MIB to Table 34, “Private MIBs Supported,” on page 511
- the command “json-gw synchronous-request-timeout” on page 556
- the command “show interfaces status” on page 622
- the command “show mac-address-table interface” on page 744
- the command “clear lldp counters” on page 678
- Section 5.17, “Storm Control,” on page 1009
- the command “storm-control level” on page 1010
- the command “show storm-control” on page 1011
- Section 5.25, “Store-and-Forward,” on page 1077
- the command “ip pim ssm range” on page 1341
- the command “interface vlan <id> no-autostate” on page 1098

Updated:

- the command “switchmode store-and-forward” on page 1078
- the command “ssh server security strict” on page 115
- the commands ntp peer \* and ntp server \* to support hostname as ip\_address option – see Section 4.2.3, “Commands,” on page 191
- the command “crypto certificate generation” on page 430
- the command “crypto certificate name” on page 431
- the command “clear counters” on page 481
- Section 4.17.2, “JSON API,” on page 519
- the command “show json-gw” on page 557
- the command “module-type” on page 613
- the command “show interfaces counters” on page 625

- the command “show interfaces ethernet transceiver diagnostics” on page 634
- the command “channel-group” on page 652
- the command “destination interface” on page 1027
- the command “switchport” on page 1095
- the command “ip pim hello-interval” on page 1339
- the command “ip pim join-prune-interval” on page 1340

Removed:

- the command debug ethernet ip dhcp-relay
- the command debug ethernet ip ospf
- the command debug ethernet ip arp
- the command debug ethernet ip igmp-l3
- the command debug ethernet ip pim
- the command debug ethernet ip bgp
- the command debug ethernet ip all

## Rev 4.60

### Software Ver. 3.6.3640, June 4, 2017

Added:

- the command “switchmode store-and-forward” on page 64
- the command “show switchmode” on page 65
- the command “fae switchmode verify” on page 66

Updated:

- the command “show running-config” on page 308
- the command “docker install-sdk commit” on page 682
- the command “show interfaces ethernet” on page 754
- the command “show interfaces port-channel compatibility-parameters” on page 798
- the command “interface port-channel” on page 777
- the command “channel-group” on page 782
- the command “module-type” on page 742

### Software Ver. 3.6.3552, May 23, 2017

- No changes

### Software Ver. 3.6.3550, May 19, 2017

Updated:

- the command “nve bridge” on page 952

- the command “nve fdb flood bridge address” on page 953

### **Software Ver. 3.6.3532, May 14, 2017**

Updated:

- the command “show lldp interfaces” on page 1005
- the command “dcb application-priority” on page 1002

### **Software Ver. 3.6.3522, May 4, 2017**

Added:

- Section 4.27, “Linux Dockers,” on page 703

### **Software Ver. 3.6.3508, April 23, 2017**

- No changes

### **Software Ver. 3.6.3506, April 23, 2017**

- No changes

### **Software Ver. 3.6.3504, April 13, 2017**

Updated:

- the command “redistribute” on page 943
- the command “show ip ospf request-list” on page 972
- the command “show ip ospf retransmission-list” on page 973
- the command “show ip ospf summary-address” on page 974

### **Software Ver. 3.6.3234, April 3, 2017**

Removed:

- the command “led uid”
- the command “show leds”

Updated:

- the command “logging port”
- the command “logging trap”
- the command “show logging”
- the command “show log”

### **Software Ver. 3.6.3232, March 29, 2017**

Removed:

- the command “show proxy-arp mode”
- Section “Unit Identification LED”

## **Software Ver. 3.6.3200, February 2017**

Added:

- the command “show openflow groups” on page 935
- the command “show openflow meters” on page 937
- the command “show openflow flows table” on page 938
- the command “show openflow flows cookie” on page 939
- the command “show openflow table match-keys” on page 940
- the command “show openflow table match-keys supported” on page 941

## **Software Ver. 3.6.3130, February 28, 2017**

Added:

- Appendix C: Show Commands Supported by JSON API

Updated:

- the command “show logging” on page 332
- the command “show log” on page 333

## **Software Ver. 3.6.3004, January 31, 2017**

Added:

- Section 5.11.2, “VMware Network Virtualization and Security Platform (NSX) Configuration,” on page 944
- the command “protocol nve” on page 950
- the command “interface nve” on page 951
- the command “shutdown” on page 954
- the command “vxlan source interface loopback” on page 955
- the command “nve mode only” on page 956
- the command “clear nve counters” on page 957
- the command “show interfaces nve” on page 958
- the command “show interfaces nve counters” on page 959
- the command “show interfaces nve flood” on page 960
- the command “show interfaces nve mac-address-table” on page 961
- the command “show interfaces nve mac-address-table local learned unicast” on page 962
- the command “show interfaces nve mac-address-table remote configured multicast” on page 963
- the command “show interfaces nve mac-address-table remote configured unicast” on page 964
- the command “show interfaces nve peers” on page 965
- the command “ovs ovsdb server” on page 966

- the command “ovs ovsdb manager remote” on page 967
- the command “ovs ovsdb server listen” on page 968
- Section 3.1.7.3, ““json-print” CLI Option,” on page 70
- Section 4.21.2, “JSON API,” on page 583
- Section 4.21.4.3, “JSON API Commands,” on page 622
- Section 4.14, “Telemetry,” on page 389 (Including subsections)
- the command “neighbor no-password” on page 1010
- the command “neighbor no-route-map” on page 1016
- the command “neighbor no-update-source” on page 1027
- the command “show snmp set-permission” on page 618
- the command “snmp-server enable set-permission” on page 606
- the command “show interfaces ethernet counters tc” on page 1027
- the command “show interfaces ethernet counters pg” on page 1028
- the command “show interfaces ethernet counters pfc prio” on page 1029
- the command “show ip igmp snooping membership” on page 986
- the command “show lldp remote” on page 1006
- the command “ip dhcp relay” on page 1189
- the command “ip dhcp relay instance” on page 1196
- the command “vrf” on page 1193
- the command “port” on page 1194
- the command “vrf-auto-helper” on page 1195
- Section 5.11, “VXLAN,” on page 942
- Appendix C, “Show Commands Supported by JSON API,” on page 1174

Updated:

- the command “system resource table” on page 700
- the command “show system resource table” on page 701
- the command “bestpath as-path multipath-relax” on page 985
- the command “bgp listen range peer-group” on page 988
- the command “cluster-id” on page 990
- the command “graceful-restart helper” on page 994
- the command “neighbor advertisement-interval” on page 996
- the command “neighbor allowas-in” on page 997
- the command “neighbor ebgp-multihop” on page 999
- the command “neighbor export-localpref” on page 1000
- the command “neighbor import-localpref” on page 1002
- the command “neighbor local-as” on page 1003

- the command “neighbor maximum-prefix” on page 1005
- the command “neighbor next-hop-peer” on page 1006
- the command “neighbor peer-group” on page 1011
- the command “neighbor route-reflector-client” on page 1017
- the command “neighbor send-community” on page 1018
- the command “neighbor timers” on page 1023
- the command “neighbor transport connection-mode passive” on page 1025
- the command “router-id” on page 1031
- the command “match as-path” on page 1078
- the command “set community-list” on page 1092
- the command “hostname” on page 160
- the command “image options” on page 267 “serve all” parameter description
- note in Section 4.7.6, “Downgrading MLNX-OS Software,” on page 249
- Section 4.8.4.2, “Text Configuration Files,” on page 272
- the command “show running-config” on page 308
- Section 4.21.3, “XML API,” on page 598
- Section 4.26, “Resource Scale,” on page 696
- the command “fec-override” on page 680
- Section 5.10.2, “OpenFlow 1.3 Support,” on page 900
- the command “ip igmp snooping static-group” on page 978
- the command “ip igmp snooping version” on page 980
- the command “openflow mode hybrid” on page 911
- the command “show ip igmp snooping groups” on page 984
- the command “show ip igmp snooping querier” on page 988
- the command “show ip igmp snooping statistics” on page 990
- the command “show sflow” on page 1101
- Section 6.4.7, “Commands,” on page 980 under BGP
- Section 6.6, “Policy Rules,” on page 1071
- the command “address” on page 1190
- the command “always-on” on page 1191
- the command “information option” on page 1192
- the command “clear ip dhcp relay counters” on page 1197
- the command “show ip dhcp relay” on page 1199
- the command “show ip dhcp relay counters” on page 1200
- the command “clear ip bgp” on page 981
- the command “logging port” on page 312

- the command “logging trap” on page 331

## Rev 4.50 – September 30, 2016

Added:

- Section 3.2.7.2, ““watch” CLI Monitoring Option,” on page 74
- the command “ntp server trusted-enable” on page 198
- the command “logging <syslog IPv4 address/Hostname> port” on page 272
- the command “install-from-usb” on page 566
- the command “boot-delay” on page 671
- the command “show interfaces ethernet rates” on page 688
- the command “show interfaces ethernet transceiver diagnostics” on page 693
- the command “show mac-address-table summary” on page 782
- Section 5.10.2, “OpenFlow 1.3 Support,” on page 819
- Section 8.3, “Proxy-ARP Event Notifications,” on page 1571
- Appendix B, “Mellanox NEO™ on Switch” on page 1331

Updated:

- Section 1.2, “Ethernet Features,” on page 41 with Spectrum™ unicast addresses
- Section 4.8.4.1, “BIN Configuration Files,” on page 271
- Section 4.8.4.2, “Text Configuration Files,” on page 272
- the command “reset factory” on page 245
- the command “show running-config” on page 308
- Section 4.9.2, “Remote Logging,” on page 310 with Step 3
- the command “username” on page 419
- Section 4.13.5, “Unit Identification LED,” on page 468
- the command “led uid” on page 471
- the command “show leds” on page 548
- Section 4.14.1.2, “Private MIB,” on page 499
- Section “Changing Configuration with SNMP” on page 506
- Section 4.16.1, “Virtual Machine Configuration,” on page 557
- the command “show interfaces ethernet” on page 682
- Section 5.4.6, “Configuring MLAG,” on page 729
- Section 5.9.7, “MSTP,” on page 785
- Section 5.10.4, “Configuring Secure Connection to OpenFlow,” on page 825
- the command “controller-ip” on page 832
- the command “controller-ip” on page 833
- Section 5.12, “IGMP Snooping,” on page 868 with IGMPv3 note

- Section 5.15.2, “ACL Actions,” on page 949
- the command “deny/permit (IPv4 TCP/UDP/ICMP ACL rule)” on page 956
- the command “monitor session” on page 971
- Section 6.7.1, “Configuring MAGP,” on page 1305

## Rev 4.40 – June 28, 2016

Added:

- Section 4.6.5.3, “Switching to Partition with Older Software Version,” on page 258 for clarity
- Section 4.7.4.1, “BIN Configuration Files,” on page 278
- Section 4.10.1, “System File Encryption,” on page 407
- Section 4.13.5, “Unit Identification LED,” on page 468
- the command “crypto encrypt-data” on page 408
- the command “show crypto encrypt-data” on page 423
- the command “led uid” on page 471
- the command “show leds” on page 480
- the command “show protocols” on page 485
- the command “show system capabilities” on page 487
- Section 5.1.5, “Forward Error Correction,” on page 668
- the command “show interfaces ethernet transceiver counters” on page 691
- the command “show interfaces ethernet transceiver counters details” on page 692
- the command “show interfaces ethernet transceiver raw” on page 695
- Section 5.2, “Interface Isolation,” on page 696
- the command “show interfaces port-channel counters” on page 722
- “Enabling L3 Forwarding with User VRF” on page 733
- the command “show interfaces mlag-port-channel counters” on page 749
- the command “switchport voice” on page 764
- Section 5.6, “Voice VLAN,” on page 766
- the command “ip igmp snooping clear counters” on page 874
- the command “ip igmp snooping version” on page 879
- the command “show ip igmp snooping querier counters” on page 888
- the command “lldp med-tlv-select” on page 900
- Section 5.14.1, “QoS Classification,” on page 909
- Section 5.14.2, “QoS Rewrite,” on page 911
- Section 5.14.3, “Queuing and Scheduling (ETS) for SwitchX,” on page 912
- Section 5.14.6.1, “QoS Classification,” on page 917
- the command “no area” on page 1121

- the command “neighbor send-community” on page 1184

Updated:

- the command “ip arp timeout” on page 180
- Section 4.3.6, “Image Maintenance via Mellanox ONIE,” on page 222
- the command “image fetch” on page 229
- the command “configuration switch-to” on page 259
- “Changing Configuration with SNMP” on page 506 with `BinaryDelete` and `TextDelete` commands
- the command “show inventory” on page 479
- the command “show interfaces ethernet” on page 682
- the command “show interfaces ethernet counters” on page 685
- the command “show interfaces port-channel” on page 720
- the command “show interfaces mlag-port-channel” on page 748
- Section 5.8.1, “Configuring Unicast Static MAC Address,” on page 775
- the command “show openflow” on page 837
- the command “show openflow detail” on page 838
- the command “show openflow flows” on page 839
- the command “show openflow statistics” on page 840
- the command “ip igmp snooping static-group” on page 877
- the command “show ip igmp snooping” on page 882
- the command “show ip igmp snooping groups” on page 883
- the command “show ip igmp snooping statistics” on page 889
- Section 5.13.2, “DCBX,” on page 892
- the command “show lldp interfaces” on page 903
- Section 5.21, “Shared Buffers,” on page 1027
- the command “ip arp timeout” on page 1095
- the command “router ospf” on page 1110
- the command “area stub” on page 1119
- the command “show ip ospf” on page 1136
- the command “show ip ospf border-routers” on page 1137
- the command “show ip ospf database” on page 1138
- the command “show ip ospf interface” on page 1140
- the command “show ip ospf neighbors” on page 1142
- the command “neighbor peer-group” on page 1177
- the command “always-on” on page 1316
- the command “clear ip dhcp relay counters” on page 1322
- the command “ip dhcp relay information option circuit-id” on page 1323

- the command “show ip dhcp relay” on page 1324
- the command “show ip dhcp relay counters” on page 1324

Removed “Security Vulnerabilities and Exposures” appendix and moved it to [www.mellanox.com/page/mlnx\\_os\\_security\\_vulnerabilities\\_and\\_exposures](http://www.mellanox.com/page/mlnx_os_security_vulnerabilities_and_exposures).

## Rev 4.30 – March 02, 2016

Added:

- Section 3.1.8, “CLI Shortcuts,” on page 71
- Section 3.4, “Management Information Bases (MIBs),” on page 79
- the command “cli max-sessions” on page 85
- the command “show cli max-sessions” on page 92
- the command “show cli num-sessions” on page 93
- the command “banner logout” on page 97
- the command “banner logout-local” on page 98
- the command “banner logout-remote” on page 99
- the command “ssh server login attempts” on page 106
- the command “ssh server login timeout” on page 107
- Section 4.1.6, “Configuring Hostname via DHCP (DHCP Client Option 12),” on page 142
- the command “dhcp hostname” on page 155
- Section 4.2.1, “NTP Authenticate,” on page 194
- Section 4.2.2, “NTP Authentication Key,” on page 194
- the command “ntp authenticate” on page 199
- the command “ntp authentication-key” on page 200
- the command “ntp peer disable” on page 201
- the command “ntp peer keyID” on page 202
- the command “ntp peer version” on page 203
- the command “ntp server disable” on page 204
- the command “ntp server keyID” on page 205
- the command “ntp server version” on page 207
- the command “ntp trusted-key” on page 208
- the command “show ntp configured” on page 211
- the command “show ntp keys” on page 212
- Section 4.3.6, “Image Maintenance via Mellanox ONIE,” on page 222
- Section 4.9.2.1, “User Re-authentication,” on page 356
- the command “aaa authentication attempts fail-delay” on page 366
- the command “show system type” on page 490

- Section 4.17, “IP Table Filtering,” on page 583
- the command “show interfaces ethernet counters” on page 685
- Section 5.14.5, “RED and ECN,” on page 915
- Section 5.14.6.4, “RED & ECN,” on page 946
- the command “ip multicast filter” on page 1614
- the command “show ip multicast interface proxy-arp” on page 1630
- the command “show ip multicast interface proxy-arp count” on page 1631
- the command “show ip multicast filter interface proxy-arp” on page 1633

Updated:

- the command “show banner” on page 101
- the command “ssh server login attempts” on page 106
- the command “ssh server security strict” on page 110
- the command “show ssh server” on page 119
- Section 4.1, “Management Interface,” on page 140
- the command “show interface configured” on page 167
- the command “show ntp” on page 210
- the command “show aaa authentication attempts” on page 378
- Table 28, “System Health Monitor Alerts Scenarios,” on page 457
- the command “show inventory” on page 479
- the command “show power” on page 483
- the command “show power consumers” on page 484
- Table 31, “Standard MIBs – Chassis and Switch,” on page 497
- Section 5.1.1, “Break-Out Cables,” on page 664
- Section 5.1.2, “56GbE Link Speed,” on page 666
- Section 5.1.5, “Forward Error Correction,” on page 668
- the command “speed” on page 677
- the command “deny/permit (MAC ACL rule)” on page 953
- the command “deny/permit (IPv4 ACL rule)” on page 955
- the command “deny/permit (IPv4 TCP/UDP/ICMP ACL rule)” on page 956
- Section 5.16.1.2, “Destination Interface,” on page 967
- the command “add source interface” on page 974
- the command “header-format” on page 975
- the command “show monitor session” on page 979
- Section 5.21, “Shared Buffers,” on page 1027
- the command “ip load-sharing” on page 1090
- the command “ip arp timeout” on page 1095

- the command “bgp listen range peer-group” on page 1158
- the command “show ip mroute” on page 1275
- the command “vrrp” on page 1295
- Section A.6.1, “Upgrading Software on the MEX6200,” on page 1650
- Section A.4, “SSH,” on page 1327

## About this Manual

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

## Intended Audience

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

## Related Documentation

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

**Table 1 - Reference Documents**

Document Name	Description
System Hardware User Manual	This document contains hardware descriptions, LED assignments and hardware specifications among other things.
Switch Product Release Notes	Please look up the relevant SwitchX®-based switch system/series release note file
Mellanox Virtual Modular Switch Reference Guide	This reference architecture provides general information concerning Mellanox L2 and L3 Virtual Modular Switch (VMS) configuration and design.
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).
CLI	Command Line Interface. A user interface in which you type commands at the prompt
DCB	Data Center Bridging

**Table 2 - Glossary**

DCBX	DCBX protocol is an extension of the Link Layer Discovery Protocol (LLDP). DCBX end points exchange request and acknowledgment messages. For flexibility, parameters are coded in a type-length-value (TLV) format.
DHCP	The Dynamic Host Configuration Protocol (DHCP) is an automatic configuration protocol used on IP networks.
DNS	Domain Name System. A hierarchical naming system for devices in a computer network
ETS	ETS provides a common management framework for assignment of bandwidth to traffic classes.
FTP/TFTP/sFTP	File Transfer Protocol (FTP) is a standard network protocol used to transfer files from one host to another over a TCP-based network, such as the Internet.
Gateway	A network node that interfaces with another network using a different network protocol
HA (High Availability)	A system design protocol that provides redundancy of system components, thus enables overcoming single or multiple failures in minimal downtime
Host	A computer platform executing an Operating System which may control one or more network adapters
LACP	Link Aggregation Control Protocol (LACP) provides a method to control the bundling of several physical ports together to form a single logical channel. LACP allows a network device to negotiate an automatic bundling of links by sending LACP packets to the peer (directly connected device that also implements LACP).
LDAP	The Lightweight Directory Access Protocol is an application protocol for reading and editing directories over an IP network.
LLDP (Link Layer Discovery Protocol)	A vendor neutral link layer protocol used by network devices to advertise their identify, capabilities and for neighbor discovery
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.

**Table 2 - Glossary**

RDMA (Remote Direct Memory Access)	Accessing memory in a remote side without involvement of the remote CPU
RSTP	Rapid Spanning Tree Protocol. A spanning-tree protocol used to prevent loops in bridge configurations. RSTP is not aware of VLANs and blocks ports at the physical level.
SA (Subnet Administrator)	The interface for querying and manipulating subnet management data
SCP	Secure Copy or SCP is a means of securely transferring computer files between a local and a remote host or between two remote hosts. It is based on the Secure Shell (SSH) protocol.
SNMP	Simple Network Management Protocol. A network protocol for the management of a network and the monitoring of network devices and their functions
NTP	Network Time Protocol. A protocol for synchronizing computer clocks in a network
SSH	Secure Shell. A protocol (program) for securely logging in to and running programs on remote machines across a network. The program authenticates access to the remote machine and encrypts the transferred information through the connection.
syslog	A standard for forwarding log messages in an IP network
TACACS+	Terminal Access Controller Access-Control System Plus. A networking protocol that enables access to a network of devices via one or more centralized servers. TACACS+ provides separate AAA services.
XML Gateway	Extensible Markup Language Gateway. Provides an XML request-response protocol for setting and retrieving HW management information.

# 1 Introduction

Mellanox® Operating System (MLNX-OS®) enables the management and configuration of Mellanox Technologies' switch system platforms.

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

## 1.1 System Features

*Table 3 - General System Features*

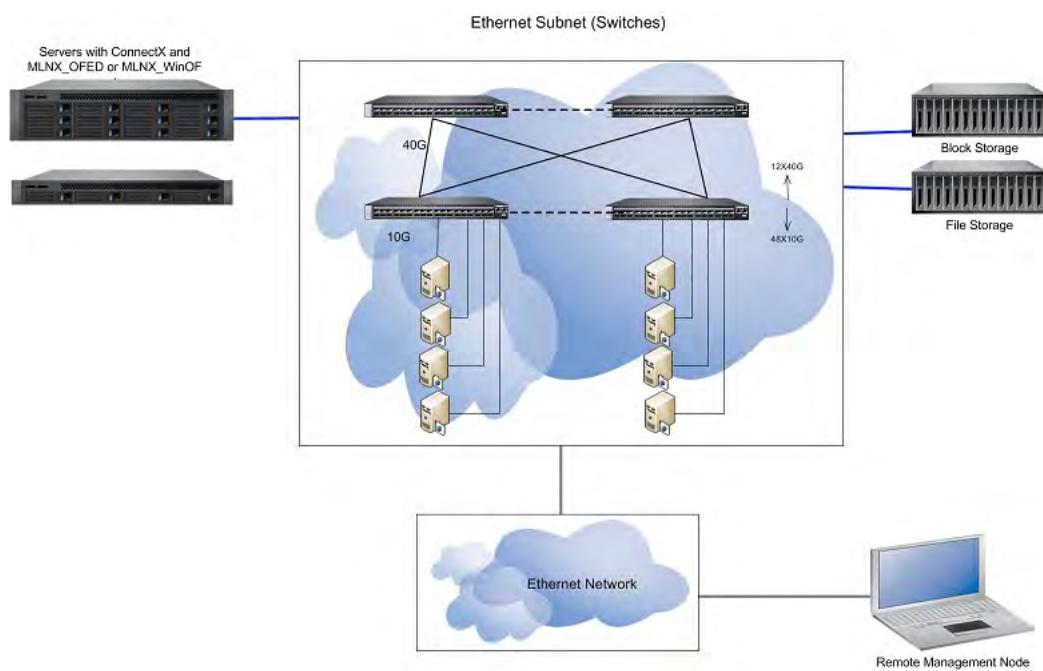
Feature	Description
Software Management	<ul style="list-style-type: none"><li>Dual software image</li><li>Software and firmware updates</li></ul>
File management	<ul style="list-style-type: none"><li>FTP</li><li>TFTP</li><li>SCP</li></ul>
Logging	<ul style="list-style-type: none"><li>Event history log</li><li>SysLog support</li></ul>
Management Interface	<ul style="list-style-type: none"><li>DHCP/Zeroconf</li><li>IPv6</li></ul>
Chassis Management	<ul style="list-style-type: none"><li>Monitoring environmental controls</li><li>Power management</li><li>Auto-temperature control</li><li>High availability</li></ul>
Network Management Interfaces	<ul style="list-style-type: none"><li>SNMP v1,v2c,v3</li><li>interfaces (XML Gateway)</li><li>Puppet Agent</li></ul>
Security	<ul style="list-style-type: none"><li>SSH</li><li>Telnet</li><li>RADIUS</li><li>TACACS+</li></ul>
Date and Time	<ul style="list-style-type: none"><li>NTP</li></ul>
Cables & Transceivers	<ul style="list-style-type: none"><li>Transceiver info</li></ul>
Unbreakable links	<ul style="list-style-type: none"><li>LLR</li></ul>

## 1.2 Ethernet Features

**Table 4 - Ethernet Features**

Feature	Description
General	<ul style="list-style-type: none"> <li>• ACL – 6400 rules (permit/deny)</li> <li>• Breakout cables</li> <li>• Jumbo Frames (9K)</li> </ul>
Ethernet support	<ul style="list-style-type: none"> <li>• 48K unicast MAC addresses on SwitchX®-2 based systems <ul style="list-style-type: none"> <li>• 2K static multicast MAC addresses</li> </ul> </li> <li>• 90100 unicast MAC addresses on Spectrum™ based systems</li> <li>• DCBX</li> <li>• DHCP Relay</li> <li>• ETS (802.1Qaz)</li> <li>• Flow control (802.3x)</li> <li>• IGMP snooping v1,2</li> <li>• LAG/LACP (802.3ad), 16 links per LAG (64 LAGs)</li> <li>• LLDP</li> <li>• MLAG</li> <li>• MSTP</li> <li>• OpenFlow 1.3</li> <li>• PFC (802.1Qbb)</li> <li>• Rapid Spanning Tree (802.1w)</li> <li>• sFlow</li> <li>• VLAN (802.1Q) – 4K</li> </ul>
IP routing	<ul style="list-style-type: none"> <li>• BGP</li> <li>• DHCP Relay</li> <li>• ECMP</li> <li>• IGMP</li> <li>• IPv4</li> <li>• IPv6</li> <li>• OSPF</li> <li>• PIM</li> <li>• VLAN interface</li> <li>• Loopback interface</li> <li>• Router interface</li> <li>• VRRP</li> </ul>

**Figure 1: Managing an Ethernet Fabric Using MLNX-OS®**



## 2 Getting Started

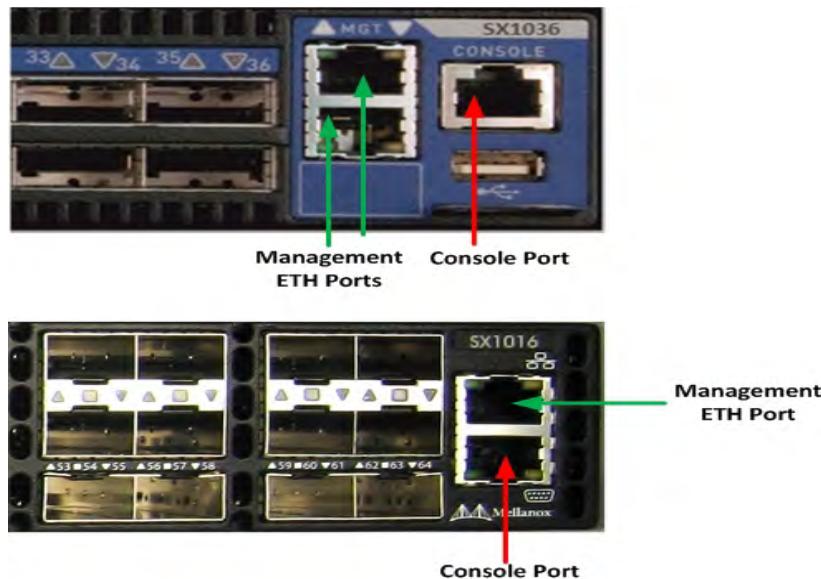
The procedures described in this chapter assume that you have already installed and powered on your switch according to the instructions in the *Hardware Installation Guide*, which was shipped with the product.

### 2.1 Configuring the Switch for the First Time

➤ *To configure the switch:*

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

**Figure 2: Console Ports SX10xx 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 for PPC Based Systems**

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

**Table 6 - Serial Terminal Program Configuration for x86 Based Systems**

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

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

- Step 5.** Go through the Mellanox configuration wizard.

The following table shows an example of a wizard session.

**Table 7 - 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>.
<b>Step1:</b> Hostname? [switch-1]	If you wish to accept the default hostname, then press <Enter>. Otherwise, type a different hostname and press <Enter>.
<b>Step 2:</b> Use DHCP on mgmt0 interface? [yes]  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 8.  If you enter “no” (no Zeroconf), then you need to enter a <i>static</i> IP, and the session will continue as shown in Table 9.	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 8.  If you enter “no” (no Zeroconf), then you need to enter a <i>static</i> IP, and the session will continue as shown in Table 9.
<b>Step 3:</b> Enable IPv6 [yes]  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.	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.
<b>Step 4:</b> Enable IPv6 autoconfig (SLAAC) on mgmt0 interface  If you wish to enable it, type “yes” and press <Enter>.  If you wish to disable it, enter “no”.	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”.
<b>Step 5:</b> Use DHCPv6 on mgmt0 interface? [yes]	Perform this step to enable DHCPv6 on the MGMT0 interface.
<b>Step 5:</b> Admin password (Press <Enter> to leave unchanged)? <new_password> <b>Step 4:</b> 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 <i>not</i> printed.

**Table 7 - Configuration Wizard Session - IP Configuration by DHCP (Sheet 2 of 2)**

Wizard Session Display (Example)	Comments
<p>You have entered the following information:</p> <ul style="list-style-type: none"> <li>1. Hostname: &lt;switch name&gt;</li> <li>2. Use DHCP on mgmt0 interface: yes</li> <li>3. Enable IPv6: yes</li> <li>4. Enable IPv6 autoconfig (SLAAC) on mgmt0 interface: yes</li> <li>5. Enable DHCPv6 on mgmt0 interface: no</li> <li>6. Admin password (Enter to leave unchanged): (CHANGED)</li> </ul> <p>To change an answer, enter the step number to return to. Otherwise hit &lt;enter&gt; to save changes and exit.</p> <p>Choice: &lt;Enter&gt;</p> <p>Configuration changes saved. To return to the wizard from the CLI, enter the “configuration jump-start” command from configuration mode. Launching CLI...</p> <p>&lt;switch name&gt; [standalone: master] &gt;</p>	<p>The wizard displays a summary of your choices and then asks you to confirm the choices or to re-edit them.</p> <p>Either press &lt;Enter&gt; to save changes and exit, or enter the configuration step number that you wish to return to.</p> <p><b>Note:</b> To run the command “configuration jump-start” you must be in Config mode.</p>

**Table 8 - Configuration Wizard Session - IP Zeroconf Configuration**

Wizard Session Display - IP Zeroconf Configuration (Example)
<p>Mellanox configuration wizard</p> <p>Do you want to use the wizard for initial configuration? y</p> <p>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)?</p> <p>You have entered the following information:</p> <ol style="list-style-type: none"> <li>1. Hostname: switch-112126</li> <li>2. Use DHCP on mgmt0 interface: no</li> <li>3. Use zeroconf on mgmt0 interface: yes</li> <li>4. Default gateway: 192.168.10.1</li> <li>5. Primary DNS server:</li> <li>6. Domain name:</li> <li>7. Enable IPv6: yes</li> <li>8. Enable IPv6 autoconfig (SLAAC) on mgmt0 interface: yes</li> <li>9. Admin password (Enter to leave unchanged): (unchanged)</li> </ol> <p>To change an answer, enter the step number to return to.  Otherwise hit &lt;enter&gt; to save changes and exit.</p> <p>Choice:</p> <p>Configuration changes saved.</p> <p>To return to the wizard from the CLI, enter the “configuration jump-start” command from configure mode. Launching CLI...</p> <p>&lt;switch name&gt; [standalone: master] &gt;</p>

**Table 9 - Configuration Wizard Session - Static IP Configuration**

Wizard Session Display - Static IP Configuration (Example)
<p>Mellanox configuration wizard</p> <p>Do you want to use the wizard for initial configuration? y</p> <p>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)</p> <p>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)?</p> <p>You have entered the following information:</p> <ol style="list-style-type: none"> <li>1. Hostname: switch-112126</li> <li>2. Use DHCP on mgmt0 interface: no</li> <li>3. Use zeroconf on mgmt0 interface: no</li> <li>4. Primary IP address: 192.168.10.4</li> <li>5. Netmask: 255.255.255.0</li> <li>6. Default gateway: 192.168.10.1</li> <li>7. Primary DNS server:</li> <li>8. Domain name:</li> <li>9. Enable IPv6: yes</li> <li>10. Enable IPv6 autoconfig (SLAAC) on mgmt0 interface: no</li> <li>11. Admin password (Enter to leave unchanged): (unchanged)</li> </ol> <p>To change an answer, enter the step number to return to.  Otherwise hit &lt;enter&gt; to save changes and exit.</p> <p>Choice:</p> <p>Configuration changes saved.</p> <p>To return to the wizard from the CLI, enter the “configuration jump-start” command from configure mode. Launching CLI...</p> <p>&lt;switch name&gt;[standalone: master] &gt;</p>

- 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
    Secondary address: 10.10.10.254/24 (alias: 'mgmt0:0')
    IPv6 enabled:      yes
    Autoconf enabled: no
    Autoconf route:   yes
    Autoconf privacy: no
    DHCPv6 running:   no
    IPv6 addresses:   1
    IPv6 address:     fe80::202:c9ff:fe11:a1b2/64
    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:
    15139846        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 53.

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

**Step 4.** Read and accept the EULA when prompted.

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

```
Mellanox MLNX-OS Switch Management  
  
Password:  
Last login: <time> from <ip-address>  
  
Mellanox Switch  
Please read and accept the Mellanox End User License Agreement located at:  
http://www.mellanox.com/related-docs/prod\_management\_software/MLNX-OS\_EULA.pdf  
  
switch >
```

## 2.3 Starting the Web User Interface (WebUI)

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

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

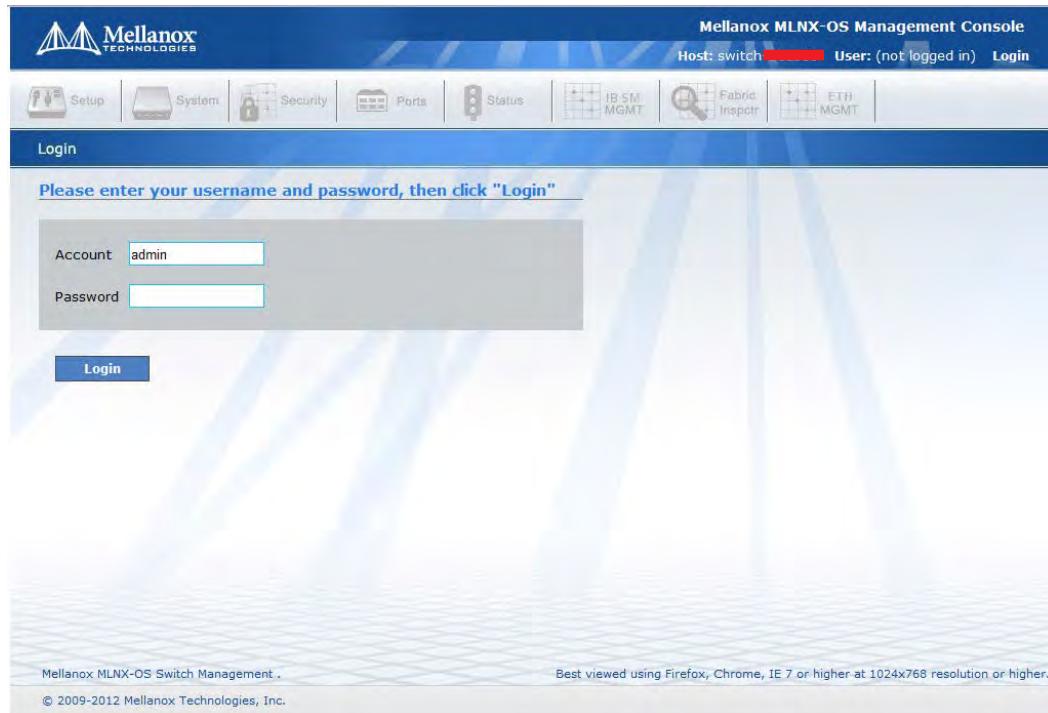
**Step 2.** Open a web browser – Firefox 12, Chrome 18, IE 8, Safari 5 or higher.

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

**Step 3.** Type in the IP address of the switch or its DNS name in the format: http://<switch\_IP\_address>.

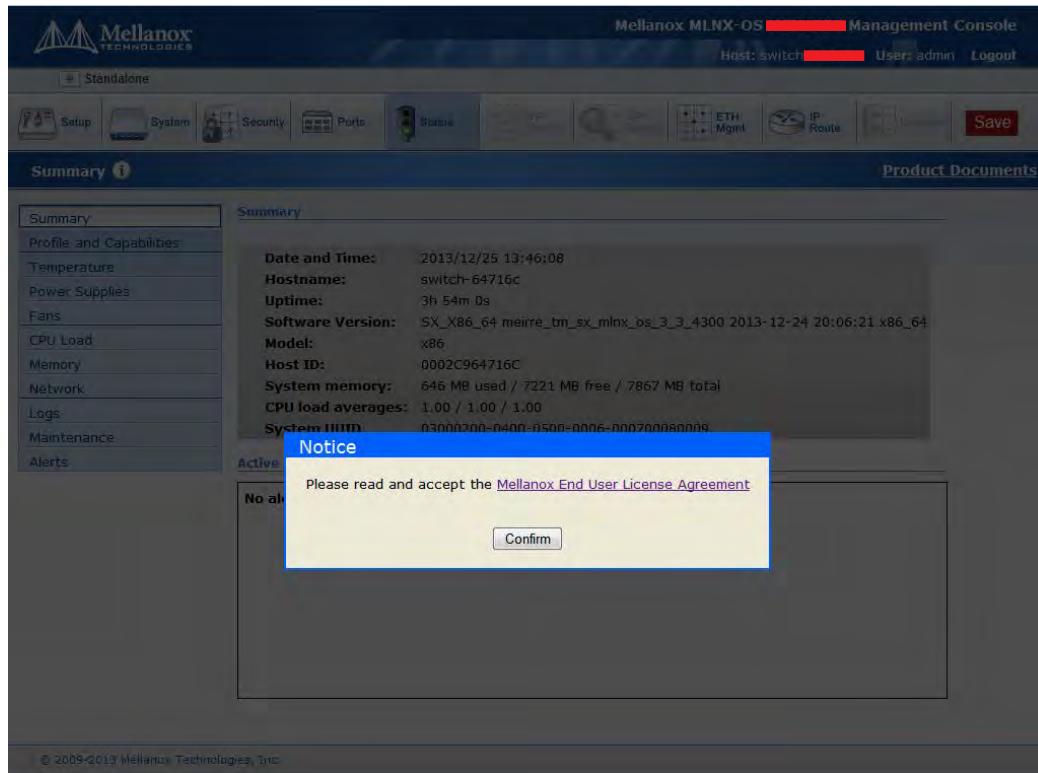
**Step 4.** Login to the switch (default user name is *admin*, password *admin*).

**Figure 3: MLNX-OS Login Window**



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

**Figure 4: EULA Prompt**



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

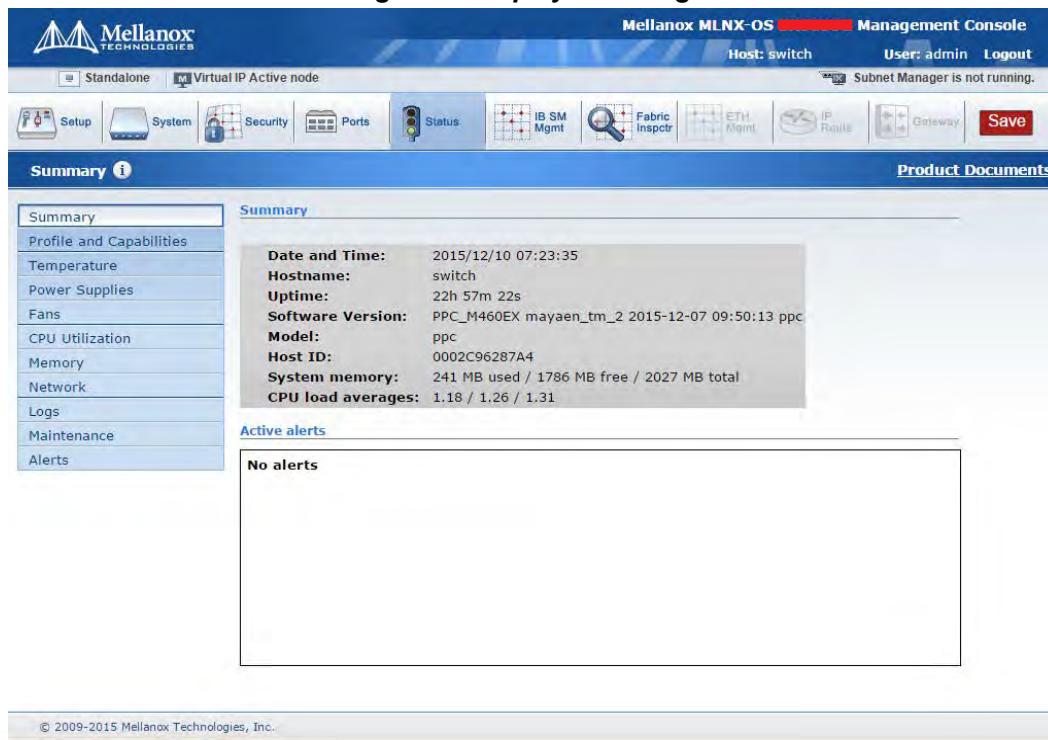
**Figure 5: Welcome Popup**



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

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

**Figure 6: Display After Login**



## 2.4 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. If docker image file URL is not specified, or the switch is not a standalone x86 box, skip this step. 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.

<b>Syntax Description</b>	N/A
<b>Default</b>	Enabled
<b>Configuration Mode</b>	Config
<b>History</b>	3.6.5000
<b>Role</b>	admin
<b>Example</b>	<pre>switch (config) # no zero-touch suppress-write</pre>
<b>Related Commands</b>	<a href="#">show zero-touch</a>
<b>Notes</b>	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.

<b>Syntax Description</b>	N/A
<b>Default</b>	Enabled
<b>Configuration Mode</b>	Config
<b>History</b>	3.6.5000
<b>Role</b>	admin
<b>Example</b>	<pre>switch (config) # zero-touch abort Zero-touch failed [Zero-touch is aborted by operator] Zero-touch provisioning will be aborted</pre>
<b>Related Commands</b>	show zero-touch
<b>Notes</b>	

## show zero-touch

### show zero-touch

Displays zero-touch status.

<b>Syntax Description</b>	N/A
<b>Default</b>	N/A
<b>Configuration Mode</b>	Any Command Mode
<b>History</b>	3.6.5000
<b>Role</b>	admin
<b>Example</b>	<pre>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</pre>
<b>Related Commands</b>	<a href="#">zero-touch abort</a> <a href="#">zero-touch suppress-write</a>
<b>Notes</b>	

## 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.** Login as *admin* and change to *Config* mode.

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

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

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

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

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

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

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

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



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

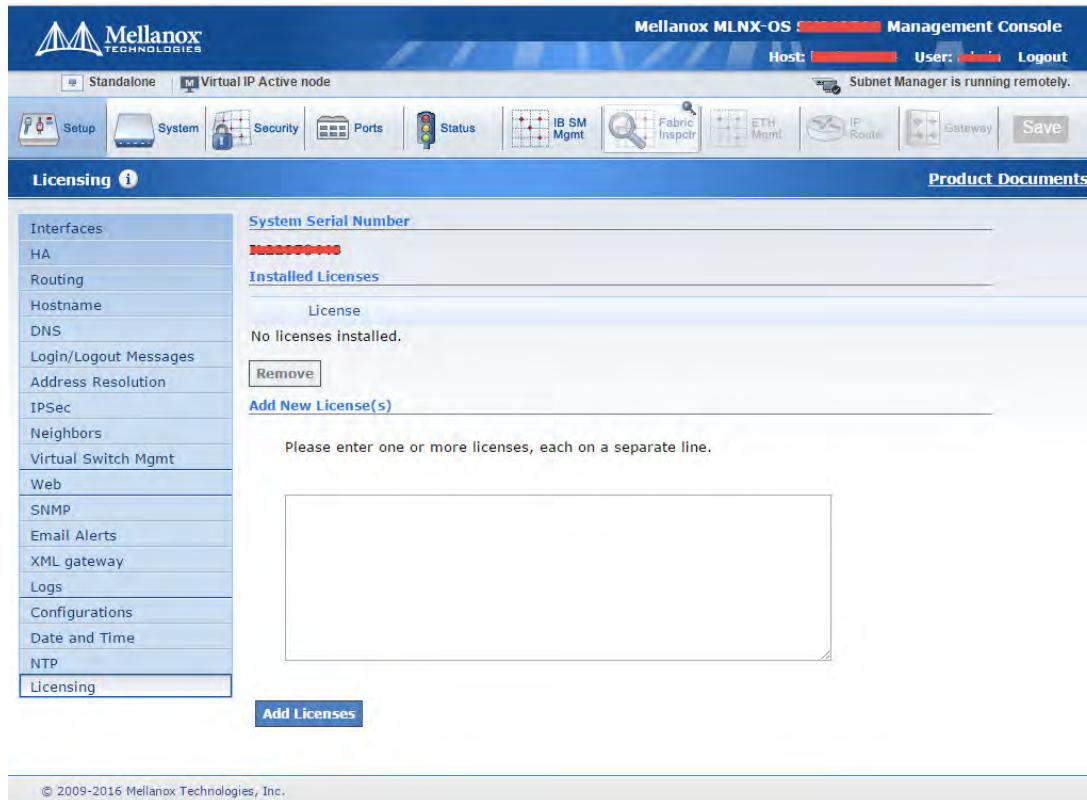
### 2.5.2 Installing MLNX-OS License (Web)

- *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 7: No Licenses Installed**

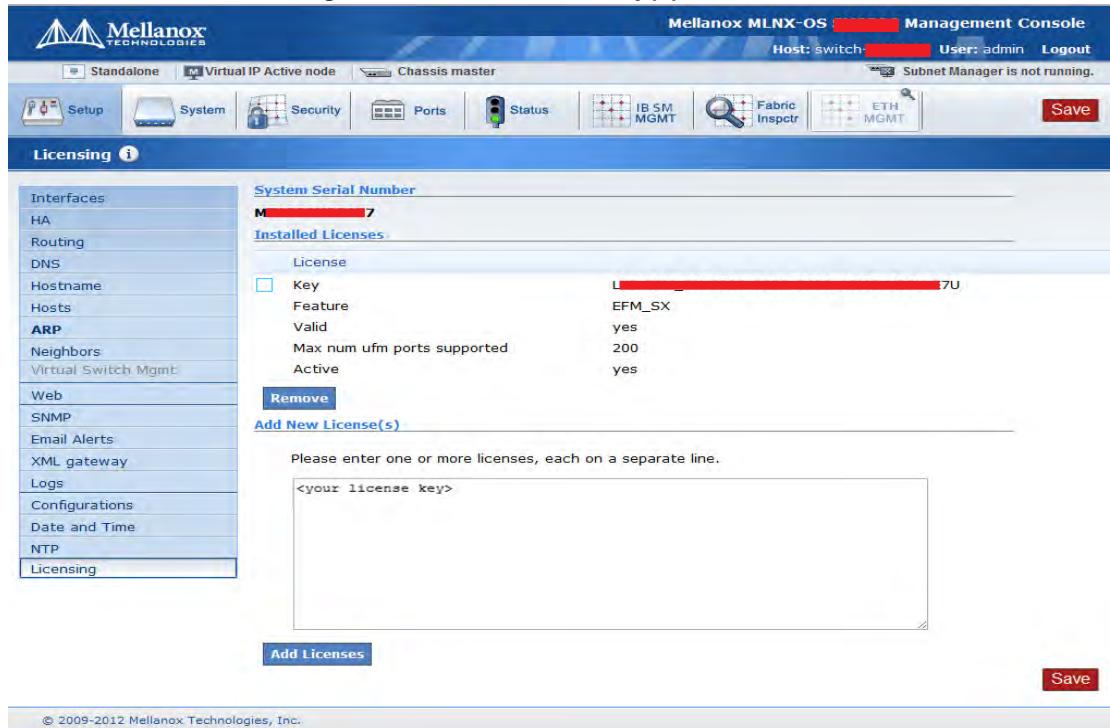


**Step 3.** Enter your license key(s) in the text box. If you have more than one license, please enter each license in a separate line. Click “Add Licenses” after entering the last license key to install them.



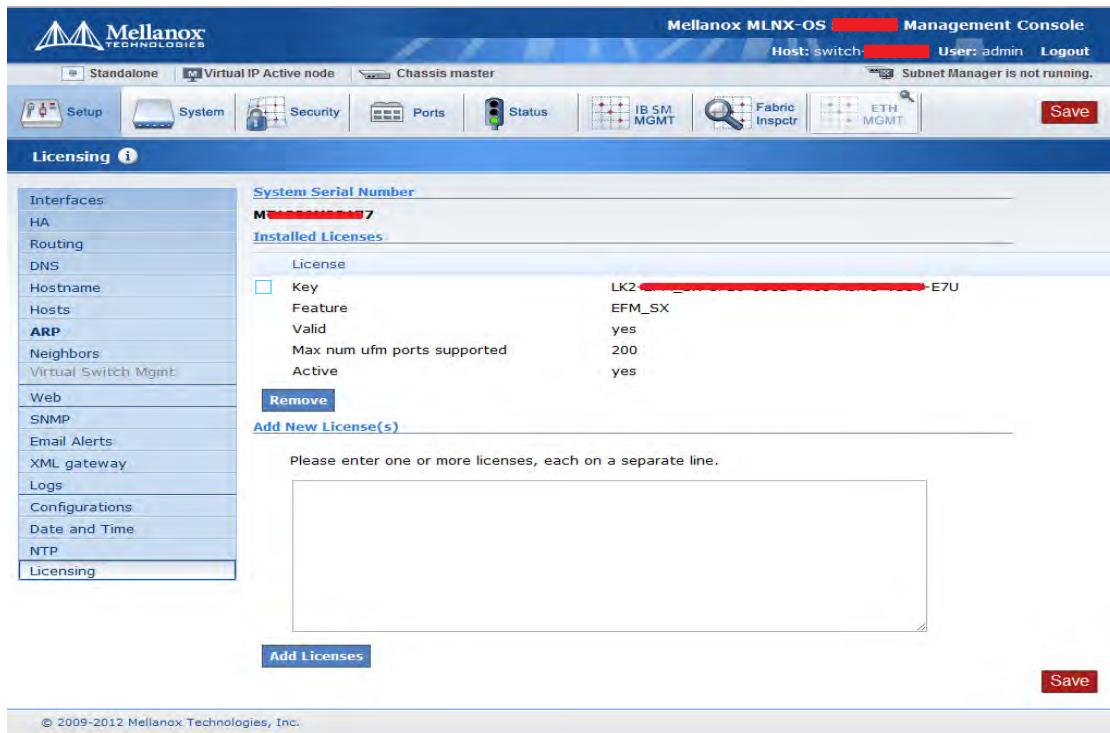
If you wish to add another license key in the future, you can simply enter it in the text box and click “Add Licenses” to install it.

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



All installed licenses should now be displayed.

**Figure 9: Installed License**



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



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

### 2.5.3 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        MSX1036B-1SFR    MT1205X01549    N/A         A1
MGMT           MSX1036B-1SFR    MT1205X01549    0          A1
FAN            MSX60-FF        MT1206X07209    N/A         A3
PS1             MSX60-PF       MT1206X06697    N/A         A2
switch (config) #
```

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

- The chassis serial number
- The type of license you need to retrieve. Refer to “Licenses” on page 60.

- 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.

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

## file help-docs upload

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

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

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

## license delete

**license delete <license-number>**

Removes license keys by ID.

<b>Syntax Description</b>	N/A
<b>Default</b>	N/A
<b>Configuration Mode</b>	Config
<b>History</b>	3.4.1100
<b>Role</b>	admin
<b>Example</b>	<pre>switch (config) # license delete &lt;license-key&gt; switch (config) #</pre>
<b>Related Commands</b>	
<b>Note</b>	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.

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

## 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

<b>Syntax Description</b>	N/A
<b>Default</b>	N/A
<b>Configuration Mode</b>	Config
<b>History</b>	3.4.1100
<b>Role</b>	admin
<b>Example</b>	<pre>switch (config) # show licenses License 1: &lt;license key&gt; Feature: SX_CONFIG Valid: yes Active: yes switch (config) #</pre>
<b>Related Commands</b>	
<b>Note</b>	

## 3 User Interfaces

### 3.1 LED Indicators

**Table 10 - 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

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 11 - 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 11 - 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.
Config Interface Ethernet	Configuration mode for Ethernet interface.
Config Interface Port Channel	Configuration mode for Port channel (LAG).
Config VLAN	Configuration mode for VLAN.
Any Command Mode	Several commands such as “show” can be applied within any context.

### 3.2.2 Syntax Conventions

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

**Table 12 - Syntax Conventions**

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



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



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

### 3.2.3 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 13 - Angled Brackets Parameter Description**

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



This feature is available on x86 based systems only.

The MLNX-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 519](#).

For a list of commands supporting the JSON API, please refer to [Appendix B, “Show Commands Supported by JSON API,” on page 1424](#).

### 3.2.8 CLI Shortcuts

[Table 14](#) presents the available keyboard shortcuts on the MLNX-OS® CLI.

**Table 14 - 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

**Table 14 - CLI Keyboard Shortcuts**

Key Combination	Description
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

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

The following web browsers are supported:

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

The web interface makes available the following perspective tabs:

- Setup
- System
- Security
- Ports
- Status
- Fabric Inspector
- Ethernet Management
- Setup-JSON API
- Port-telemetry
- IP Route
- Gateway



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

**Figure 10: WebUI**



### 3.3.1 Setup Menu

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

**Table 15 - 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.
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
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

**Table 15 - WebUI Setup Submenus**

Submenu Title	Description
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
Logging	Sets up system log files, remote log sinks, and log formats
Configurations	Manages, activates, saves, and imports MLNX-OS® SwitchX® configuration files, and executes CLI commands
Date and Time	Configures the date, time, and time zone of the switch system
NTP	Configures NTP (Network Time Protocol) and NTP servers
Licensing	Manages MLNX-OS licenses

### 3.3.2 System Menu

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

**Table 16 - WebUI System Submenus**

Submenu Title	Description
Modules	Displays a graphic illustration of the system modules. By moving the mouse over the ports in the front view, a pop-up caption is displayed to indicate the status of the port. The port state (active/down) is differentiated by a color scheme (green for active, gray/black for down). By moving the mouse over the rear view, a pop-up caption is displayed to indicate the leaf part information.
Inventory	Displays a table with the following information about the system modules: module name, type, serial number, ordering part number and ASIC firmware version
Power Management	Displays a table with the following information about the system power supplies: power supply name, power, voltage level, current consumption, and status. A total power summary table is also displayed providing the power used, the power capacity, and the power available.
MLNX-OS Upgrade	Displays the installed MLNX-OS® images (and the active partition), uploads a new image, and installs a new image
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 17 - 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 18 - WebUI Ports Submenus**

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

### 3.3.5 Status Menu

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

**Table 19 - 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

**Table 19 - WebUI Status Submenus**

Submenu Title	Description
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 ETH Mgmt



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

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

**Table 20 - WebUI ETH Mgmt Submenus**

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

### 3.3.7 IP Route

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

**Table 21 - WebUI IP Route Submenus**

Submenu Title	Description
Router Global	Enables/disables IP routing protocol
IP Route	Configures, removes, and displays the routing table for router interfaces
IP Interface	Displays router interfaces
Address Resolution	Not implemented
IP Diagnostic	Not implemented

## 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/05ryIc="
switch [standalone: master] (config) #
```

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

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

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

No SSH user identities configured.

No SSH authorized keys configured.

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

### 3.4.2 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 11: Index Scheme*

Mod. Type	2-Digit Module Index	Device Name	Device Index #1	Device Index #2	Sensor Type	Sensor Index
--------------	-------------------------	-------------	-----------------------	-----------------------	----------------	-----------------

1    2    3    4    5    6    7    8    9

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.

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

## 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.

<b>Syntax Description</b>	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. <ul style="list-style-type: none"> <li>“prefix-modes enable” enables prefix modes for current and all future sessions</li> <li>“prefix-modes show-config” uses prefix modes in “show configuration” output for current and all future sessions</li> </ul>
	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.
<b>Default</b>	N/A	
<b>Configuration Mode</b>	Config	
<b>History</b>	3.1.0000	
<b>Role</b>	admin	

---

**Example**

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

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

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

---

**Related Commands**    [show cli](#)

---

**Note**

## cli 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.

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

## 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.

<b>Syntax Description</b>	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. <ul style="list-style-type: none"> <li>“prefix-modes enable” enables prefix modes for current and all future sessions</li> <li>“prefix-modes show-config” uses prefix modes in “show configuration” output for current and all future sessions</li> </ul>
	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: <ul style="list-style-type: none"> <li>ansi</li> <li>console</li> <li>dumb</li> <li>linux</li> <li>unknown</li> <li>vt52</li> <li>vt100</li> <li>vt102</li> <li>vt220</li> <li>vt320</li> <li>xterm</li> </ul>
	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.
<b>Default</b>	N/A	

<b>Configuration Mode</b>	Config
<b>History</b>	3.1.0000
<b>Role</b>	admin
<b>Example</b>	<pre>switch (config) # cli session auto-logout switch (config) #</pre>
<b>Related Commands</b>	show terminal
<b>Note</b>	

## 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.

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

## 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).

<b>Syntax Description</b>	N/A
<b>Default</b>	Enabled
<b>Configuration Mode</b>	Config
<b>History</b>	3.4.3000
<b>Role</b>	admin
<b>Example</b>	<pre>switch (config) # terminal sysrq enable switch (config) #</pre>
<b>Related Commands</b>	show terminal
<b>Note</b>	

## show cli

### show cli

Displays the CLI configuration and status.

<b>Syntax Description</b>	N/A
<b>Default</b>	N/A
<b>Configuration Mode</b>	Any Command Mode
<b>History</b>	3.1.0000
<b>Role</b>	admin
<b>Example</b>	<pre>switch (config) # show cli CLI current session settings:     Maximum line size:          8192     Terminal width:             171 columns     Terminal length:            38 rows     Terminal type:              xterm     X display setting:          (none)     Auto-logout:                disabled     Paging:                     enabled     Progress tracking:          enabled     Prefix modes:               disabled  CLI defaults for future sessions:     Auto-logout:                disabled     Paging:                      enabled     Progress tracking:           enabled     Prefix modes:                enabled (and use in 'show configuration')  Settings for both this session and future ones:     Show hidden config:          yes     Confirm losing changes:       yes     Confirm reboot/shutdown:     no     Confirm factory reset:       yes     Prompt on empty password:    yes switch (config) #</pre>
<b>Related Commands</b>	cli default
<b>Note</b>	

## show cli max-sessions

### show cli max-sessions

Displays maximum number of sessions.

<b>Syntax Description</b>	N/A
<b>Default</b>	N/A
<b>Configuration Mode</b>	Any Command Mode
<b>History</b>	3.5.0200
<b>Role</b>	admin
<b>Example</b>	<pre>switch (config) # show cli max-sessions Maximum number of CLI sessions: 5 switch (config) #</pre>
<b>Related Commands</b>	
<b>Note</b>	

## 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.

<b>Syntax Description</b>	string	Text string.
<b>Default</b>	“Mellanox MLNX-OS Switch Management”	
<b>Configuration Mode</b>	Config	
<b>History</b>	3.1.0000	
<b>Role</b>	admin	
<b>Example</b>	switch (config) # banner login Example switch (config) #	
<b>Related Commands</b>	show banner	
<b>Note</b>	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.

<b>Syntax Description</b>	string	Text string.
<b>Default</b>	N/A	
<b>Configuration Mode</b>	Config	
<b>History</b>	3.1.0000	
	3.5.0200	Added no form of the command
<b>Role</b>	admin	
<b>Example</b>	<pre>switch (config) # banner login-local Testing switch (config) #</pre>	
<b>Related Commands</b>	show banner	
<b>Note</b>	<ul style="list-style-type: none"><li>The login-local refers to the serial connection banner</li><li>If more than one word is used (there is a space) quotation marks should be added (i.e. “xxxx xxxx”).</li></ul>	

## **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.

<b>Syntax Description</b>	string	Text string.
<b>Default</b>	N/A	
<b>Configuration Mode</b>	Config	
<b>History</b>	3.1.0000	
	3.5.0200	Added no form of the command
<b>Role</b>	admin	
<b>Example</b>	<pre>switch (config) # banner login-remote Testing switch (config) #</pre>	
<b>Related Commands</b>	show banner	
<b>Note</b>	<ul style="list-style-type: none"><li>The login-remote refers to the SSH connections banner</li><li>If more than one word is used (there is a space) quotation marks should be added (i.e. “xxxx xxxx”).</li></ul>	

## 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.

<b>Syntax Description</b>	string	Text string.
<b>Default</b>	N/A	
<b>Configuration Mode</b>	Config	
<b>History</b>	3.5.0200	
<b>Role</b>	admin	
<b>Example</b>	switch (config) # banner logout Testing switch (config) #	
<b>Related Commands</b>	show banner	
<b>Note</b>	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.

<b>Syntax Description</b>	string	Text string.
<b>Default</b>	N/A	
<b>Configuration Mode</b>	Config	
<b>History</b>	3.5.0200	
<b>Role</b>	admin	
<b>Example</b>	switch (config) # banner logout-local Testing switch (config) #	
<b>Related Commands</b>	show banner	
<b>Note</b>	<ul style="list-style-type: none"><li>The logout-local refers to the serial connection banner</li><li>If more than one word is used (there is a space) quotation marks should be added (i.e. “xxxx xxxx”).</li></ul>	

## 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.

<b>Syntax Description</b>	string	Text string.
<b>Default</b>	N/A	
<b>Configuration Mode</b>	Config	
<b>History</b>	3.5.0200	
<b>Role</b>	admin	
<b>Example</b>	<pre>switch (config) # banner logout-remote Testing switch (config) #</pre>	
<b>Related Commands</b>	show banner	
<b>Note</b>	<ul style="list-style-type: none"><li>The logout-remote refers to SSH connections banner</li><li>If more than one word is used (there is a space) quotation marks should be added (i.e. “xxxx xxxx”).</li></ul>	

## 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.

<b>Syntax Description</b>	string	Text string
<b>Default</b>	“Mellanox Switch”	
<b>Configuration Mode</b>	Config	
<b>History</b>	3.1.0000	
<b>Role</b>	admin	
<b>Example</b>	switch (config) # banner motd "My Banner"	
<b>Related Commands</b>	show banner	
<b>Note</b>	<ul style="list-style-type: none"><li>• If more than one word is used (there is a space) quotation marks should be added (i.e. “xxxx xxxx”).</li><li>• 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.</li></ul>	

## show banner

### show banner

Displays configured banners.

<b>Syntax Description</b>	N/A
<b>Default</b>	N/A
<b>Configuration Mode</b>	Config
<b>History</b>	3.1.0000
	3.5.0200 Updated Example
<b>Role</b>	Any Command Mode
<b>Example</b>	<pre>switch (config) # show banner Banners:     Message of the Day (MOTD):     Mellanox Switch      Login:     Mellanox MLNX-OS Switch Management      Logout:     Goodbye switch (config) #</pre>
<b>Related Commands</b>	<a href="#">banner login</a> <a href="#">banner login-local</a> <a href="#">banner login-remote</a> <a href="#">banner logout</a> <a href="#">banner logout-local</a> <a href="#">banner logout-remote</a> <a href="#">banner motd</a>
<b>Note</b>	

### 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.

<b>Syntax Description</b>	N/A
<b>Default</b>	SSH server is enabled
<b>Configuration Mode</b>	Config
<b>History</b>	3.1.0000
<b>Role</b>	admin
<b>Example</b>	<pre>switch (config) # ssh server enable switch (config) # show ssh server SSH server configuration:     SSH server enabled:          yes     Server security strict mode: no     Minimum protocol version:   2     TCP forwarding enabled:     yes     X11 forwarding enabled:    no     SSH server ports:           22      Interface listen enabled:    yes     No Listen Interfaces.  Host Key Finger Prints:     RSA v1 host key: SHA256:ElFoK7Jts7ejiws0Jgs3yt46go0Ckln0JzNzAGx0ue4 (2048)     RSA v2 host key: SHA256:N4n+Un/lErjtzmmDJH+qcdsmHgHc0itlYArFgqP+UFI (2048)     DSA v2 host key: SHA256:2rIuzmPD90AWooQaEji1SH5EF0DjQ9DDSTaAMrzDFCY (1024) switch (config) #</pre>
<b>Related Commands</b>	show ssh server
<b>Note</b>	Disabling SSH server does not terminate existing SSH sessions, it only prevents new ones from being established.

## ssh server host-key

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

Manipulates host keys for SSH.

<b>Syntax Description</b>	key-type	<ul style="list-style-type: none"><li>rsa1 - RSAv1</li><li>rsa2 - RSAv2</li><li>dsa2 - DSAv2</li></ul>
	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.
<b>Default</b>	SSH keys are locally generated	
<b>Configuration Mode</b>	Config	
<b>History</b>	3.1.0000	
	3.4.2300	Added notes
<b>Role</b>	admin	

**Example**

```

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

    Interface listen enabled: yes
    No Listen Interfaces.

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

    Host Keys:
        RSA v1 host key: "switch-5ea5d8 1024 35
12457497995374010105491416867919987976776882016984375942831915584962796
99375406596085804272210942450456598705866658144854493132172365068789517
13570509420864336951833046700451354269467758379288848962624165330724512
1609189998303869157103621938557797859628221464453344813712105628654158
302298222056029771297093"
        RSA v2 host key: "switch-5ea5d8 ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAA-
IEArB9i5OnukAHNUOkwpCmEl0m88kJgBzL22+F5tfaSn+S0pVYxrceZeyuzXsoZ1VtFTk2-
Fydwy0YvMS0Kcv2PuCrPZV/
GYd3lQEnn22rEmrlPrKCrM11XlUy6DF1r3OgwWmlbaobmD1G/gSzIWz/gc4Jgqf2CyX-
Fq4pzar1jar1Vk="
        DSA v2 host key: "switch-5ea5d8 ssh-dss AAAAB3NzaC1kc3MAAAC-
BAMeJ3S+nyaHhRbwv3tJqlWttDC35RZVC5iG4ZEvMMHp28VL940cyyuGh39VCdM9pEVaI7h
zZrsgHrNqakb/YLD/7anGH3wp19Fx81fe0RH3bloJzG+mJ6R5momdoPCrKwEKiKABKE00-
jLz1VznpP0IHxjwF+TbR3dK5HwVzQYw/bAAAAFQCB0DPqBZza+2Ky1KlzUsbZ2pKhgQAAA-
IAJK+StiQdtORwlB5UCMzTrTef5L07DSfVreMEYtTRnBBtgVSNqQFWpSQIYbVDHQr9T6qCM
4VO39DuHUGQ1TMDIX7t+9mfB87YYUu5a/ndbf3GhNhxHWwbzlr9hgLL7FSHA7DYH7bvoZ-
R1qxH64eQKGZqy1ps/F4E31lyn7GC4EQAAAIA/2osHipXf+NRjp1gfHROVVf/mGE9Vzc9/
AMUx1JJn5VhvEJ5CZW9cI+LxMOJojhOj3YW3B1czGxRObDA9vUbKXTNc8bkgoUrxySAH1rh
NOPqJgeT4L009AItSp3mlmxHqdS7jixfTvOTEKWXrgpczlmTB8+zjhUah/YuuBl2H
g=="
switch (config) #

```

**Related Commands**

show ssh server  
system secure-mode enable

**Note**

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

## ssh server listen

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

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

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

<b>Syntax Description</b>	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”.
<b>Default</b>	SSH listen is enabled	
<b>Configuration Mode</b>	Config	
<b>History</b>	3.1.0000	
<b>Role</b>	admin	
<b>Example</b>	<pre>switch (config) # ssh server listen enable switch (config) # show ssh server SSH server configuration:     SSH server enabled:      yes     Minimum protocol version: 2     X11 forwarding enabled:   no     SSH server ports:        22      Interface listen enabled: yes     No Listen Interfaces.      Host Key Finger Prints:         RSA v1 host key: a0:63:db:96:e2:95:5a:5a:fd:a8:d0:f4:ab:e3:5f:f8         RSA v2 host key: 1e:b7:8b:ec:ab:35:98:be:6b:d6:12:c2:18:72:12:d6         DSA v2 host key: 7c:4a:f7:72:51:67:b5:0b:cd:a2:d2:b9:f3:be:3e:68 switch (config) #</pre>	
<b>Related Commands</b>	show ssh server	
<b>Note</b>		

## 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.

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

## 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.

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

## 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.

<b>Syntax Description</b>	version	Possible versions are 1 and 2.
<b>Default</b>	2	
<b>Configuration Mode</b>	Config	
<b>History</b>	3.1.0000	
<b>Role</b>	admin	
<b>Example</b>	<pre>switch (config) # ssh server min-version 2 switch (config) # show ssh server SSH server configuration:     SSH server enabled:      yes     Minimum protocol version: 2     X11 forwarding enabled:   no     SSH server ports:        22      Interface listen enabled: yes     No Listen Interfaces.      Host Key Finger Prints:         RSA v1 host key: a0:63:db:96:e2:95:5a:5a:fd:a8:d0:f4:ab:e3:5f:f8         RSA v2 host key: 1e:b7:8b:ec:ab:35:98:be:6b:d6:12:c2:18:72:12:d6         DSA v2 host key: 7c:4a:f7:72:51:67:b5:0b:cd:a2:d2:b9:f3:be:3e:68 switch (config) #</pre>	
<b>Related Commands</b>	show ssh server	
<b>Note</b>		

## ssh server ports

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

Specifies which ports the SSH server listens on.

<b>Syntax Description</b>	port	Port number in [1...65535].
<b>Default</b>	22	
<b>Configuration Mode</b>	Config	
<b>History</b>	3.1.0000	
<b>Role</b>	admin	
<b>Example</b>	<pre>switch (config) # ssh server ports 22 switch (config) # show ssh server SSH server configuration:     SSH server enabled:      yes     Minimum protocol version: 2     X11 forwarding enabled:   no     SSH server ports:        22      Interface listen enabled: yes     No Listen Interfaces.      Host Key Finger Prints:         RSA v1 host key: a0:63:db:96:e2:95:5a:5a:fd:a8:d0:f4:ab:e3:5f:f8         RSA v2 host key: 1e:b7:8b:ec:ab:35:98:be:6b:d6:12:c2:18:72:12:d6         DSA v2 host key: 7c:4a:f7:72:51:67:b5:0b:cd:a2:d2:b9:f3:be:3e:68 switch (config) #</pre>	
<b>Related Commands</b>	show ssh server	
<b>Note</b>	<ul style="list-style-type: none"> <li>Multiple ports can be specified by repeating the &lt;port&gt; parameter</li> <li>The command will remove any previous ports if not listed in the command</li> </ul>	

## ssh server security strict

**ssh server security strict**

Enables strict security settings.

The no form of the command disables strict security settings.

<b>Syntax Description</b>	N/A
<b>Default</b>	N/A
<b>Configuration Mode</b>	Config
<b>History</b>	3.3.5060 3.6.4000
<b>Role</b>	admin
<b>Example</b>	<pre>switch (config) # ssh server security strict switch (config) #</pre>
<b>Related Commands</b>	<a href="#">show ssh server</a>
<b>Note</b>	<p>The following ciphers are disabled for SSH when strict security is enabled:</p> <ul style="list-style-type: none"><li>• aes256-cbc</li><li>• aes192-cbc</li><li>• aes128-cbc</li><li>• arcfour</li><li>• blowfish-cbc</li><li>• cast128-cbc</li><li>• rijndael-cbc@lysator.liu.se</li><li>• 3des-cbc</li></ul>

## ssh server tcp-forwarding enable

**ssh server tcp-forwarding enable**

Enables TCP port forwarding.

The no form of the command disables TCP port forwarding.

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

## 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.

<b>Syntax Description</b>	N/A
<b>Default</b>	X11-forwarding is disabled.
<b>Configuration Mode</b>	Config
<b>History</b>	3.1.0000
<b>Role</b>	admin
<b>Example</b>	<pre>switch (config) # ssh server x11-forwarding enable switch (config) # show ssh server SSH server configuration:     SSH server enabled:      yes     Minimum protocol version: 2     X11 forwarding enabled:   yes     SSH server ports:        22      Interface listen enabled: yes     No Listen Interfaces.      Host Key Finger Prints:         RSA v1 host key: a0:63:db:96:e2:95:5a:5a:fd:a8:d0:f4:ab:e3:5f:f8         RSA v2 host key: 1e:b7:8b:ec:ab:35:98:be:6b:d6:12:c2:18:72:12:d6         DSA v2 host key: 7c:4a:f7:72:51:67:b5:0b:cd:a2:d2:b9:f3:be:3e:68 switch (config) #</pre>
<b>Related Commands</b>	N/A
<b>Note</b>	

## 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.

<b>Syntax Description</b>	host-key-check <policy>	Sets SSH client configuration to control how host key checking is performed. This parameter may be set in 3 ways. <ul style="list-style-type: none"> <li>If set to “no” it always permits connection, and accepts any new or changed host keys without checking</li> <li>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</li> <li>If set to “yes” it only permits connection if a matching host key is already in the known hosts file</li> </ul>
	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>”.
<b>Default</b>	host-key-check - ask, no keys are configured by default	
<b>Configuration Mode</b>	Config	
<b>History</b>	3.1.0000	
<b>Role</b>	admin	
<b>Example</b>	<pre>switch (config) # ssh client global host-key-check no switch (config) # ssh client global known-host "72.30.2.2 ssh-rsa AAAAAB3NzaC1yc2EAAAIEArB9i5OnukAHNUOkwpCmEl0m88kJgB- zL22+F5tfaSn+S0pVYxrceZeyuzXsoZ1VtFTk2FydwY0YvMS0Kcv2PuCrPZV/ GYd31QEnn22rEmrlPrKCrM11XlUy6DFlr3OgwWmlbaobmDlG/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) #</pre>	

---

**Related Commands** show ssh client

---

**Note**

---

## ssh client user

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

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

<b>Syntax Description</b>	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.
<b>Default</b>	No keys are created by default	
<b>Configuration Mode</b>	Config	
<b>History</b>	3.1.0000	
<b>Role</b>	admin	
<b>Example</b>	<pre>switch (config) # ssh client user admin known-host 172.30.1.116 remove switch (config) #</pre>	
<b>Related Commands</b>	show ssh client	
<b>Note</b>	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.

<b>Syntax Description</b>	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@]hostname [command]
<b>Default</b>	N/A	
<b>Configuration Mode</b>	Config	
<b>History</b>	3.1.0000	
<b>Role</b>	monitor/admin	
<b>Example</b>	<pre>switch (config) # slogin 192.168.10.70 The authenticity of host '192.168.10.70 (192.168.10.70)' can't be established. RSA key fingerprint is 2e:ad:2d:23:45:4e:47:e0:2c:ae:8c:34:f0:la:88:cb. Are you sure you want to continue connecting (yes/no)? yes Warning: Permanently added '192.168.10.70' (RSA) to the list of known hosts.  Mellanox MLNX-OS Switch Management  Last login: Sat Feb 28 22:55:17 2009 from 10.208.0.121  Mellanox Switch  switch (config) #</pre>	
<b>Related Commands</b>	N/A	
<b>Note</b>		

## show ssh client

### show ssh client

Displays the client configuration of the SSH server.

<b>Syntax Description</b>	N/A
<b>Default</b>	N/A
<b>Configuration Mode</b>	Config
<b>History</b>	3.1.0000
<b>Role</b>	admin
<b>Example</b>	<pre>switch (config) # show ssh client SSH client Strict Hostkey Checking: ask  SSH Global Known Hosts: Entry 1: 72.30.2.2 Finger Print: 1e:b7:8b:ec:ab:35:98:be:6b:d6:12:c2:18:72:12:d6  No SSH user identities configured.  No SSH authorized keys configured.  switch (config) #</pre>
<b>Related Commands</b>	N/A
<b>Note</b>	

## show ssh server

### show ssh server

Displays SSH server configuration.

<b>Syntax Description</b>	N/A
<b>Default</b>	N/A
<b>Configuration Mode</b>	Config
<b>History</b>	3.1.0000 3.4.0000                      Updated Example 3.5.0200                      Added SSH login timeout and max attempts
<b>Role</b>	admin
<b>Example</b>	<pre>switch (config) # show ssh server SSH server configuration:     SSH server enabled: yes     Server security strict mode: no     Minimum protocol version: 2     TCP forwarding enabled: yes     X11 forwarding enabled: no     SSH login timeout: 120     SSH login max attempts: 6     SSH server ports: 22      Interface listen enabled: yes     No Listen Interfaces.      Host Key Finger Prints and Key Lengths:         RSA v1 host key: 5f:4e:5f:4a:81:bb:6a:b4:06:52:77:eb:d3:ad:78:92 (2048)         RSA v2 host key: 15:e2:a8:45:1c:58:1b:00:cc:29:ec:00:38:83:49:00 (2048)         DSA v2 host key: df:c0:ac:a6:3e:a5:52:a5:d1:f6:22:37:ef:f1:08:f9 (1024)  switch (config) #</pre>
<b>Related Commands</b>	ssh server
<b>Note</b>	

### 3.6.4 Remote Login

#### telnet

**telnet**

Logs into another system using telnet.

<b>Syntax Description</b>	N/A
<b>Default</b>	N/A
<b>Configuration Mode</b>	Config
<b>History</b>	3.1.0000
<b>Role</b>	admin
<b>Example</b>	<pre>switch (config) # telnet telnet&gt;</pre>
<b>Related Commands</b>	telnet-server
<b>Note</b>	

## telnet-server enable

**telnet-server enable**  
**no telnet-server enable**

Enables the telnet server.

The no form of the command disables the telnet server.

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

## show telnet-server

### show telnet-server

Displays telnet server settings.

<b>Syntax Description</b>	N/A
<b>Default</b>	N/A
<b>Configuration Mode</b>	Config
<b>History</b>	3.1.0000
<b>Role</b>	admin
<b>Example</b>	<pre>switch (config) # show telnet-server Telnet server enabled: yes switch (config) #</pre>
<b>Related Commands</b>	<a href="#">telnet-server enable</a>
<b>Note</b>	

### 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 log out due to inactivity).

<b>Syntax Description</b>	number of minutes	The length of user inactivity in minutes. 0 will disable the inactivity timer (same as a “no web auto-logout” command).
<b>Default</b>	60 minutes	
<b>Configuration Mode</b>	Config	
<b>History</b>	3.1.0000	
	3.4.0000	Updated Example
<b>Role</b>	admin	
<b>Example</b>	<pre>switch (config) # web auto-logout 60 switch (config) # show web  Web User Interface:   Web interface enabled: yes   HTTP enabled: yes   HTTP port: 80   HTTP redirect to HTTPS: no   HTTPS enabled: yes   HTTPS port: 443   HTTPS ssl-ciphers: all   HTTPS certificate name: default-cert   Listen enabled: yes   No Listen Interfaces.    Inactivity timeout: 1 hr   Session timeout: 2 hr 30 min   Session renewal: 30 min    Web file transfer proxy:     Proxy enabled: no    Web file transfer certificate authority:     HTTPS server cert verify: yes     HTTPS supplemental CA list: default-ca-list switch (config) #</pre>	
<b>Related Commands</b>	show web	
<b>Note</b>	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.

<b>Syntax Description</b>	N/A
<b>Default</b>	Enabled
<b>Configuration Mode</b>	Config
<b>History</b>	3.4.1100
<b>Role</b>	admin
<b>Example</b>	switch (config) # no web cache-enable
<b>Related Commands</b>	N/A
<b>Note</b>	

## 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.

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

## 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.

<b>Syntax Description</b>	N/A
<b>Default</b>	enable
<b>Configuration Mode</b>	Config
<b>History</b>	3.1.0000
	3.4.0000 Updated Example
<b>Role</b>	admin
<b>Example</b>	<pre>switch (config) # web enable switch (config) # show web  Web User Interface:   Web interface enabled: yes   HTTP enabled: yes   HTTP port: 80   HTTP redirect to HTTPS: no   HTTPS enabled: yes   HTTPS port: 443   HTTPS ssl-ciphers: all   HTTPS certificate name: default-cert   Listen enabled: yes   No Listen Interfaces.    Inactivity timeout: 1 hr   Session timeout: 2 hr 30 min   Session renewal: 30 min    Web file transfer proxy:     Proxy enabled: no    Web file transfer certificate authority:     HTTPS server cert verify: yes     HTTPS supplemental CA list: default-ca-list switch (config) #</pre>
<b>Related Commands</b>	show web
<b>Note</b>	

## 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.

<b>Syntax Description</b>	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.
<b>Default</b>	HTTP is enabled HTTP TCP port is 80 HTTP redirect to HTTPS is disabled	
<b>Configuration Mode</b>	Config	
<b>History</b>	3.1.0000	
	3.4.0000	Updated Example
<b>Role</b>	admin	

---

**Example**

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

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

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

Web file transfer proxy:
  Proxy enabled: no

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

---

**Related Commands**

show web  
web enable

---

**Note**

Enabling HTTP is meaningful if the WebUI as a whole is enabled.

---

## web httpd

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

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

<b>Syntax Description</b>	enable	Enables Web interface restrictions on access to this system.
	interface <ifName>	Adds interface to Web server access restriction list (i.e. mgmt0, mgmt1)

**Default** Listening is enabled.  
all interfaces are permitted.

**Configuration Mode** Config

**History** 3.1.0000

3.4.0000 Updated Example

**Role** admin

**Example**

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

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

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

Web file transfer proxy:
  Proxy enabled: no

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

---

**Related Commands**

N/A

**Note**

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

---

## web https

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

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

<b>Syntax Description</b>	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.
<b>Default</b>	HTTPS is enabled Default port is 443	
<b>Configuration Mode</b>	Config	
<b>History</b>	3.1.0000	
	3.4.0000	Added “ssl ciphers” parameter
	3.4.0010	Added TLS parameter to “ssl ciphers”
<b>Role</b>	admin	

**Example**

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

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

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

Web file transfer proxy:
  Proxy enabled: no

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

**Related Commands**

show web  
web enable

**Note**

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

## 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>
MellanoxMLNX-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 In-Band Management

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

The in-band management feature does not require any license. However, it works only for the system profile Ethernet. It can be enabled with IP Routing but not with IP Proxy-ARP.

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

**Step 1.** Create a VLAN. Run:

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

**Step 2.** Create a VLAN interface. Run:

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

**Step 3.** Configure L3 attributes on the newly created VLAN interface. Run:

```
switch (config interface vlan 10) # ip address 10.10.10.10 /24
```

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

```
switch (config) # show interfaces vlan 10
Admin state: Enabled
Operational state: Up
Mac Address: f4:52:14:67:07:e8
Internet Address: 10.10.10.10/24
Broadcast address: 10.10.10.255
MTU: 1500 bytes
Arp timeout: 1500 seconds
Icmp redirect: Disabled
Description: N/A
VRF: default
Counters: Enabled
RX
 0 Unicast packets
 0 Multicast packets
 0 Unicast bytes
 0 Multicast bytes
 0 Bad packets
 0 Bad bytes
TX
 0 Unicast packets
 0 Multicast packets
 0 Unicast bytes
 0 Multicast bytes
switch (config) #
```

#### 4.1.6 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 the user would need to make sure the HA master has the same HA node names as the DHCP server.

## 4.1.7 Commands

#### **4.1.7.1 Interface**

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

## interface

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

Enters a management interface context.

<b>Syntax Description</b>	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).
<b>Default</b>	N/A	
<b>Configuration Mode</b>	Config	
<b>History</b>	3.1.0000	
<b>Role</b>	admin	
<b>Example</b>	<pre>switch (config) # interface mgmt0 switch (config interface mgmt0) #</pre>	
<b>Related Commands</b>	show interfaces <ifname>	
<b>Notes</b>		

## 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.

<b>Syntax Description</b>	IP address	IPv4 address
	netmask	Subnet mask of IP address
<b>Default</b>	0.0.0.0/0	
<b>Configuration Mode</b>	Config Interface Management	
<b>History</b>	3.1.0000	
<b>Role</b>	admin	
<b>Example</b>	<pre>switch (config) # interface mgmt0 switch (config interface mgmt0) # ip address 10.10.10.10 255.255.255.0 switch (config interface mgmt0) # show interfaces mgmt0 Interface mgmt0 state     Admin up: yes     Link up: yes     IP address: 10.10.10.10     Netmask: 255.255.255.0     IPv6 enabled: yes     Autoconf enabled: no     Autoconf route: yes     Autoconf privacy: no     IPv6 addresses: 1     IPv6 address: fe80:202:c9ff:fe5e:a5d8/64     Speed: 1000Mb/s (auto)     Duplex: full (auto)     Interface type: ethernet     Interface ifindex: 2     Interface source: physical     MTU: 1500     HW address: 00:02:C9:5E:A5:D8     Comment:      RX bytes: 2946769856 TX bytes: 467577486     RX packets: 44866091 TX packets: 1385520     RX mcast packets: 0 TX discards: 0     RX discards: 0 TX errors: 0     RX errors: 0 TX overruns: 0     RX overruns: 0 TX carrier: 0     RX frame: 0 TX collisions: 0  TX queue len: 1000  switch (config interface mgmt0) #</pre>	

---

**Related Commands** show interfaces <ifname>

**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.

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

### 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.

<b>Syntax Description</b>	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.
<b>Default</b>	N/A	
<b>Configuration Mode</b>	Config Interface Management	
<b>History</b>	3.1.0000	
<b>Role</b>	admin	

**Example**

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

    RX bytes:        2970074221      TX bytes:        468579522
    RX packets:       44983023       TX packets:       1390539
    RX mcast packets: 0               TX discards:    0
    RX discards:      0               TX errors:       0
    RX errors:        0               TX overruns:    0
    RX overruns:      0               TX carrier:     0
    RX frame:         0               TX collisions:  0
                                         TX queue len: 1000

switch (config interface mgmt0) #
```

**Related Commands**

show interfaces <ifname>

**Notes**

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

## mtu

**mtu <bytes>**  
**no mtu <bytes>**

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

<b>Syntax Description</b>	bytes	The entry range is 68-1500.
<b>Default</b>	1500	
<b>Configuration Mode</b>	Config Interface Management	
<b>History</b>	3.6.3004	
<b>Role</b>	admin	
<b>Example</b>	<pre>switch (config interface mgmt0) # mtu 1500 switch (config interface mgmt0) # show interfaces mgmt0 Interface mgmt0 state     Admin up:          yes     Link up:          yes     IP address:      172.30.2.2     Netmask:         255.255.0.0     Secondary address: 9.9.9.9/32 (alias: 'mgmt0:2')     IPv6 enabled:     yes     Autoconf enabled: no     Autoconf route:   yes     Autoconf privacy: no     IPv6 addresses:   1     IPv6 address:     fe80:202:c9ff:fe5e:a5d8/64     Speed:           1000Mb/s (auto)     Duplex:          full (auto)     Interface type:  ethernet     Interface ifindex: 2     Interface source: physical     MTU:             1500     HW address:      00:02:C9:5E:A5:D8     Comment:      RX bytes:        2970074221      TX bytes:        468579522     RX packets:       44983023      TX packets:       1390539     RX mcast packets: 0            TX discards:     0     RX discards:      0            TX errors:       0     RX errors:        0            TX overruns:    0     RX overruns:      0            TX carrier:     0     RX frame:         0            TX collisions:  0                                 TX queue len: 1000  switch (config interface mgmt0) #</pre>	
<b>Related Commands</b>	show interfaces <ifname>	
<b>Notes</b>		

## 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.

<b>Syntax Description</b>	duplex	Sets the duplex mode of the interface. The following are the possible values: <ul style="list-style-type: none"><li>• half - half duplex</li><li>• full - full duplex</li><li>• auto - auto duplex sensing (half or full)</li></ul>
<b>Default</b>	auto	
<b>Configuration Mode</b>	Config Interface Management	
<b>History</b>	3.1.0000	
<b>Role</b>	admin	
<b>Example</b>	<pre>switch (config interface mgmt0) # duplex auto switch (config interface mgmt0) # show interfaces mgmt0 Interface mgmt0 state     Admin up:          yes     Link up:          yes     IP address:       172.30.2.2     Netmask:          255.255.0.0     Secondary address: 9.9.9.9/32 (alias: 'mgmt0:2')     IPv6 enabled:     yes     Autoconf enabled: no     Autoconf route:   yes     Autoconf privacy: no     IPv6 addresses:   1     IPv6 address:     fe80::202:c9ff:fe5e:a5d8/64     Speed:            1000Mb/s (auto)     Duplex:           full (auto)     Interface type:   ethernet     Interface ifindex: 2     Interface source: physical     MTU:              1500     HW address:       00:02:C9:5E:A5:D8     Comment:      RX bytes:        2970074221      TX bytes:        468579522     RX packets:       44983023       TX packets:       1390539     RX mcast packets: 0               TX discards:    0     RX discards:      0               TX errors:       0     RX errors:        0               TX overruns:    0     RX overruns:      0               TX carrier:     0     RX frame:         0               TX collisions:  0  TX queue len: 1000  switch (config interface mgmt0) #</pre>	

**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.

<b>Syntax Description</b>	speed	Sets the speed of the interface. The following are the possible values: <ul style="list-style-type: none"> <li>• 10 - fixed to 10Mbps</li> <li>• 100 - fixed to 100Mbps</li> <li>• 1000 - fixed to 1000Mbps</li> <li>• auto - auto speed sensing (10/100/1000Mbps)</li> </ul>
<b>Default</b>	auto	
<b>Configuration Mode</b>	Config Interface Management	
<b>History</b>	3.1.0000	
<b>Role</b>	admin	
<b>Example</b>	<pre>switch (config interface mgmt0) # speed auto switch (config interface mgmt0) # show interfaces mgmt0 Interface mgmt0 state     Admin up: yes     Link up: yes     IP address: 172.30.2.2     Netmask: 255.255.0.0     Secondary address: 9.9.9.9/32 (alias: 'mgmt0:2')     IPv6 enabled: yes     Autoconf enabled: no     Autoconf route: yes     Autoconf privacy: no     IPv6 addresses: 1     IPv6 address: fe80::202:c9ff:fe5e:a5d8/64     Speed: 1000Mb/s (auto)     Duplex: full (auto)     Interface type: ethernet     Interface ifindex: 2     Interface source: physical     MTU: 1500     HW address: 00:02:C9:5E:A5:D8     Comment:      RX bytes: 2970074221 TX bytes: 468579522     RX packets: 44983023 TX packets: 1390539     RX mcast packets: 0 TX discards: 0     RX discards: 0 TX errors: 0     RX errors: 0 TX overruns: 0     RX overruns: 0 TX carrier: 0     RX frame: 0 TX collisions: 0     TX queue len: 1000  switch (config interface mgmt0) #</pre>	

**Related Commands**

show interfaces <ifname>

**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.

<b>Syntax Description</b>	renew  Forces a renewal of the IP address. A restart on the DHCP client for the specified interface will be issued.
<b>Default</b>	Could be enabled or disabled (per part number) manufactured with 3.2.0500
<b>Configuration Mode</b>	Config Interface Management
<b>History</b>	3.1.0000
<b>Role</b>	admin
<b>Example</b>	<pre>switch (config interface mgmt0) # dhcp switch (config) # show interfaces mgmt0 configured Interface mgmt0 configuration     Enabled:          yes     DHCP:             yes     Zeroconf:         no     IP address:     Netmask:     IPv6 enabled:     yes     Autoconf enabled: no     Autoconf route:   yes     Autoconf privacy: no     IPv6 addresses:   0     Speed:     Duplex:     MTU:              1500     Comment:</pre>
<b>Related Commands</b>	show interfaces <ifname> configured
<b>Notes</b>	<ul style="list-style-type: none"> <li>When enabling DHCP, the IP address and netmask are received via DHCP hence, the static IP address configuration is ignored</li> <li>Enabling DHCP disables zeroconf and vice versa</li> <li>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.</li> </ul>

## 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.

<b>Syntax Description</b>	N/A
<b>Default</b>	Enabled
<b>Configuration Mode</b>	Config Interface Management
<b>History</b>	3.5.1000
<b>Role</b>	admin
<b>Example</b>	<pre>switch (config interface mgmt0) # dhcp hostname switch (config interface mgmt0) #</pre>
<b>Related Commands</b>	<code>hostname &lt;hostname&gt;</code> <code>show interfaces &lt;ifname&gt; configured</code>
<b>Notes</b>	<ul style="list-style-type: none"><li>If a hostname is configured manually by the user, that configuration would override the “dhcp hostname” configuration</li><li>After upgrading to version 3.5.1000 when a default hostname is not configured, the DHCP server assigns the new hostname for your machine</li><li>These commands do not work on in-band interfaces</li></ul>

## shutdown

**shutdown**  
**no shutdown**

Disables the specified interface.

The no form of the command enables the specified interface.

<b>Syntax Description</b>	N/A
<b>Default</b>	no shutdown
<b>Configuration Mode</b>	Config Interface Management
<b>History</b>	3.1.0000
<b>Role</b>	admin
<b>Example</b>	<pre>switch (config interface mgmt0) # no shutdown switch (config) # show interfaces mgmt0 configured Interface mgmt0 configuration     Enabled:          yes     DHCP:             yes     DHCP Hostname:   yes     Zeroconf:         no     IP address:     Netmask:     IPv6 enabled:     yes     Autoconf enabled: no     Autoconf route:   yes     Autoconf privacy: no     IPv6 addresses:   0     Speed:            auto     Duplex:           auto     MTU:              1500     Comment: switch (config) #</pre>
<b>Related Commands</b>	show interfaces <ifname> configured
<b>Notes</b>	

## 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.

<b>Syntax Description</b>	N/A
<b>Default</b>	no zeroconf
<b>Configuration Mode</b>	Config Interface Management
<b>History</b>	3.1.0000
<b>Role</b>	admin
<b>Example</b>	<pre>switch (config interface mgmt0) # zeroconf switch (config) # show interfaces mgmt0 configured Interface mgmt0 configuration     Enabled:           yes     DHCP:              no     DHCP Hostname:    yes     Zeroconf:          yes     IP address:     Netmask:     IPv6 enabled:     yes     Autoconf enabled: no     Autoconf route:   yes     Autoconf privacy: no     IPv6 addresses:   0     Speed:             auto     Duplex:            auto     MTU:               1500     Comment:</pre>
<b>Related Commands</b>	show interfaces <ifname> configured
<b>Notes</b>	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.

<b>Syntax Description</b>	comment	A free-form string that has no semantics other than being displayed when the interface records are listed.
<b>Default</b>	no comment	
<b>Configuration Mode</b>	Config Interface Management	
<b>History</b>	3.1.0000	
<b>Role</b>	admin	
<b>Example</b>	<pre>switch (config interface mgmt0) # comment my-interface switch (config interface mgmt0) # show interfaces mgmt0 Interface mgmt0 state     Admin up:           yes     Link up:           yes     IP address:        172.30.2.2     Netmask:           255.255.0.0     IPv6 enabled:      yes     Autoconf enabled: no     Autoconf route:   yes     Autoconf privacy: no     IPv6 addresses:   1     IPv6 address:     fe80::202:c9ff:fe5e:a5d8/64     Speed:             1000Mb/s (auto)     Duplex:            full (auto)     Interface type:   ethernet     Interface ifindex: 2     Interface source: physical     MTU:               1500     HW address:       00:02:C9:5E:A5:D8     Comment:           my-interface      RX bytes:          962067812          TX bytes:        40658219     RX packets:         3738865           TX packets:       142345     RX mcast packets:  0                 TX discards:    0     RX discards:        0                 TX errors:      0     RX errors:          0                 TX overruns:   0     RX overruns:        0                 TX carrier:    0     RX frame:          0                 TX collisions: 0  TX queue len: 1000  switch (config interface mgmt0) #</pre>	
<b>Related Commands</b>	N/A	
<b>Notes</b>		

## 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.

<b>Syntax Description</b>	N/A
<b>Default</b>	IPv6 addressing is disabled
<b>Configuration Mode</b>	Config Interface Management
<b>History</b>	3.1.0000
<b>Role</b>	admin
<b>Example</b>	<pre>switch (config interface mgmt0) # ipv6 enable switch (config interface mgmt0) # show interfaces mgmt0 Interface mgmt0 state     Admin up:          yes     Link up:          yes     IP address:      172.30.2.2     Netmask:         255.255.0.0     IPv6 enabled:     yes     Autoconf enabled: no     Autoconf route:   yes     Autoconf privacy: no     IPv6 addresses:   1     IPv6 address:    fe80::202:c9ff:fe5e:a5d8/64     Speed:           1000Mb/s (auto)     Duplex:          full (auto)     Interface type:  ethernet     Interface ifindex: 2     Interface source: physical     MTU:             1500     HW address:      00:02:C9:5E:A5:D8     Comment:         my-interface      RX bytes:        962067812      TX bytes:      40658219     RX packets:       3738865       TX packets:      142345     RX mcast packets: 0            TX discards:   0     RX discards:      0            TX errors:      0     RX errors:        0            TX overruns:   0     RX overruns:      0            TX carrier:    0     RX frame:         0            TX collisions: 0                                 TX queue len: 1000  switch (config interface mgmt0) #</pre>

**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.

---

<b>Syntax Description</b>	IPv6 address/netmask  autoconfig	Configures a static IPv6 address and netmask. Format example: 2001:db8:1234::5678/64.  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.
<b>Default</b>	No IP address available, auto config is enabled	
<b>Configuration Mode</b>	Config Interface Management	
<b>History</b>	3.1.0000	
<b>Role</b>	admin	

---

**Example**

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

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

switch (config interface mgmt0) #
```

**Related Commands**

ipv6 enable  
show interface <ifname>

**Notes**

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

## ipv6 dhcp primary-intf

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

Sets the interface from which non-interface-specific (resolver) configuration is accepted via DHCPv6.

The no form of the command resets non-interface-specific (resolver) configuration.

<b>Syntax Description</b>	if-name	Interface name: <ul style="list-style-type: none"><li>• lo</li><li>• mgmt0</li><li>• mgmt1</li></ul>
<b>Default</b>	N/A	
<b>Configuration Mode</b>	Config	
<b>History</b>	3.1.0000	
<b>Role</b>	admin	
<b>Example</b>	<pre>switch (config) # ipv6 dhcp primary-intf mgmt0 switch (config) #</pre>	
<b>Related Commands</b>	ipv6 enable ipv6 address show interface <ifname>	
<b>Notes</b>		

## ipv6 dhcp stateless

**ipv6 dhcp stateless**  
**no ipv6 dhcp stateless**

Enables stateless DHCPv6 requests.

The no form of the command disables stateless DHCPv6 requests.

<b>Syntax Description</b>	N/A
<b>Default</b>	N/A
<b>Configuration Mode</b>	Config
<b>History</b>	3.1.0000
<b>Role</b>	admin
<b>Example</b>	<pre>switch (config) # ipv6 dhcp stateless switch (config) #</pre>
<b>Related Commands</b>	<a href="#">ipv6 enable</a> <a href="#">ipv6 address</a> <a href="#">show interface &lt;ifname&gt;</a>
<b>Notes</b>	<ul style="list-style-type: none"><li>This command only gets DNS configuration, not an IPv6 address</li><li>The no form of the command requests all information, including an IPv6 address</li></ul>

## show interface brief

**show interface <ifname> brief**

Displays a brief info on the interface configuration and status.

<b>Syntax Description</b>	ifname	The interface name e.g., “mgmt0”, “mgmt1”, “lo” (loopback), etc.
<b>Default</b>	N/A	
<b>Configuration Mode</b>	Any Command Mode	
<b>History</b>	3.1.0000	
<b>Role</b>	admin	
<b>Example</b>	<pre>switch (config) # show interfaces mgmt0 brief Interface mgmt0 state   Admin up: yes   Link up: yes   IP address: 172.30.2.2   Netmask: 255.255.0.0   IPv6 enabled: yes   Autoconf enabled: no   Autoconf route: yes   Autoconf privacy: no   IPv6 addresses: 1   IPv6 address: fe80::202:c9ff:fe5e:a5d8/64   Speed: 1000Mb/s (auto)   Duplex: full (auto)   Interface type: ethernet   Interface ifindex: 2   Interface source: physical   MTU: 1500   HW address: 00:02:C9:5E:A5:D8   Comment: my-interface switch (config) #</pre>	
<b>Related Commands</b>	N/A	
<b>Notes</b>		

## show interface configured

### show interface <ifname> configured

Displays configuration information about the specified interface.

<b>Syntax Description</b>	ifname	The interface name e.g., “mgmt0”, “mgmt1”, “lo” (loopback), etc.
<b>Default</b>	N/A	
<b>Configuration Mode</b>	Any Command Mode	
<b>History</b>	3.1.0000	
	3.5.1000	Updated Example with “DHCP Hostname”
<b>Role</b>	admin	
<b>Example</b>	<pre>switch (config) # show interfaces mgmt0 configured Interface mgmt0 configuration     Enabled:          yes     DHCP:             yes     DHCP Hostname:   yes     Zeroconf:         no     IP address:     Netmask:     IPv6 enabled:    yes     Autoconf enabled: no     Autoconf route:  yes     Autoconf privacy: no     IPv6 addresses:  0     Speed:            auto     Duplex:           auto     MTU:              1500     Comment:          my-interface</pre>	
<b>Related Commands</b>	N/A	
<b>Notes</b>		

#### 4.1.7.2 Hostname Resolution

##### hostname

**hostname <hostname>**  
**no hostname**

Sets a static system hostname.

The no form of the command clears the system hostname.

<b>Syntax Description</b>	hostname	A free-form string.
<b>Default</b>	Default hostname	
<b>Configuration Mode</b>	Config	
<b>History</b>	3.1.0000	
	3.6.3004	Added support for the character “.”
<b>Role</b>	admin	
<b>Example</b>	switch (config) # hostname my-switch-hostname my-switch-hostname (config) #	
<b>Related Commands</b>	show hosts	
<b>Notes</b>	<ul style="list-style-type: none"><li>• Hostname may contain letters, numbers, and hyphens ('-'), in any combination</li><li>• Hostname may not contain other characters, such as "%", "_" etc.</li><li>• The character “.” is supported</li><li>• Hostname may not begin with a hyphen</li><li>• Hostname may be 1-63 characters long</li><li>• Changing hostname stamps a new HTTPS certificate</li></ul>	

## 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.
<b>Default</b>	No server name	
<b>Configuration Mode</b>	Config	
<b>History</b>	3.1.0000	
<b>Role</b>	admin	
<b>Example</b>	<pre>switch (config) # ip name-server 9.9.9.9 switch (config) # show hosts Hostname: switch Name server: 9.9.9.9 (configured) Name server: 10.211.0.121 (dynamic) Name server: 172.30.0.126 (dynamic) Name server: 10.4.0.135 (dynamic) Domain name: lab.mtl.com (dynamic) Domain name: vmlab.mtl.com (dynamic) Domain name: yok.mtl.com (dynamic) Domain name: mtl.com (dynamic) IP 127.0.0.1 maps to hostname localhost IPv6 ::1 maps to hostname localhost Automatically map hostname to loopback address: yes Automatically map hostname to IPv6 loopback address: no switch (config) #</pre>	
<b>Related Commands</b>	show hosts	
<b>Notes</b>		

## 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.

<b>Syntax Description</b>	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).
<b>Default</b>	No static domain name	
<b>Configuration Mode</b>	Config	
<b>History</b>	3.1.0000	
<b>Role</b>	admin	
<b>Example</b>	<pre>switch (config) # ip domain-list mydomain.com switch (config) # show hosts Hostname: switch Name server: 10.211.0.121 (dynamic) Name server: 172.30.0.126 (dynamic) Name server: 10.4.0.135 (dynamic) Domain name: mydomain.com (configured) Domain name: lab.mtl.com (dynamic) Domain name: vmlab.mtl.com (dynamic) Domain name: yok.mtl.com (dynamic) Domain name: mtl.com (dynamic) IP 1.1.1.1 maps to hostname p IP 127.0.0.1 maps to hostname localhost IPv6 ::1 maps to hostname localhost6 Automatically map hostname to loopback address: yes Automatically map hostname to IPv6 loopback address: no switch (config) #</pre>	
<b>Related Commands</b>	show hosts	
<b>Notes</b>		

## 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.

<b>Syntax Description</b>	hostname IP Address	The hostname in a string form. The IPv4 or IPv6 address.
<b>Default</b>	No static domain name.	
<b>Configuration Mode</b>	Config	
<b>History</b>	3.1.0000	
<b>Role</b>	admin	
<b>Example</b>	<pre>switch (config) # ip host my-host 2.2.2.2 switch (config) # ipv6 host my-ipv6-host 2001::8f9 switch (config) # show hosts Hostname: switch Name server: 9.9.9.9 (configured) Name server: 10.211.0.121 (dynamic) Name server: 172.30.0.126 (dynamic) Name server: 10.4.0.135 (dynamic) Domain name: mydomain.com (configured) Domain name: lab.mtl.com (dynamic) Domain name: vmlab.mtl.com (dynamic) Domain name: yok.mtl.com (dynamic) Domain name: mtl.com (dynamic) IP 1.1.1.1 maps to hostname p IP 127.0.0.1 maps to hostname localhost IP 2.2.2.2 maps to hostname my-host IPv6 2001::8f9 maps to hostname my-ipv6-host IPv6 ::1 maps to hostname localhost6 Automatically map hostname to loopback address: yes Automatically map hostname to IPv6 loopback address: yes switch (config) #</pre>	
<b>Related Commands</b>	show hosts	
<b>Notes</b>		

## 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.

<b>Syntax Description</b>	N/A
<b>Default</b>	IPv4 mapping is enabled by default IPv6 mapping is disabled by default
<b>Configuration Mode</b>	Config
<b>History</b>	3.1.0000
<b>Role</b>	admin
<b>Example</b>	<pre>switch (config) # ip map-hostname switch (config) # # show hosts Hostname: switch Name server: 9.9.9.9 (configured) Name server: 10.211.0.121 (dynamic) Name server: 172.30.0.126 (dynamic) Name server: 10.4.0.135 (dynamic) Domain name: mydomain.com (configured) Domain name: lab.mtl.com (dynamic) Domain name: vmlab.mtl.com (dynamic) Domain name: yok.mtl.com (dynamic) Domain name: mtl.com (dynamic) IP 1.1.1.1 maps to hostname p IP 127.0.0.1 maps to hostname localhost IP 2.2.2.2 maps to hostname my-host IPv6 2001::8f9 maps to hostname my-ipv6-host IPv6 ::1 maps to hostname localhost6 Automatically map hostname to loopback address: yes Automatically map hostname to IPv6 loopback address: yes switch (config) # switch (config) # ping my-host-name PING localhost (127.0.0.1) 56(84) bytes of data. 64 bytes from localhost (127.0.0.1): icmp_seq=1 ttl=64 time=0.078 ms 64 bytes from localhost (127.0.0.1): icmp_seq=2 ttl=64 time=0.052 ms 64 bytes from localhost (127.0.0.1): icmp_seq=3 ttl=64 time=0.058 ms</pre>

**Related Commands**

show hosts

**Notes**

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

## show hosts

### show hosts

Displays hostname, DNS configuration, and static host mappings.

<b>Syntax Description</b>	N/A
<b>Default</b>	N/A
<b>Configuration Mode</b>	Any Command Mode
<b>History</b>	3.1.0000
<b>Role</b>	admin
<b>Example</b>	<pre>switch (config) # show hosts Hostname: my-host-name Name server: 9.9.9.9 (configured) Name server: 10.211.0.121 (dynamic) Name server: 172.30.0.126 (dynamic) Name server: 10.4.0.135 (dynamic) Domain name: mydomain.com (configured) Domain name: lab.mtl.com (dynamic) Domain name: vmlab.mtl.com (dynamic) Domain name: yok.mtl.com (dynamic) Domain name: mtl.com (dynamic) IP 1.1.1.1 maps to hostname p IP 127.0.0.1 maps to hostname localhost IP 2.2.2.2 maps to hostname my-host IPv6 ::1 maps to hostname localhost6 Automatically map hostname to loopback address: yes Automatically map hostname to IPv6 loopback address: no switch (config) #</pre>
<b>Related Commands</b>	N/A
<b>Notes</b>	

#### 4.1.7.3 Routing

##### ip/ipv6 route

**{ip | ipv6} route vrf <vrf-name> <network-prefix> <netmask> <next-hop>**  
**no ip route <vrf-name> <network-prefix> <netmask> <next-hop>**

Sets a static route for a given IP.

The no form of the command deletes the static route.

<b>Syntax Description</b>	network-prefix	IPv4 or IPv6 network prefix.
	netmask	IPv4 netmask formats are: <ul style="list-style-type: none"> <li>• /24</li> <li>• 255.255.255.0</li> </ul> IPv6 netmask format is: <ul style="list-style-type: none"> <li>• /48 (as a part of the network prefix)</li> </ul>
	nexthop-address	The IPv4 or IPv6 address of the next hop router for this route.
	ifname	The interface name (e.g., mgmt0, mgmt1).
<b>Default</b>	N/A	
<b>Configuration Mode</b>	Config	
<b>History</b>	3.1.0000	
<b>Role</b>	admin	
<b>Example</b>	switch (config) # ip route 20.20.20.0 255.255.255.0 mgmt0	
<b>Related Commands</b>	show ip route	
<b>Notes</b>		

## 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.

<b>Syntax Description</b>	ip address	The default gateway IP address (IPv6).
	ifname	The interface name (e.g., mgmt0, mgmt1).
<b>Default</b>	N/A	
<b>Configuration Mode</b>	Config	
<b>History</b>	3.1.0000	
	3.2.0500	removed IPv4 configuration option
<b>Role</b>	admin	
<b>Example</b>	switch (config) # ipv6 default-gateway ::1	
<b>Related Commands</b>	show ip/ipv6 route show ipv6 default-gateway	
<b>Notes</b>	<ul style="list-style-type: none"><li>The configured default gateway will not be used if DHCP is enabled.</li><li>In order to configure ipv4 default-gateway use ‘ip route’ command.</li></ul>	

## show ip/ipv6 route

**show {ip | ipv6} route [static]**

Displays the routing table in the system.

<b>Syntax Description</b>	static	Filters the table with the static route entries.
<b>Default</b>	N/A	
<b>Configuration Mode</b>	Any Command Mode	
<b>History</b>	3.1.0000	
<b>Role</b>	admin	
<b>Example</b>	<pre>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 ::: ::1/128 :: 2222:2222:2222::/64 :: switch (config) #</pre>	
<b>Related Commands</b>	show ip default-gateway	
<b>Notes</b>		

## show ipv6 default-gateway

**show ipv6 default-gateway [static]**

Displays the default gateway.

<b>Syntax Description</b>	static	Displays the static configuration of the default gateway
<b>Default</b>	N/A	
<b>Configuration Mode</b>	Any Command Mode	
<b>History</b>	3.1.0000	
<b>Role</b>	admin	
<b>Example</b>	<pre>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</pre>	
<b>Related Commands</b>	ipv6 default-gateway	
<b>Notes</b>	The configured IPv4 default gateway will not be used if DHCP is enabled.	

#### 4.1.7.4 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.

<b>Syntax Description</b>	IP address	IPv4 address.
	MAC address	MAC address.
<b>Default</b>	N/A	
<b>Configuration Mode</b>	Config Interface Management	
<b>History</b>	3.2.0500	
<b>Role</b>	admin	
<b>Example</b>	switch (config interface mgmt0) #ip arp 20.20.20.20 aa:aa:aa:aa:aa:aa	
<b>Related Commands</b>	show ip arp ip route	
<b>Notes</b>		

## 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.

<b>Syntax Description</b>	timeout-value	Time (in seconds) that an entry remains in the ARP cache. Range: 60-28800.
	vrf-name	VRF session name
<b>Default</b>	1500 seconds	
<b>Configuration Mode</b>	Config	
<b>History</b>	3.2.0230	
	3.5.1000	Added VRF parameter and updated Notes
<b>Role</b>	admin	
<b>Example</b>	<pre>switch (config) # ip arp timeout 2000 switch (config) #</pre>	
<b>Related Commands</b>	ip arp show ip arp	
<b>Notes</b>	<ul style="list-style-type: none"><li>This value is used as the default ARP timeout whenever a new IP interface is created</li><li>The time interval after which each ARP entry becomes stale may actually vary from 50-150% of the configured value</li></ul>	

## show ip arp

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

Displays ARP table.

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

## 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.

<b>Syntax Description</b>	IPv6 address ifname MAC address	The IPv6 address. The management interface (i.e. mgmt0, mgmt1). The MAC address.
<b>Default</b>	N/A	
<b>Configuration Mode</b>	Config	
<b>History</b>	3.1.0000	
<b>Role</b>	admin	
<b>Example</b>	<pre>switch (config) # ipv6 neighbor 2001:db8:701f::8f9 mgmt0 00:11:22:33:44:55 switch (config) #</pre>	
<b>Related Commands</b>	show ipv6 neighbor ipv6 route arp clear ipv6 neighbors	
<b>Notes</b>	<ul style="list-style-type: none"> <li>ARP is used only with IPv4. In IPv6 networks, Neighbor Discovery Protocol (NDP) is used similarly.</li> <li>Use The no form of the command to remove static entries. Dynamic entries can be cleared via the “clear ipv6 neighbors” command.</li> </ul>	

## clear ipv6 neighbors

```
clear ipv6 neighbors {ethernet <port> | vlan <vlan-id> | port-channel <id> | vrf <vrf-id>} [<ip-addr>]
```

Clears the dynamic neighbors cache.

<b>Syntax Description</b>	N/A
<b>Default</b>	N/A
<b>Configuration Mode</b>	Config
<b>History</b>	3.1.0000
	3.6.4110 Updated command.
<b>Role</b>	admin
<b>Example</b>	<pre>switch (config) # clear ipv6 neighbors switch (config) #</pre>
<b>Related Commands</b>	ipv6 neighbor show ipv6 neighbor arp
<b>Notes</b>	<ul style="list-style-type: none"><li>• Clearing Neighbor Discovery Protocol (NDP) cache removes only the dynamic entries learned and not the static entries configured</li><li>• Use the no form of the command to remove static entries</li></ul>

## show ipv6 neighbors

### show ipv6 neighbors [static]

Displays the Neighbor Discovery Protocol (NDP) table.

<b>Syntax Description</b>	static	Filters only the table of the static entries.
<b>Default</b>	N/A	
<b>Configuration Mode</b>	Config	
<b>History</b>	3.1.0000	
<b>Role</b>	admin	
<b>Example</b>	<pre>switch (config) # show ipv6 neighbors IPv6 Address          Age MAC Address      State      Interf ----- 2001::2                9428 AA:AA:AA:AA:AA permanent mgmt0 switch (config) #</pre>	
<b>Related Commands</b>	<ul style="list-style-type: none"><li>ipv6 neighbor</li><li>clear ipv6 neighbor</li><li>show ipv6</li></ul>	
<b>Notes</b>		

#### 4.1.7.5 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-host-
name}
```

Sets global DHCP configuration.

The no form of the command deletes the DHCP configuration.

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

## show ip dhcp

### show ip dhcp

Displays the DHCP configuration and status.

<b>Syntax Description</b>	N/A
<b>Default</b>	N/A
<b>Configuration Mode</b>	Any Command Mode
<b>History</b>	3.1.0000 3.6.5000                          Updated Example
<b>Role</b>	admin
<b>Example</b>	<pre>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</pre>
<b>Related Commands</b>	ip dhcp dhcp [renew]
<b>Notes</b>	

#### 4.1.7.6 General IPv6 Commands

##### ipv6 enable

**ipv6 enable**  
**no ipv6 enable**

Enables IPv6 globally on the management interface.

The no form of the command disables IPv6 globally on the management interface.

<b>Syntax Description</b>	N/A
<b>Default</b>	IPv6 is disabled
<b>Configuration Mode</b>	Config
<b>History</b>	3.1.0000
<b>Role</b>	admin
<b>Example</b>	<pre>switch (config) # ipv6 enable switch (config) # show ipv6 IPv6 summary     IPv6 supported:          yes     IPv6 admin enabled:      yes     IPv6 interface count:   2 switch (config) #</pre>
<b>Related Commands</b>	<a href="#">ipv6 default-gateway</a> <a href="#">ipv6 host</a> <a href="#">ipv6 map-hostname</a> <a href="#">ipv6 neighbor</a> <a href="#">ipv6 route</a> <a href="#">show ipv6</a> <a href="#">show ipv6 default-gateway</a> <a href="#">show ipv6 route</a>
<b>Notes</b>	

#### 4.1.7.7 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.

<b>Syntax Description</b>	Linux Ping options <a href="http://linux.about.com/od/commands/l/blcmdl8_ping.htm">http://linux.about.com/od/commands/l/blcmdl8_ping.htm</a>
<b>Default</b>	N/A
<b>Configuration Mode</b>	Config
<b>History</b>	3.1.0000
<b>Role</b>	admin
<b>Example</b>	<pre>switch (config) # ping 172.30.2.2 PING 172.30.2.2 (172.30.2.2) 56(84) bytes of data. 64 bytes from 172.30.2.2: icmp_seq=1 ttl=64 time=0.703 ms 64 bytes from 172.30.2.2: icmp_seq=2 ttl=64 time=0.187 ms 64 bytes from 172.30.2.2: icmp_seq=3 ttl=64 time=0.166 ms 64 bytes from 172.30.2.2: icmp_seq=4 ttl=64 time=0.161 ms 64 bytes from 172.30.2.2: icmp_seq=5 ttl=64 time=0.153 ms 64 bytes from 172.30.2.2: icmp_seq=6 ttl=64 time=0.144 ms ^C --- 172.30.2.2 ping statistics --- 6 packets transmitted, 6 received, 0% packet loss, time 5004ms rtt min/avg/max/mdev = 0.144/0.252/0.703/0.202 ms switch (config) #</pre>
<b>Related Commands</b>	traceroutes
<b>Notes</b>	

## traceroute

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

Traces the route packets take to a destination.

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

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

---

**Related Commands**

---

**Notes**

---

## tcpdump

```
tcpdump [-aAdDefLnNOpqRStuUvxX] [-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.

<b>Syntax Description</b>	N/A
<b>Default</b>	N/A
<b>Configuration Mode</b>	Config
<b>History</b>	3.1.0000
<b>Role</b>	admin
<b>Example</b>	<pre>switch (config) # tcpdump ..... 09:37:38.678812 IP 192.168.10.7.ssh &gt; 192.168.10.1.54155: P 1494624:1494800(176) ack 625 win 90 &lt;nop,nop,timestamp 5842763 858672398&gt; 09:37:38.678860 IP 192.168.10.7.ssh &gt; 192.168.10.1.54155: P 1494800:1495104(304) ack 625 win 90 &lt;nop,nop,timestamp 5842763 858672398&gt; ... 9141 packets captured 9142 packets received by filter 0 packets dropped by kernel switch (config) #</pre>
<b>Related Commands</b>	N/A
<b>Notes</b>	

## 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.

<b>Syntax Description</b>	hh:mm:ss yyyy/mm/dd	Time. Date.
<b>Default</b>	N/A	
<b>Configuration Mode</b>	Config	
<b>History</b>	3.1.0000	
<b>Role</b>	admin	
<b>Example</b>	<pre>switch (config) # clock set 23:23:23 2010/08/19 switch (config) # show clock Time:      23:23:26 Date:      2010/08/19 Time zone: UTC           (Etc/UTC) UTC offset: same as UTC switch (config) #</pre>	
<b>Related Commands</b>	show clock	
<b>Notes</b>	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).

<b>Syntax Description</b>	zone word	The possible forms this could take include: continent, city, continent, country, city, continent, region, country, city, ocean, and/or island.
<b>Default</b>	GMT	
<b>Configuration Mode</b>	Config	
<b>History</b>	3.1.0000	
<b>Role</b>	admin	
<b>Example</b>	<pre>switch (config) # clock timezone America North United_States Other New_York switch (config) # show clock Time:      10:08:53 Date:      2015/10/29 Time zone: America North United_States Other New_York (America/New_York) UTC offset: -0400 (UTC minus 4 hours) switch (config) #</pre>	
<b>Related Commands</b>	show clock	
<b>Notes</b>		

## 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.

<b>Syntax Description</b>	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
<b>Default</b>	NTP is enabled NTP version number is 4	
<b>Configuration Mode</b>	Config	
<b>History</b>	3.1.0000	
<b>Role</b>	admin	
<b>Example</b>	<pre>switch (config) # no ntp peer 192.168.10.24 disable switch (config) #</pre>	
<b>Related Commands</b>	N/A	
<b>Notes</b>		

## ntpdate

**ntpdate <IP address>**

Sets the system clock using the specified SNTP server.

<b>Syntax Description</b>	IP address	IP.
<b>Default</b>	N/A	
<b>Configuration Mode</b>	Config	
<b>History</b>	3.1.0000	
<b>Role</b>	admin	
<b>Example</b>	<pre>switch (config) # ntpdate 192.168.10.10 26 Feb 17:25:40 ntpdate[15206]: adjust time server 192.168.10.10 offset -0.000092 sec switch (config) #</pre>	
<b>Related Commands</b>	N/A	
<b>Notes</b>	<p>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.</p>	

## 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
<b>Default</b>	Disabled	
<b>Configuration Mode</b>	Config	
<b>History</b>	3.5.0200	
<b>Role</b>	admin	
<b>Example</b>	switch (config) # ntp authenticate	
<b>Related Commands</b>	N/A	
<b>Notes</b>		

## 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.

<b>Syntax Description</b>	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
<b>Default</b>	Disabled	
<b>Configuration Mode</b>	Config	
<b>History</b>	3.5.0200	
<b>Role</b>	admin	
<b>Example</b>	<pre>switch (config) # ntp authentication-key 123 md5 examplepass switch (config) # ntp authentication-key 1234 sha1 Password: ** Confirm: ** switch (config) #</pre>	
<b>Related Commands</b>	N/A	
<b>Notes</b>	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.

<b>Syntax Description</b>	ip_address	IP address of the peer. IPv4, IPv6 and hostname (FQDN) are acceptable.
<b>Default</b>	Disabled	
<b>Configuration Mode</b>	Config	
<b>History</b>	3.5.0200	
	3.6.4000	Added hostname as option for ip_address, and added Notes.
<b>Role</b>	admin	
<b>Example</b>	<pre>switch (config) # ntp peer 10.10.10.10 disable switch (config) #</pre>	
<b>Related Commands</b>	N/A	
<b>Notes</b>	<ul style="list-style-type: none"><li>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').</li><li>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.</li></ul>	

## 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.

<b>Syntax Description</b>	ip_address	IP address of the peer. IPv4, IPv6 and hostname (FQDN) are acceptable.
	key_id	Range: 1-65534
<b>Default</b>	Disabled	
<b>Configuration Mode</b>	Config	
<b>History</b>	3.5.0200	
	3.6.4000	Added hostname as ip_address option and added Notes.
<b>Role</b>	admin	
<b>Example</b>	switch (config) # ntp peer 10.10.10.10 keyID 120	
<b>Related Commands</b>	N/A	
<b>Notes</b>	<ul style="list-style-type: none"> <li>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').</li> <li>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.</li> </ul>	

## 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.

<b>Syntax Description</b>	ip_address	IP address of the peer. IPv4, IPv6 and hostname (FQDN) are acceptable.
	ver_num	NTP version (3 or 4)
<b>Default</b>	4	
<b>Configuration Mode</b>	Config	
<b>History</b>	3.5.0200	
	3.6.4000	Added hostname as ip_address option and added Notes.
<b>Role</b>	admin	
<b>Example</b>	switch (config) # ntp peer 10.10.10.10 version 4	
<b>Related Commands</b>	N/A	
<b>Notes</b>	<ul style="list-style-type: none"><li>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').</li><li>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.</li></ul>	

## 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.

<b>Syntax Description</b>	ip_address	IP address of the peer. IPv4, IPv6 and hostname (FQDN) are acceptable.
<b>Default</b>	Disabled	
<b>Configuration Mode</b>	Config	
<b>History</b>	3.5.0000	
	3.6.4000	Added hostname as ip_address option and added Notes.
<b>Role</b>	admin	
<b>Example</b>	<pre>switch (config) # ntp server 10.10.10.10 disable switch (config) #</pre>	
<b>Related Commands</b>	N/A	
<b>Notes</b>	<ul style="list-style-type: none"><li>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').</li><li>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.</li></ul>	

## 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.

<b>Syntax Description</b>	ip_address	IP address of the peer. IPv4, IPv6 and hostname (FQDN) are acceptable.
	key_id	Range: 1-65534
<b>Default</b>	Disabled	
<b>Configuration Mode</b>	Config	
<b>History</b>	3.5.0200	
	3.6.4000	Added hostname as ip_address option and added Notes.
<b>Role</b>	admin	
<b>Example</b>	switch (config) # ntp server 10.10.10.10 keyID 120	
<b>Related Commands</b>	N/A	
<b>Notes</b>	<ul style="list-style-type: none"><li>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').</li><li>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.</li></ul>	

## 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

<b>Syntax Description</b>	ip_address	IP address of the peer. IPv4, IPv6 and hostname (FQDN) are acceptable.
<b>Default</b>	N/A	
<b>Configuration Mode</b>	Config	
<b>History</b>	3.6.2002	
	3.6.4000	Added hostname as ip_address option and added Notes.
<b>Role</b>	admin	
<b>Example</b>	switch (config) # ntp server 10.10.10.10 trusted-enable	
<b>Related Commands</b>	N/A	
<b>Notes</b>	<ul style="list-style-type: none"><li>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').</li><li>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.</li><li>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.</li></ul>	

## 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.

<b>Syntax Description</b>	ip_address	IP address of the peer. IPv4, IPv6 and hostname (FQDN) are acceptable.
	ver_num	NTP version (3 or 4)
<b>Default</b>	4	
<b>Configuration Mode</b>	Config	
<b>History</b>	3.5.0200	
	3.6.4000	Added hostname as ip_address option and added Notes.
<b>Role</b>	admin	
<b>Example</b>	switch (config) # ntp server 10.10.10.10 version 4	
<b>Related Commands</b>	N/A	
<b>Notes</b>	<ul style="list-style-type: none"><li>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').</li><li>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.</li></ul>	

## 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.

<b>Syntax Description</b>	key(s)	Range: 1-65534.
<b>Default</b>	Disabled	
<b>Configuration Mode</b>	Config	
<b>History</b>	3.5.0200	
<b>Role</b>	admin	
<b>Example</b>	switch (config) # ntp trusted-key 1,3,5 switch (config) # ntp trusted-key 1-5	
<b>Related Commands</b>	ntp authentication-key	
<b>Notes</b>	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.

<b>Syntax Description</b>	N/A
<b>Default</b>	N/A
<b>Configuration Mode</b>	Any Command Mode
<b>History</b>	3.1.0000
<b>Role</b>	admin
<b>Example</b>	<pre>switch (config) # show clock Time: 04:21:44 Date: 2012/02/26 Time zone: America North_United_States Other New_York switch (config) #</pre>
<b>Related Commands</b>	N/A
<b>Notes</b>	

## show ntp

**show ntp**

Displays the current NTP settings.

<b>Syntax Description</b>	N/A
<b>Default</b>	N/A
<b>Configuration Mode</b>	Any Command Mode
<b>History</b>	3.1.0000 3.5.0200                          Updated Example
<b>Role</b>	admin
<b>Example</b>	<pre>switch (config) # show ntp NTP is administratively enabled. NTP Authentication is administratively disabled. Clock is synchronized. Reference: 10.134.46.4. Offset: -9.605 ms. Active servers and peers:  10.1.1.1 Conf Type : dual Status : pending Stratum : 16 Offset(msec) : 0.000 Ref clock : .INIT. Poll Interval (sec): 64 Last Response (sec): N/A Auth state : none  10.134.46.4 Conf Type : serv Status : sys.peer(*) Stratum : 4 Offset(msec) : -9.605 Ref clock : 10.7.77.134 Poll Interval (sec): 64 Last Response (sec): 55 Auth state : none  switch (config) #</pre>
<b>Related Commands</b>	N/A
<b>Notes</b>	

## show ntp configured

### show ntp configured

Displays NTP configuration.

<b>Syntax Description</b>	N/A
<b>Default</b>	N/A
<b>Configuration Mode</b>	Any Command Mode
<b>History</b>	3.5.0200
<b>Role</b>	admin
<b>Example</b>	<pre>switch (config) # show ntp configured NTP enabled: yes NTP Authentication enabled: no No NTP peers configured. NTP server 10.10.10.10     Enabled: yes     NTP version: 4     Key ID: none switch (config) #</pre>
<b>Related Commands</b>	N/A
<b>Notes</b>	

## show ntp keys

### show ntp configured

Displays NTP keys.

<b>Syntax Description</b>	N/A
<b>Default</b>	N/A
<b>Configuration Mode</b>	Any Command Mode
<b>History</b>	3.5.0200
<b>Role</b>	admin
<b>Example</b>	<pre>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) #</pre>
<b>Related Commands</b>	N/A
<b>Notes</b>	

## 4.3 PTP

Synchronizing network applications require their wall clock time to be aligned precisely with a reference time source (to the order of micro seconds or less). To achieve such accuracy, the application needs the support of networking HW (switch and NIC), to provide the means to stamp time sensitive packets. It also requires a time synchronization protocol which would make use of the HW time stamping to adjust its wall clock time to an accurate clock in the network.

### 4.3.1 Precision Time Protocol Principles

The basic principle of PTP is as follows: Slave time = master time + propagation delay + offset.

The purpose of the protocol is to align the slave and the master time so that the gap between them is the propagation delay of the packet. Or in other words, the purpose of the protocol is to use the offset to correct the slave time so the offset between the master sending the packet and the slave receiving the packet is the propagation delay.

Master time is sent periodically by a reliable clock source named Master Clock (MC). In a PTP network, one single reference source is elected called Grand Master Clock (GMC). Propagation delay is calculated between each node and the MC by one of the two methods provided by the standard and further explained below.

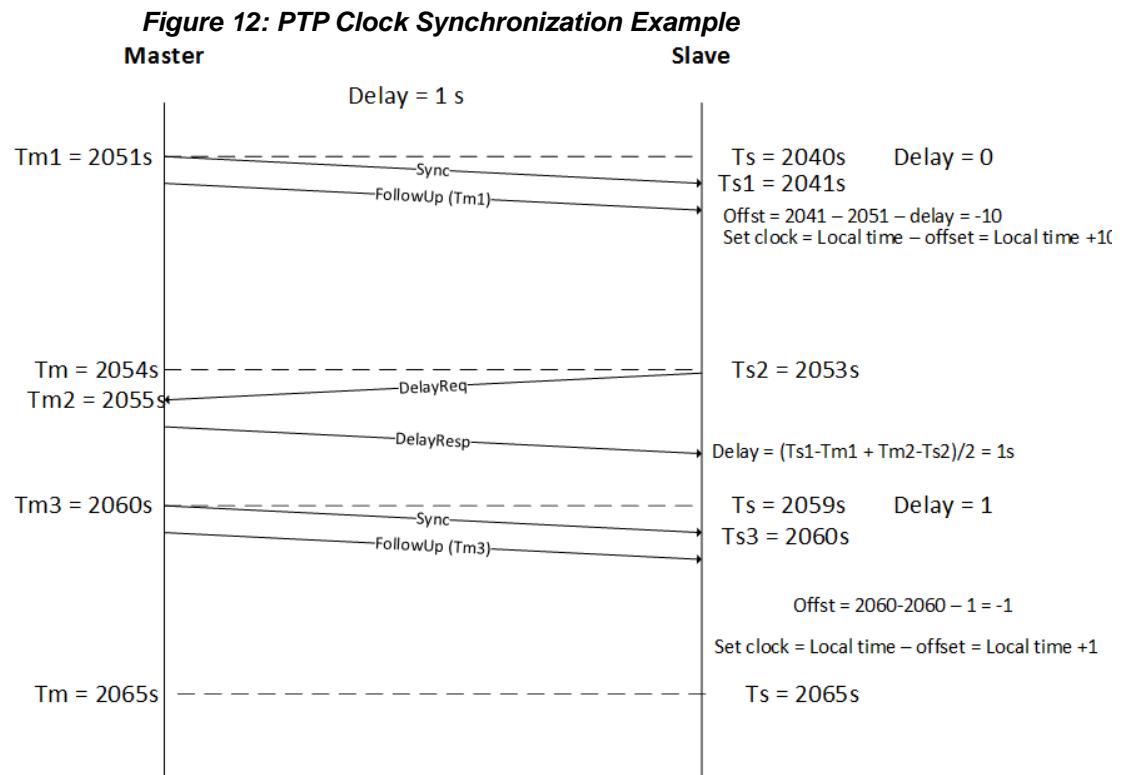
To reach sub-micro second resolutions, all the time stamps which record when a packet is sent and received should be done in the HW. This may impose interaction between SW and HW to query the HW time and send follow-up messages. This issue is further explained below in 2 step section.

Assuming that the propagation delay in the network is symmetric, the propagation time is the average time that took the sync and delay req messages to be switched.

$$\text{Propagation delay} = (T4-T1-(T3-T2))/2 = (T4-T1+T2-T3)/2$$

T1 represents the time that the packet left the master which is actually the master time.

Figure 12 provides an example of the stages required by a slave clock to align its time to the master clock:



**Table 25 - PTP Message Formats**

Message Type	Hex Value	Class
Sync	0	Event
Follow-up	8	General
Delay_Req	1	Event
Delay_Resp	9	General
Pdelay_Req	2	Event
Pdelay_Resp	3	Event
Pdelay_Resp followup	A	General
Announce	B	General
Signaling	C	General
Management	D	General

#### 4.3.2 Clock Types and Operation Modes

The types of clocks available are as follows:

- Grand Master Clock (GMC) – the reference time source derived from an accurate clock such as a GNSS driven clock (i.e. GPS, GLONASS, GALILEO)
- Boundary Clock (BC) – a network device that acts as slave to its master and as master to its slaves. (Mellanox implements only this)
- Ordinary Clock (OC) – a clock that operates either as a Master or a Slave. In the case of a slave, the end point whose clock is been synced (normally a host/server).
- Master Clock (MC) – a clock which operates as a Master and derives its timing capabilities from the clock chain up to the GMC. It typically serves as a port on a BC connected to a host running as a slave.
- Transparent Clock (TC) – a PTP aware switch capable of measuring the PTP packet switching delay (transient time) and updating the data in the packet. In peer-to-peer (P2P) delay calculation mechanism, a TC device is also required to calculate its delay from the next hop toward the MC and add the value to the switching delay.

Two modes of delay calculations are defined:

- End-to-End (E2E) – each slave calculates its delay from the MC by running Delay request/ delay response sequence (Mellanox implements only this)
- Peer-to-Peer – propagation delay (Pdelay) is calculated periodically on each link between the slave and the MC independently. The time synchronization packet sent from the MC to all the slaves in the network is updated by each of the downstream nodes with both switching delay (the time that the packet traversed the switch) and upstream hop Pdelay.

### 4.3.3 PTP Domains

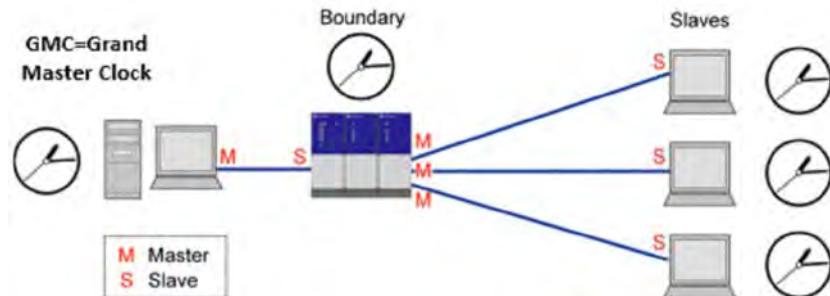
A domain consists of one or more PTP devices communicating with each other. PTP domain defines the scope of PTP message communication, state, operations, data sets, and timescale.

#### 4.3.3.1 Boundary Clock

In a full E2E PTP deployment, the GMC needs to respond to each slave's delay request message. A normal profile of PTP may require few delay calculations per second. An average GMC is capable of addressing few thousands of messages per second. This imposes that direct slave/GMC communication limits the number of overall OCs to ~8K. To scale beyond that, there is a need for a hierarchy between the GMC and the slave. This is achieved by implementing BC, either in the TOR switches or on all the switches in the DC.

Figure 13 shows the master/slave role that a boundary clock implements between the MC and the Slave (OC).

**Figure 13: Boundary Clock Master/Slave Functionality**



Each BC acts as a slave towards the GMC and as GMC to its local slaves. Although adding a BC device introduces accuracy degradation as explained above, it becomes mandatory when the number of slaves on a single MC exceeds few thousand devices.

Another use of BC is to bridge between networks. When running PTP over native Ethernet packets, to create larger PTP domains, there is a need to bridge between the broadcast domains. This is done by BC switches.

**Table 26 - Default PTP Profile Attributes**

Name	Range	Default
Announce interval	-3 (0.125s), 1 (2s)	-2 (0.25s)
Announce timeout interval	2, 10	3
Sync interval (logSyncInt)	-7, -1	-3
Delay request interval	logSyncInt, logSyncInt +5	logSyncInt
PTP domain	0, 127	127
Priority 1	0, 255	128
Priority 2	0, 255	128

#### 4.3.4 Commands

##### protocol ptp

**protocol ptp**

Enables PTP on the switch.

<b>Syntax Description</b>	N/A
<b>Default</b>	N/A
<b>Configuration Mode</b>	Config
<b>History</b>	3.6.4110
<b>Role</b>	admin
<b>Example</b>	<pre>switch (config) # protocol ptp ... switch (config) #</pre>
<b>Related Commands</b>	N/A
<b>Notes</b>	

## ptp domain

**ptp domain <domain number>**

Inserts the number of ptp domain.

<b>Syntax Description</b>	domain number	Range: 0-127
<b>Default</b>	N/A	
<b>Configuration Mode</b>	Config	
<b>History</b>	3.6.4110	
<b>Role</b>	admin	
<b>Example</b>	<pre>switch (config) # ptp domain ... switch (config) #</pre>	
<b>Related Commands</b>	N/A	
<b>Notes</b>		

## ptp priority

**ptp priority{1 | 2} <priority>**

Configures PTP primary priority.

<b>Syntax Description</b>	priority	Range: 0-255
<b>Default</b>	N/A	
<b>Configuration Mode</b>	Config	
<b>History</b>	3.6.4110	
<b>Role</b>	admin	
<b>Example</b>	<pre>switch (config) # ptp priority1 128 ... switch (config) #</pre>	
<b>Related Commands</b>	N/A	
<b>Notes</b>		

## ptp enable

### ptp enable

Enables PTP per interface.

<b>Syntax Description</b>	N/A
<b>Default</b>	N/A
<b>Configuration Mode</b>	Config Interface Ethernet
<b>History</b>	3.6.4110
<b>Role</b>	admin
<b>Example</b>	<pre>switch (config interface ethernet 1/1) # ptp enable ... switch (config interface ethernet 1/1) #</pre>
<b>Related Commands</b>	N/A
<b>Notes</b>	

## ptp announce interval

**ptp announce interval <interval>**

Configures PTP announce interval.

<b>Syntax Description</b>	interval	Range: -3 to 1
<b>Default</b>	N/A	
<b>Configuration Mode</b>	Config Interface Ethernet	
<b>History</b>	3.6.4110	
<b>Role</b>	admin	
<b>Example</b>	<pre>switch (config interface ethernet 1/1) # ptp announce interval -2 ... switch (config interface ethernet 1/1) #</pre>	
<b>Related Commands</b>	N/A	
<b>Notes</b>		

## ptp announce timeout

**ptp announce timeout <timeout>**

Configures PTP announce timeout.

<b>Syntax Description</b>	timeout	Range: 2-10
<b>Default</b>	N/A	
<b>Configuration Mode</b>	Config Interface Ethernet	
<b>History</b>	3.6.4110	
<b>Role</b>	admin	
<b>Example</b>	<pre>switch (config interface ethernet 1/1) # ptp announce timeout 3 ... switch (config interface ethernet 1/1) #</pre>	
<b>Related Commands</b>	N/A	
<b>Notes</b>		

## ptp delay-req interval

**ptp delay-req interval <interval>**

Configures PTP delay-req interval.

<b>Syntax Description</b>	interval	Range is LogSyncInt -7 to 7
<b>Default</b>	N/A	
<b>Configuration Mode</b>	Config Interface Ethernet	
<b>History</b>	3.6.4110	
<b>Role</b>	admin	
<b>Example</b>	<pre>switch (config interface ethernet 1/1) # ptp delay-req interval -3 ... switch (config interface ethernet 1/1) #</pre>	
<b>Related Commands</b>	N/A	
<b>Notes</b>		

## ptp sync interval

**ptp sync interval <interval>**

Configures PTP sync interval.

<b>Syntax Description</b>	interval	Range: -1 to -7
<b>Default</b>	N/A	
<b>Configuration Mode</b>	Config Interface Ethernet	
<b>History</b>	3.6.4110	
<b>Role</b>	admin	
<b>Example</b>	<pre>switch (config interface ethernet 1/1) # ptp sync interval -3 ... switch (config interface ethernet 1/1) #</pre>	
<b>Related Commands</b>	N/A	
<b>Notes</b>		

## show ptp

**show ptp**

Displays PTP configuration and operation data.

<b>Syntax Description</b>	N/A
<b>Default</b>	N/A
<b>Configuration Mode</b>	Any Command Mode
<b>History</b>	3.6.4110
<b>Role</b>	admin
<b>Example</b>	<pre>switch (config) # show ptp PTP mode:                               Boundary Clock Domain:                                  127 Clock identity:                         e41d2d.ffffe.46f801 GMC identity:                           000102.ffffe.030405 Number of master ports:                 0 Slave port interface:                  Eth1/1 PTP enabled interfaces: Name      Role -----  ----- Eth1/1    SLAVE . .</pre>
<b>Related Commands</b>	N/A
<b>Notes</b>	

## show ptp clock

### show ptp clock

Displays configuration and operation data of PTP clock.

<b>Syntax Description</b>	N/A
<b>Default</b>	N/A
<b>Configuration Mode</b>	Any Command Mode
<b>History</b>	3.6.4110
<b>Role</b>	admin
<b>Example</b>	<pre>switch (config) # show ptp clock Domain: 127 Number of PTP ports: 1 Priority1: 128 Priority2: 128 Clock identity: e41d2d.ffffe.46f801 Offset From Master (ns): 65535 Mean path delay (ns): 13303808 Clock Quality Class: 248 Accuracy: 254 Offset (log variance): 65535 Steps Removed from GMC: 1 Local clock time: 13:59:27 Etc/UTC 2017/05/23</pre>
<p style="text-align: center;">...</p>	
<b>Related Commands</b>	N/A
<b>Notes</b>	

## show ptp clock parent

### show ptp clock parent

Displays configuration and operation data of parent PTP clock.

<b>Syntax Description</b>	N/A
<b>Default</b>	N/A
<b>Configuration Mode</b>	Any Command Mode
<b>History</b>	3.6.4110
<b>Role</b>	admin
<b>Example</b>	<pre>switch (config) # show ptp clock parent Parent Clock Parent Clock identity: 7cfe90.ffffe.fa2141 Parent Port number: 2  GMC GMC Identity: 7cfe90.ffffe.fa2141  GMC Clock Quality Priority1: 128 Priority2: 128 Class: 248 Accuracy: 254 Offset (log variance): 65535</pre> <p>...</p>
<b>Related Commands</b>	N/A
<b>Notes</b>	

## show ptp interface ethernet

**show ptp interface ethernet <number>**

Displays PTP configuration and operation data, per interface.

<b>Syntax Description</b>	number	Port ID
<b>Default</b>	N/A	
<b>Configuration Mode</b>	Any Command Mode	
<b>History</b>	3.6.4110	
<b>Role</b>	admin	
<b>Example</b>	<pre>switch (config) # show ptp interface ethernet 1/1 Interface name:                                Eth1/1 Port Clock identity:                            7cfe90.ffff.ea21c1 PTP Port number:                               1 PTP interface state:                           SLAVE Delay request interval(log mean):            -3 Announce receipt time out:                   3 Announce interval(log mean):                 -2 Sync interval(log mean):                      -3 Delay Mechanism:                             End to End Transport protocol:                          UDP IPv4</pre>	
...		
<b>Related Commands</b>	N/A	
<b>Notes</b>		

## show ptp interface ethernet counters

**show ptp interface ethernet <number> counters**

Displays PTP counters, per interface.

<b>Syntax Description</b>	number	Port ID
<b>Default</b>	N/A	
<b>Configuration Mode</b>	Any Command Mode	
<b>History</b>	3.6.4110	
<b>Role</b>	admin	
<b>Example</b>	<pre>switch (config) # show ptp interface ethernet 1/5 counters Eth1/5 RX 108      Sync message count 0        Delay request message count 0        PDelay request message count 0        PDelay response message count 108      Follow Up message count 17       Delay response message count 0        PDelay response follow Up message count 54       Announce message count 0        Signalling message count 0        Management message count  TX 74188    Sync message count 17       Delay request message count 0        PDelay request message count 0        PDelay response message count 74188    Follow Up message count 0        Delay response message count 0        PDelay response follow Up message count 37117    Announce message count 0        Signalling message count 57       Management message count  ... </pre>	
<b>Related Commands</b>	N/A	
<b>Notes</b>		

## 4.4 Software Management

### 4.4.1 Upgrading MLNX-OS Software



When upgrading from a software version older than 3.2.0100 to software version 3.3.0000 or higher, the upgrade procedure must be done in two steps. First update the software to 3.2.0506 , then update to the desired software version.



The system being upgraded becomes indisposed throughout the upgrade procedure.



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



To upgrade the MLNX-OS version on a gateway, SM, or MLAG cluster, please refer to Section 4.4.2, “Upgrading MLNX-OS HA Groups,” on page 230.



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

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

**Step 1.** Change to Config mode.

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

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

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

Partition 1:
SX_PPC_M460EX 3.3.3130 2013-03-20 21:32:25 ppc

Partition 2:
SX_PPC_M460EX 3.3.3130 2013-03-20 21:32:25 ppc

Images available to be installed:
```

```
image-PPC_M460EX-SX_3.3.3256.img
SX_PPC_M460EX 3.3.3256 2013-03-20 21:32:25 ppc

Serve image files via HTTP/HTTPS: no

No image install currently in progress.

Boot manager password is set.

No image install currently in progress.

Require trusted signature in image being installed: yes (default)
switch (config) #
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 3.6.4110-12 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)
M2100-106 [standalone: master] (config) #
```

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

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



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

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

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

**Step 5.** Display the available images.



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

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

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

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

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

Serve image files via HTTP/HTTPS: no

No image install currently in progress.

Boot manager password is set.

No image install currently in progress.

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

**Step 6.** Install the new image.

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

```
100.0% [#####
switch (config) #
```



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

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

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

- Step 8.** Run show images to review your images. Run:

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

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

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

Last boot partition: 1
Next boot partition: 2

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

- Step 9.** Save current configuration. Run:

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

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

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



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



In order to upgrade the system on dual management system refer to Section 4.4.1, “Upgrading MLNX-OS Software,” on page 226.



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).

#### 4.4.2 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 MLAG. Run:

```
switch (config)# show mlag-vip
MLAG VIP
=====
MLAG group name: my-mlag-group
MLAG VIP address: 1.1.1.1/30
Active nodes: 2

Hostname          VIP-State      IP Address
-----
SwitchA          master        10.10.10.1
SwitchB          standby       10.10.10.2
```

**Step 2.** Upgrade standby nodes in the HA group according to steps 1-10 in section [Section 4.4.1, on page 226](#).

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

**Step 4.** Upgrade the master node in the HA group according to steps 1-10 in section [Section 4.4.1, on page 226](#).

#### 4.4.3 Deleting Unused Images

➤ ***To delete unused images:***

**Step 1.** Enter Config mode. Run:

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

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

```
switch (config) # show images
Images available to be installed:
```

```
image-PPC_M460EX-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.

#### 4.4.4 Downgrading MLNX-OS® Software

##### IMPORTANT NOTE

If in possession of an MSX1xxx or MSX6xxx switch system housing a SwitchX®-2 IC, then the oldest MLNX-OS version to which you may downgrade is 3.3.5006; otherwise, the switch system will malfunction.

To find out whether your system is based on SwitchX®-2, please run the command “show inventory” and make sure that the “Asic Rev” column of the MGMT indicates “2”.

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.

#### 4.4.4.1 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/SupportLogin> and 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%[######################################## #####]
```

#### 4.4.4.2 Downgrading Image



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

- Step 1.** Log in as admin.

- Step 2.** Enter config mode. Run:

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

- Step 3.** 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
```

#### 4.4.4.3 Switching to Partition with Older Software Version

The system saves a backup configuration file when upgrading from an older software version to a newer one. If the system returns to the older software partition, it uses this backup configuration file.



##### \*\*\*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 than 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
```

#### 4.4.5 Upgrading System Firmware

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

##### 4.4.5.1 After Updating MLNX-OS Software

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

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



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

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

Some subsystems are not updated with a default firmware.



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

#### 4.4.5.2 Importing Firmware and Changing the Default Firmware

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

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

**Step 2.** Save the configuration. Run:

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

**Step 3.** Reboot the system to enable auto update.

#### 4.4.6 Image Maintenance via Mellanox ONIE



Supported only on MSX1710-BS2F2O, and Mellanox Spectrum™ based switch systems.

ONIE is an “open compute” Open Network Install Environment for bare metal network switches. ONIE enables a bare metal network switch ecosystem where end-users have a choice among different network operating systems.

MLNX-OS® is distributed in way that allows installation on an ONIE environment. Certain Mellanox switch models come pre-installed with ONIE and MLNX-OS and support changing to a different operating system (OS).

➤ **To change the switch system’s OS:**

- Step 1.** Reboot the switch and wait for it to reach the GRUB menu:

```
GNU GRUB version 2.02
```

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

- Step 2.** Select the ONIE option using the arrow keys. The following message appears:

```
Due to security constraints, this option will uninstall your current MLNX OS system.
Are you sure ?
```

- Step 3.** Type YES to continue.

Since MLNX-OS is being uninstalled and deleted from the hard drive, the process takes a few hours. After this is finished, the system reboots into the ONIE shell and auto discovery begins.

```
Info: Fetching tftp://<ip-address>/7C-FE-90-5E-6A-4A/onie-installer-x86_64-mlnx_x86-
r5.0.1400 ...
Failure: Unable to find installer: /installer
Info: Fetching tftp://<ip-address>/0AE016FB/onie-installer-x86_64-mlnx_x86-r5.0.1400
...
Failure: Unable to find installer: /installer
Info: Fetching tftp://<ip-address>/0AE016F/onie-installer-x86_64-mlnx_x86-r5.0.1400
...
...
```

- Step 4.** In order to manually insert an install URL, press Enter and insert the command “install\_url <http> / <tftp> <url> <image name .bin>”. For example:

```
install_url http://<ip_address>/sx_mlnx_os/sx_mlnx_os-3.5.1000-21/X86_64/X86_64-
3.5.1000-21-installer.bin
```

Once you hit Enter, you have about 4 second to insert the command so it is recommended to prepare the command in advance and simply pasting it in. At this stage, the OS installation begins.

- Step 5.** Wait for the installation to end and reboot this switch to boot into the OS.

```
ONIE:/ # install_url http://<ip_address>/sx_mlnx_os/sx_mlnx_os-3.5.1000-21/X86_64/X86_64-3.5.1000-21-installer.bin
Stopping: discover... done.
down.
ONIE: eth1: link down. Skipping configuration.
ONIE: Failed to configure eth1 interface
Info: Fetching http://<ip_address>/sx_mlnx_os/sx_mlnx_os-3.5.1000-21/X86_64/X86_64-3.5.1000-21-installer.bin ...
Connecting to <ip_address>
installer          100% |*****| 392M 0:00:00 ETA
ONIE: Executing installer: http://<ip_address>/sx_mlnx_os/sx_mlnx_os-3.5.1000-21/X86_64/X86_64-3.5.1000-21-installer.bin
```

## 4.4.7 Commands

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

### image boot

**image boot {location <location ID> | next}**

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

<b>Syntax Description</b>	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.
<b>Default</b>	N/A	
<b>Configuration Mode</b>	enable/config	
<b>History</b>	3.1.0000	
<b>Role</b>	admin	
<b>Example</b>	switch (config) # image boot location 2 switch (config) #	
<b>Related Commands</b>	show images	
<b>Notes</b>		

## 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.

<b>Syntax Description</b>	N/A
<b>Default</b>	N/A
<b>Configuration Mode</b>	Config
<b>History</b>	3.2.0506
<b>Role</b>	admin
<b>Example</b>	<pre>switch (config) # boot next fallback-reboot enable switch (config) #</pre>
<b>Related Commands</b>	show images
<b>Notes</b>	<ul style="list-style-type: none"><li>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.</li><li>The no form of this command tells the system not to do that <b>only</b> for the next boot. In other words, this setting is not persistent, and goes back to enabled automatically after each boot.</li><li>When downgrading to an older software version which has never been run yet on a system, the “fallback reboot” <b>always</b> happens, unless the command “no boot next fallback-reboot enable” is used. However, this also happens when the older software version <i>has</i> been run before, but the configuration file has been switched since upgrading. In general, a downgrade only works (without having the fallback reboot forcibly disabled) if the process can find a snapshot of the configuration file (by the same name as the currently active one) which was taken before upgrading from the older software version. If that is not found, a fallback reboot is performed in preference to falling back to the initial database because the latter generally involves a loss of network connectivity, and avoiding that is of paramount importance.</li></ul>

## 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.

<b>Syntax Description</b>	location	Specifies location from which to boot system <ul style="list-style-type: none"><li>• 1 – installs to location 1</li><li>• 2 – installs to location 2</li></ul>
	next	Boots system from next location after one currently booted
<b>Default</b>	N/A	
<b>Configuration Mode</b>	Config	
<b>History</b>	3.2.0506	
<b>Role</b>	admin	
<b>Example</b>	<pre>switch (config) # boot system location 2 switch (config) #</pre>	
<b>Related Commands</b>	show images	
<b>Notes</b>		

## image default-chip-fw

**image default-chip-fw <file name>**

Sets the default firmware package to be installed.

<b>Syntax Description</b>	filename	Specifies the firmware filename.
<b>Default</b>	N/A	
<b>Configuration Mode</b>	Config	
<b>History</b>	3.1.0000	
<b>Role</b>	admin	
<b>Example</b>	switch (config) # image default-chip-fw fw-SX-rel-9_2_6440-FIT.mfa	
<b>Related Commands</b>	show asic-version show images	
<b>Notes</b>		

## image delete

**image delete <image name>**

Deletes the specified image file.

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

## image fetch

**image fetch <URL> [<filename>]**

Downloads an image from the specified URL or via SCP.

<b>Syntax Description</b>	URL  filename	HTTP, HTTPS, FTP, TFTP, SCP and SFTP are supported. Example: scp://username[:password]@hostname/path/filename.  Specifies a filename for this image to be stored as locally.
<b>Default</b>	N/A	
<b>Configuration Mode</b>	Config	
<b>History</b>	3.1.0000	
<b>Role</b>	admin	
<b>Example</b>	<pre>switch (config) # image fetch scp://&lt;username&gt;@192.168.10.125/var/www/ html/&lt;image_name&gt; Password ***** 100.0%[##### switch (config) #</pre> <p><u>Other options:</u></p> <pre>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</pre>	
<b>Related Commands</b>	show images	
<b>Notes</b>	<ul style="list-style-type: none"> <li>Please delete the previously available image, prior to fetching the new image</li> <li>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.</li> <li>See section “Upgrading MLNX-OS SX Software,” in the <i>Mellanox SwitchX® User Manual</i> for a full upgrade example</li> </ul>	

## image install

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

Installs the specified image file.

<b>Syntax Description</b>	<table border="0"> <tr> <td>image filename</td><td>Specifies the image name.</td></tr> <tr> <td>location ID</td><td>Specifies the image destination location.</td></tr> <tr> <td>prog-options</td><td> <ul style="list-style-type: none"> <li>• “no-track” overrides CLI default and does not track the installation progress</li> <li>• “track” overrides CLI default and tracks the installation progress</li> </ul> </td></tr> <tr> <td>ver-options</td><td> <ul style="list-style-type: none"> <li>• “check-sig” requires an image to have either a valid signature or no signature</li> <li>• “ignore-sig” allows unsigned or invalidly signed images to be installed</li> <li>• “require-sig” requires from the installed image to have a valid signature. If a valid signature is not found on the image, the image cannot be installed.</li> </ul> </td></tr> </table>	image filename	Specifies the image name.	location ID	Specifies the image destination location.	prog-options	<ul style="list-style-type: none"> <li>• “no-track” overrides CLI default and does not track the installation progress</li> <li>• “track” overrides CLI default and tracks the installation progress</li> </ul>	ver-options	<ul style="list-style-type: none"> <li>• “check-sig” requires an image to have either a valid signature or no signature</li> <li>• “ignore-sig” allows unsigned or invalidly signed images to be installed</li> <li>• “require-sig” requires from the installed image to have a valid signature. If a valid signature is not found on the image, the image cannot be installed.</li> </ul>
image filename	Specifies the image name.								
location ID	Specifies the image destination location.								
prog-options	<ul style="list-style-type: none"> <li>• “no-track” overrides CLI default and does not track the installation progress</li> <li>• “track” overrides CLI default and tracks the installation progress</li> </ul>								
ver-options	<ul style="list-style-type: none"> <li>• “check-sig” requires an image to have either a valid signature or no signature</li> <li>• “ignore-sig” allows unsigned or invalidly signed images to be installed</li> <li>• “require-sig” requires from the installed image to have a valid signature. If a valid signature is not found on the image, the image cannot be installed.</li> </ul>								
<b>Default</b>	N/A								
<b>Configuration Mode</b>	Config								
<b>History</b>	3.1.0000								
<b>Role</b>	admin								
<b>Example</b>	<pre>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) #</pre>								
<b>Related Commands</b>	show images								
<b>Notes</b>	<ul style="list-style-type: none"> <li>• The image cannot be installed on the “active” location (the one which is currently being booted)</li> <li>• On a two-location system, the location is chosen automatically if no location is specified</li> </ul>								

## image move

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

Renames the specified image file.

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

## image options

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

Configures options and defaults for image usage.

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

Syntax Description	require-sig	Requires images to be signed by a trusted signature
	serve all	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 require-sig	
Related Commands	show images	
Notes	<p>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.</p> <p>After running “serve all” the URLs where the images will be available are:</p> <ul style="list-style-type: none"><li>• http://&lt;HOSTNAME&gt;/system_images/&lt;FILENAME&gt;</li><li>• https://&lt;HOSTNAME&gt;/system_images/&lt;FILENAME&gt;</li></ul>	

## show bootvar

### show bootvar

Displays the installed system images and the boot parameters.

<b>Syntax Description</b>	N/A
<b>Default</b>	N/A
<b>Configuration Mode</b>	Config
<b>History</b>	3.1.0000
<b>Role</b>	admin
<b>Example</b>	<pre>switch (config) # show bootvar Installed images:   Partition 1:     SX_PPC_M460EX 3.0.0000-dev-HA 2012-01-22 08:47:59 ppc     Last dobincp: 2012/01/23 14:54:23    Partition 2:     SX_PPC_M460EX 3.0.0000-dev-HA 2012-01-18 09:52:41 ppc     Last dobincp: 2012/01/19 16:48:23    Last boot partition: 1   Next boot partition: 1    Boot manager password is set.    No image install currently in progress.    Image signing: trusted signature always required   Admin require signed images: yes    Settings for next boot only:     Fallback reboot on configuration failure: yes (default) switch (config) #</pre>
<b>Related Commands</b>	N/A
<b>Notes</b>	

## show images

### show image

Displays information about the system images and boot parameters.

<b>Syntax Description</b>	N/A
<b>Default</b>	N/A
<b>Configuration Mode</b>	Any Command Mode
<b>History</b>	3.1.0000
<b>Role</b>	admin
<b>Example</b>	<pre>switch (config) # show images Images available to be installed:   image-SX_PPC_M460EX-ppc-m460ex-20120122-084759.img   SX_PPC_M460EX 3.0.0000-dev-HA 2012-01-22 08:47:59 ppc  Installed images:   Partition 1:     SX_PPC_M460EX 3.0.0000-dev-HA 2012-01-22 08:47:59 ppc     Last dobincp: 2012/01/23 14:54:23    Partition 2:     SX_PPC_M460EX 3.0.0000-dev-HA 2012-01-18 09:52:41 ppc     Last dobincp: 2012/01/19 16:48:23    Last boot partition: 1   Next boot partition: 1    Boot manager password is set.    No image install currently in progress.    Image signing: trusted signature always required   Admin require signed images: yes    Settings for next boot only:     Fallback reboot on configuration failure: yes (default)   switch (config) #</pre>
<b>Related Commands</b>	N/A
<b>Notes</b>	

## 4.5 Configuration Management

### 4.5.1 Saving a Configuration File

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

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

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

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

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

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

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

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

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

### 4.5.2 Loading a Configuration File

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

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

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

### 4.5.3 Restoring Factory Default Configuration

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

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

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

### 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 performed 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.

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

## file stats

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

Manipulates statistics report files.

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

## file tcpdump

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

Manipulates tcpdump output files.

<b>Syntax Description</b>	delete <filename>  upload <filename> <URL>	Deletes the specified tcpdump output file.  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.
<b>Default</b>	N/A	
<b>Configuration Mode</b>	Config	
<b>History</b>	3.1.0000	
<b>Role</b>	admin	
<b>Example</b>	switch (config) # file tcpcdump delete my-tcpdump-file.txt switch (config) #	
<b>Related Commands</b>	show files stats tcpdump	
<b>Notes</b>		

## reload

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

Reboots or shuts down the system.

<b>Syntax Description</b>	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.
<b>Default</b>	N/A	
<b>Configuration Mode</b>	Config	
<b>History</b>	3.1.0000	
<b>Role</b>	admin	
<b>Example</b>	<pre>switch (config) # reload Configuration has been modified; save first? [yes] yes Configuration changes saved. ... switch (config) #</pre>	
<b>Related Commands</b>	reset factory	
<b>Notes</b>		

## 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.

<b>Syntax Description</b>	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
<b>Default</b>	N/A	
<b>Configuration Mode</b>	Config	
<b>History</b>	3.1.0000 3.4.0000 3.6.2002	Added notes and “keep-virt-vols” parameter  Updated Example and Notes
<b>Role</b>	admin	
<b>Example</b>	<pre>switch (config) # reset factory Warning - confirming will cause system reboot. Type 'YES' to confirm reset: YES Resetting and rebooting the system -- please wait... ...</pre>	
<b>Related Commands</b>	reload	
<b>Notes</b>	<ul style="list-style-type: none"> <li>Effects of parameter “keep-all-cofig”: Licenses – not deleted; profile – no change; configuration – unchanged; management IP – unchanged</li> <li>Effects of parameter “keep-basic”: Licenses – not deleted; profile – reset; configuration – reset; management IP – reset</li> <li>Effects of parameter “keep-virt-vols”: Licenses – deleted; profile – reset; configuration – reset; management IP – unchanged</li> <li>Confirming the command causes system reboot</li> </ul>	

## show files debug-dump

**show files debug-dump [<filename>]**

Displays a list of debug dump files.

<b>Syntax Description</b>	filename	Displays a summary of the contents of a particular debug dump file.
---------------------------	----------	---

<b>Default</b>	N/A
----------------	-----

<b>Configuration Mode</b>	Config
---------------------------	--------

<b>History</b>	3.1.0000
----------------	----------

<b>Role</b>	admin
-------------	-------

<b>Example</b>	<pre>switch (config) # show files debug-dump sysdump-switch-112104-20114052-091707.tgz System information:</pre>
----------------	--

```
Hostname: switch-112104
Version: SX_PPC 3.1.0000 2011-05-25 13:59:00 ppc
Date: 2012-01-26 09:17:07
Uptime: 0d 18h 47m 48s
```

```
=====
Output of 'uname -a':
```

```
Linux switch-112104 2.6.27-MELLANOXuni-m405ex SX_PPC 3.1.0000 #1 2012-01-25 13:59:00 ppc ppc
ppc GNU/Linux
```

```
=====
```

```
.....
switch (config) #
```

<b>Related Commands</b>	file debug-dump
-------------------------	-----------------

<b>Notes</b>
--------------

## show files stats

**show files stats <filename>**

Displays a list of statistics report files.

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

## show files system

### show files system [detail]

Displays usage information of the file systems on the system.

<b>Syntax Description</b>	detail	Displays more detailed information on file-system.
<b>Default</b>	N/A	
<b>Configuration Mode</b>	Config	
<b>History</b>	3.1.0000	
<b>Role</b>	admin	
<b>Example</b>	<pre>switch (config) # show files system Statistics for /config filesystem:   Bytes Total          100 MB   Bytes Used           3 MB   Bytes Free           97 MB   Bytes Percent Free  97%   Bytes Available     97 MB   Inodes Total         0   Inodes Used          0   Inodes Free          0   Inodes Percent Free 0%  Statistics for /var filesystem:   Bytes Total          860 MB   Bytes Used           209 MB   Bytes Free           651 MB   Bytes Percent Free  75%   Bytes Available     651 MB   Inodes Total         0   Inodes Used          0   Inodes Free          0   Inodes Percent Free 0% switch (config) #</pre>	
<b>Related Commands</b>	N/A	
<b>Notes</b>		

## show files tcpdump

### show files tcpdump

Displays a list of statistics report files.

<b>Syntax Description</b>	N/A
<b>Default</b>	N/A
<b>Configuration Mode</b>	Config
<b>History</b>	3.1.0000
<b>Role</b>	admin
<b>Example</b>	<pre>switch (config) # show files stats test dump3 switch (config) #</pre>
<b>Related Commands</b>	<a href="#">file tcpdump</a> <a href="#">tcpdump</a>
<b>Notes</b>	

#### 4.5.5.2 Configuration Files

##### configuration audit

**configuration audit max-changes <number>**

Chooses settings related to configuration change auditing.

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

## configuration copy

**configuration copy <source name> <dest name>**

Copies a configuration file.

<b>Syntax Description</b>	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.
<b>Default</b>	N/A	
<b>Configuration Mode</b>	Config	
<b>History</b>	3.1.0000	
<b>Role</b>	admin	
<b>Example</b>	<pre>switch (config) # configuration copy initial.bak example switch (config) #</pre>	
<b>Related Commands</b>		
<b>Notes</b>	<ul style="list-style-type: none"><li>• This command does not affect the current running configuration</li><li>• 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.</li></ul>	

## configuration delete

**configuration delete <filename>**

Deletes a configuration file.

<b>Syntax Description</b>	filename	Name of file to delete.
<b>Default</b>	N/A	
<b>Configuration Mode</b>	Config	
<b>History</b>	3.1.0000	
<b>Role</b>	admin	
<b>Example</b>	<pre>switch (config) # show configuration files example      initial      initial.bak    initial.prev switch (config) # configuration delete example switch (config) # show configuration files initial      initial.bak    initial.prev switch (config) #</pre>	
<b>Related Commands</b>	show configuration	
<b>Notes</b>	<ul style="list-style-type: none"><li>This command does not affect the current running configuration</li><li>The active configuration file may not be deleted</li></ul>	

## configuration fetch

**configuration fetch <URL> [<name>]**

Downloads a configuration file from a remote host.

<b>Syntax Description</b>	URL	HTTP, HTTPS, FTP, TFTP, SCP and SFTP are supported. Example: scp://username[:password]@hostname/path/filename.
	name	The configuration file name.
<b>Default</b>	N/A	
<b>Configuration Mode</b>	Config	
<b>History</b>	3.1.0000	
<b>Role</b>	admin	
<b>Example</b>	<pre>switch (config) # configuration fetch scp://root:password@192.168.10.125/tmp/conf1 switch (config) #</pre>	
<b>Related Commands</b>	configuration switch-to	
<b>Notes</b>	<ul style="list-style-type: none"><li>The downloaded file should not override the active configuration file, using the &lt;name&gt; parameter</li><li>If no name is specified for a configuration fetch, it is given the same name as it had on the server</li><li>No configuration file may have the name “active”</li></ul>	

## configuration jump-start

### configuration jump-start

Runs the initial-configuration wizard.

<b>Syntax Description</b>	N/A
<b>Default</b>	N/A
<b>Configuration Mode</b>	Config
<b>History</b>	3.1.0000
<b>Role</b>	admin
<b>Example</b>	<pre>switch (config) # configuration jump-start Mellanox configuration wizard Step 1: Hostname? [switch-3cc29c] Step 2: Use DHCP on mgmt0 interface? y Step 3: Admin password (Enter to leave unchanged)? You have entered the following information: 1. Hostname: switch-3cc29c 2. Use DHCP on mgmt0 interface: yes 3. Enable IPv6: yes 4. Enable IPv6 autoconfig (SLAAC) on mgmt0 interface: yes 53. Admin password (Enter to leave unchanged): (unchanged) To change an answer, enter the step number to return to. Otherwise hit &lt;enter&gt; to save changes and exit. Choice: Configuration changes saved. switch (config) #</pre>
<b>Related Commands</b>	N/A
<b>Notes</b>	<ul style="list-style-type: none"><li>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)</li><li>This command invokes the wizard on demand – see chapter “Initializing the Switch for the First Time” in the <i>MLNX-OS SwitchX User Manual</i></li></ul>

## configuration merge

**configuration merge <filename>**

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

<b>Syntax Description</b>	filename	Name of file from which to merge settings.
<b>Default</b>	N/A	
<b>Configuration Mode</b>	Config	
<b>History</b>	3.1.0000	
<b>Role</b>	admin	
<b>Example</b>	<pre>switch (config) # configuration merge new-config-file switch (config) #</pre>	
<b>Related Commands</b>		
<b>Notes</b>	<ul style="list-style-type: none"><li>• No configuration files are modified during this process</li><li>• The configuration name must be a non-active configuration file</li></ul>	

## configuration move

**configuration move <source name> <dest name>**

Moves a configuration file.

<b>Syntax Description</b>	source name	Old name of file to move.
	dest name	New name for moved file.
<b>Default</b>	N/A	
<b>Configuration Mode</b>	Config	
<b>History</b>	3.1.0000	
<b>Role</b>	admin	
<b>Example</b>	<pre>switch (config) # show configuration files example1      initial      initial.bak    initial.prev switch (config) # configuration move example1 example2 switch (config) # show configuration files example2      initial      initial.bak    initial.prev switch (config) #</pre>	
<b>Related Commands</b>	show configuration	
<b>Notes</b>	<ul style="list-style-type: none"><li>This command does not affect the current running configuration</li><li>The active configuration file may not be the target of a move</li></ul>	

## 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.

<b>Syntax Description</b>	filename factory keep-basic keep-connect	Names for new configuration file. Creates new file with only factory defaults. Keeps licenses and host keys. Keeps configuration necessary for connectivity (interfaces, routes, and ARP).
<b>Default</b>	Keeps licenses and host keys	
<b>Configuration Mode</b>	Config	
<b>History</b>	3.1.0000	
<b>Role</b>	admin	
<b>Example</b>	<pre>switch (config) # show configuration files initial      initial.bak  initial.prev switch (config) # configuration new example2 switch (config) # show configuration files example2    initial      initial.bak  initial.prev switch (config) #</pre>	
<b>Related Commands</b>	show configuration	
<b>Notes</b>		

## configuration switch-to

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

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

<b>Syntax Description</b>	no-reboot	Forces configuration change without rebooting the switch
<b>Default</b>	N/A	
<b>Configuration Mode</b>	Config	
<b>History</b>	3.1.0000	
	3.6.1002	Added “no-reboot” option
<b>Role</b>	admin	
<b>Example</b>	<pre>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) #</pre>	
<b>Related Commands</b>	show configuration files	
<b>Notes</b>	<ul style="list-style-type: none"><li>The current running configuration is lost and not automatically saved to the previous active configuration file.</li><li>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.</li></ul>	

## 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.

<b>Syntax Description</b>	apply	Applies the file to the running configuration (i.e. executes the commands in it). This option has the following parameters: <ul style="list-style-type: none"> <li>• <b>discard:</b> Does not keep downloaded configuration text file after applying it to the system</li> <li>• <b>fail-continue:</b> If applying commands, continues execution even if one of them fails</li> <li>• <b>overwrite:</b> If saving the file and the filename already exists, replaces the old file</li> <li>• <b>verbose:</b> Displays all commands being executed and their output instead of just those that get errors</li> </ul>
	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: <ul style="list-style-type: none"> <li>• <b>apply:</b> Applies the downloaded configuration to the running system</li> <li>• <b>filename:</b> Specifies filename for saving downloaded text file</li> </ul>
<b>Default</b>	N/A	
<b>Configuration Mode</b>	Config	
<b>History</b>	3.2.1000	
	3.2.3000	Updated command
<b>Role</b>	admin	
<b>Example</b>	switch (config) # configuration fetch text scp://username[:password]@hostname/path/filename	
<b>Related Commands</b>	N/A	
<b>Notes</b>		

## configuration text file

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

Performs operations on text-based configuration files.

<b>Syntax Description</b>	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.
<b>Default</b>	N/A	
<b>Configuration Mode</b>	Config	
<b>History</b>	3.1.0000	
<b>Role</b>	admin	
<b>Example</b>	<pre>switch (config) # configuration text file my-config-file delete switch (config) #</pre>	
<b>Related Commands</b>	show configuration files	
<b>Notes</b>		

## 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.

<b>Syntax Description</b>	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.
<b>Default</b>	N/A	
<b>Configuration Mode</b>	Config	
<b>History</b>	3.1.0000	
<b>Role</b>	admin	
<b>Example</b>	<pre>switch (config) # configuration text generate file initial.prev save example switch (config) # show configuration files initial (active) initial.prev initial.bak Active configuration: initial Unsaved changes: yes switch (config) #</pre>	
<b>Related Commands</b>	show configuration files	
<b>Notes</b>		

## 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.

<b>Syntax Description</b>	active	Upload the active configuration file.
<b>Default</b>	N/A	
<b>Configuration Mode</b>	Config	
<b>History</b>	3.1.0000	
<b>Role</b>	admin	
<b>Example</b>		<pre>switch (config) # configuration upload active scp://root:password@192.168.10.125/tmp/conf1 switch (config) #</pre>
<b>Related Commands</b>	N/A	
<b>Notes</b>	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.

<b>Syntax Description</b>	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
<b>Default</b>	N/A	
<b>Configuration Mode</b>	Config	
<b>History</b>	3.1.0000	
<b>Role</b>	admin	
<b>Example</b>	<pre>switch (config) # configuration write switch (config) #</pre>	
<b>Related Commands</b>	write	
<b>Notes</b>		

## write

**write {memory [local] | terminal}**

Saves or displays the running configuration.

<b>Syntax Description</b>	<table border="0"> <tr> <td>memory</td><td>Saves running configuration to the active configuration file. It is the same as “configuration write”.</td></tr> <tr> <td>local</td><td>Saves the running configuration only on the local node. It is the same as “configuration write local”.</td></tr> <tr> <td>terminal</td><td>Displays commands to recreate current running configuration. It is the same as “show running-config”.</td></tr> </table>	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”.
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”.						
<b>Default</b>	N/A						
<b>Configuration Mode</b>	Config						
<b>History</b>	3.1.0000						
<b>Role</b>	admin						
<b>Example</b>	<pre>switch (config) # write terminal ## ## Running database "initial" ## Generated at 20114/05/27 10:05:16 +0000 ## Hostname: switch ## ## ## Network interface configuration ## interface mgmt0 comment "" interface mgmt0 create interface mgmt0 dhcp interface mgmt0 display interface mgmt0 duplex auto interface mgmt0 mtu 1500 no interface mgmt0 shutdown interface mgmt0 speed auto no interface mgmt0 zeroconf ## ## Local user account configuration ## username a** capability admin no username a** disable username a** disable password ..... switch (config) #</pre>						
<b>Related Commands</b>	show running-config configuration write						
<b>Notes</b>							

## 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.

<b>Syntax Description</b>	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.
<b>Default</b>	N/A	
<b>Configuration Mode</b>	Config	
<b>History</b>	3.1.0000	
	3.3.5006	Removed “running full” and “full” parameters
<b>Role</b>	monitor/admin	
<b>Example</b>	<pre>switch (config) # show configuration ## ## Active saved database "newcon" ## Generated at 2014/05/25 10:18:52 +0000 ## Hostname: switch-3cc29c ## ## Network interface configuration ## interface mgmt0 comment "" interface mgmt0 create interface mgmt0 dhcp interface mgmt0 display interface mgmt0 duplex auto interface mgmt0 mtu 1500 no interface mgmt0 shutdown interface mgmt0 speed auto no interface mgmt0 zeroconf switch (config) #</pre>	

---

**Related Commands**

---

**Notes**

---

## show running-config

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

Displays commands to recreate current running configuration.

<b>Syntax Description</b>	expanded	Displays commands in expanded format without compressing ranges
	protocol	Only displays commands relating to the specified protocol
<b>Default</b>	N/A	
<b>Configuration Mode</b>	Config	
<b>History</b>	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
<b>Role</b>	monitor/admin	

---

**Example**

```
switch (config) # show running-config
##
## Running database "initial"
## Generated at 2016/08/03 17:28:18 +0000
## Hostname: tarantula-9
##

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

##
## MLAG protocol
##
protocol mlag

##
## Interface Ethernet configuration
##
interface mlag-port-channel 1-49
interface mlag-port-channel 53-56
interface port-channel 1
interface ethernet 1/1-1/43 mtu 9216 force
interface ethernet 1/49-1/56 mtu 9216 force
interface mlag-port-channel 1-42 mtu 9216 force
interface mlag-port-channel 49 mtu 9216 force
interface mlag-port-channel 53 mtu 9216 force
##
## Port forwarding mode configuration
##
interface ethernet 1/1 switchmode store-and-forward
interface ethernet 1/2 disable switchmode store-and-forward
interface port-channel 1 switchmode store-and-forward
interface port-channel 2 disable switchmode store-and-forward
fae switchmode verify
...
switch (config) #
```

---

**Related Commands**

---

**Notes**

## 4.6 Logging

### 4.6.1 Monitor

- *To print logging events to the terminal:*

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

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

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

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

To see a list of the events, refer to Table 27, “Supported Event Notifications and MIB Mapping,” on page 326.

### 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> priority <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.

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

## 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.

<b>Syntax Description</b>	syslog IPv4 address/host-name	IPv4 address/hostname of the remote syslog server. Hostname is limited to 64 characters
	log-level	<ul style="list-style-type: none"> <li>• alert – alert notification, action must be taken immediately</li> <li>• crit – critical condition</li> <li>• debug – debug level messages</li> <li>• emerg – system is unusable (emergency)</li> <li>• err – error condition</li> <li>• info – informational condition</li> <li>• none – disables the logging locally and remotely</li> <li>• notice – normal, but significant condition</li> <li>• warning – warning condition</li> </ul>
	class	Sets or removes a per-class override on the logging level. All classes which do not have an override set will use the global logging level set with “logging local <log level>”. Classes that do have an override will do as the override specifies. If “none” is specified for the log level, MLNX-OS will not log anything from this class. Classes available: <ul style="list-style-type: none"> <li>• iss-modules – protocol stack</li> <li>• mgmt-back – system management back-end</li> <li>• mgmt-core – system management core</li> <li>• mgmt-front – system management front-end</li> <li>• mlx-daemons – management daemons</li> <li>• sx-sdk – switch SDK</li> </ul>
	log-level	<ul style="list-style-type: none"> <li>• alert – alert notification, action must be taken immediately</li> <li>• crit – critical condition</li> <li>• debug – debug level messages</li> <li>• emerg – system is unusable (emergency)</li> <li>• err – error condition</li> <li>• info – informational condition</li> <li>• none – disables the logging locally and remotely</li> <li>• notice – normal, but significant condition</li> <li>• warning – warning condition</li> </ul>

<b>Default</b>	Remote logging is disabled
<b>Configuration Mode</b>	Config
<b>History</b>	3.1.0000
<b>Role</b>	admin
<b>Example</b>	<pre>switch (config) # logging local info switch (config) # show logging Local logging level: info Default remote logging level: notice No remote syslog servers configured. Allow receiving of messages from remote hosts: no Number of archived log files to keep: 10 Log rotation size threshold: 5.000% of partition (43 megabytes) Log format: standard Subsecond timestamp field: disabled Levels at which messages are logged:   CLI commands: notice   Audit messages: notice</pre>
<b>Related Commands</b>	<a href="#">show logging</a> <a href="#">logging local override</a> <a href="#">logging &lt;syslog IPv4 address/hostname&gt; port</a>
<b>Notes</b>	

## 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.

<b>Syntax Description</b>	<b>delete {current   oldest}</b>  <b>rotation {criteria {frequency {daily   weekly   monthly}   size &lt;size&gt;   size-pct &lt;percentage&gt;}   force   max-num}</b>  <b>update {&lt;number&gt;   current}</b>  <b>upload</b>  <b>log-file</b>  <b>upload URL</b>	Deletes certain debug-log files. <ul style="list-style-type: none"> <li>• current: Deletes the current active debug-log file</li> <li>• oldest: Deletes some of the oldest debug-log files</li> </ul> Configures automatic rotation of debug-logging files. <ul style="list-style-type: none"> <li>• criteria: Sets how the system decides when to rotate debug files. <ul style="list-style-type: none"> <li>• frequency: Rotate log files on a fixed time-based schedule</li> <li>• size: Rotate log files when they pass a size threshold in megabytes</li> <li>• size-pct: Rotate logs when they surpass a specified percentage of disk</li> </ul> </li> <li>• forces: Forces an immediate rotation of the log files</li> <li>• max-num: Specifies the maximum number of old log files to keep</li> </ul> Uploads a local debug-log file to a remote host. <ul style="list-style-type: none"> <li>• current: Uploads log file “messages” to a remote host</li> <li>• number: Uploads compressed log file “debug.&lt;number&gt;.gz” to a remote host. Range is 1-10</li> </ul> Uploads debug log file to a remote host Possible values: 1-7, or current HTTP, HTTPS, FTP, TFTP, SCP and SFTP are supported (e.g.: scp://username[:password]@hostname/path/filename)
<b>Default</b>	N/A	
<b>Configuration Mode</b>	Config	
<b>History</b>	3.3.4150	
<b>Role</b>	admin	
<b>Example</b>	<pre>switch (config) # logging debug-files delete current switch (config) #</pre>	
<b>Related Commands</b>		
<b>Notes</b>		

## 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.

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

---

**Example**

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

---

**Related Commands**

show logging  
logging local

---

---

**Notes**

---

## logging fields

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

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

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

<b>Syntax Description</b>	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.
<b>Default</b>	disabled	
<b>Configuration Mode</b>	Config	
<b>History</b>	3.1.0000	
<b>Role</b>	admin	
<b>Example</b>	<pre>switch (config) # logging fields seconds enable switch (config) # logging fields seconds whole-digits 1 switch (config) # show logging Local logging level: info Override for class mgmt-front: warning Default remote logging level: notice No remote syslog servers configured. Allow receiving of messages from remote hosts: no Number of archived log files to keep: 10 Log rotation size threshold: 5.000% of partition (43 megabytes) Log format: standard Subsecond timestamp field: enabled Subsecond timestamp precision: 1 whole digit; 3 fractional digits Levels at which messages are logged:     CLI commands: notice     Audit messages: notice switch (config) #</pre>	

---

**Related Commands** show logging**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.

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

## 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.

<b>Syntax Description</b>	freq	Sets rotation criteria according to time. Possible options are: <ul style="list-style-type: none"><li>• Daily</li><li>• Weekly</li><li>• Monthly</li></ul>
	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.
<b>Default</b>	10 files are kept by default with rotation criteria of 5% of the log partition size	
<b>Configuration Mode</b>	Config	
<b>History</b>	3.1.0000	
<b>Role</b>	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.

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

## 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.

<b>Syntax Description</b>	standard welf hostname	Standard format. WebTrends Enhanced Log file (WELF) format. 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.
<b>Default</b>	standard	
<b>Configuration Mode</b>	Config	
<b>History</b>	3.1.0000	
<b>Role</b>	admin	
<b>Example</b>	<pre>switch (config) # logging format standard switch (config) # show logging Local logging level: info Default remote logging level: notice No remote syslog servers configured. Allow receiving of messages from remote hosts: yes Number of archived log files to keep: 10 Log rotation size threshold: 5.000% of partition (43 megabytes) Log format: standard Subsecond timestamp field: disabled Levels at which messages are logged:     CLI commands: notice     Audit messages: notice switch (config) #</pre>	
<b>Related Commands</b>	show logging	
<b>Notes</b>		

## 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.

<b>Syntax Description</b>	cli commands audit mgmt log-level	Sets the severity level at which CLI commands which the user executes are logged. Sets the severity level at which all network management audit messages are logged. <ul style="list-style-type: none"> <li>• alert - alert notification, action must be taken immediately</li> <li>• crit - critical condition</li> <li>• debug - debug level messages</li> <li>• emerg - system is unusable (emergency)</li> <li>• err - error condition</li> <li>• info - informational condition</li> <li>• none - disables the logging locally and remotely</li> <li>• notice - normal, but significant condition</li> <li>• warning - warning condition</li> </ul>
<b>Default</b>	CLI commands and audit message are set to notice logging level	
<b>Configuration Mode</b>	Config	
<b>History</b>	3.1.0000	
<b>Role</b>	admin	
<b>Example</b>	<pre>switch (config) # logging level cli commands info switch (config) # show logging Local logging level: info     Override for class mgmt-front: warning Default remote logging level: notice No remote syslog servers configured. Allow receiving of messages from remote hosts: no Number of archived log files to keep: 10 Log rotation size threshold: 5.000% of partition (43 megabytes) Log format: standard Subsecond timestamp field: enabled Subsecond timestamp precision: 1 whole digit; 3 fractional digits Levels at which messages are logged:     CLI commands: info     Audit messages: notice switch (config) #</pre>	

---

**Related Commands** show logging**Notes** On PPC systems, logging levels “info” and “debug” should not be logged for prolonged periods of time or switch performance may be affected.

## 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.

<b>Syntax Description</b>	facility	<ul style="list-style-type: none"><li>• mgmt-front</li><li>• mgmt-back</li><li>• mgmt-core</li><li>• events</li><li>• sx-sdk</li><li>• mlnx-daemons</li><li>• iss-modules</li></ul>
---------------------------	----------	---

priority-level	<ul style="list-style-type: none"><li>• none</li><li>• emerg</li><li>• alert</li><li>• crit</li><li>• err</li><li>• warming</li><li>• notice</li><li>• info</li><li>• debug</li></ul>
----------------	---

<b>Default</b>	no logging monitor
----------------	--------------------

<b>Configuration Mode</b>	Config
---------------------------	--------

<b>History</b>	3.3.4000
----------------	----------

<b>Role</b>	admin
-------------	-------

<b>Example</b>	<pre>switch (config) # logging monitor events notice switch (config) #</pre>
----------------	--

### 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.

<b>Syntax Description</b>	N/A
<b>Default</b>	Receiving logging is disabled
<b>Configuration Mode</b>	Config
<b>History</b>	3.1.0000
<b>Role</b>	admin
<b>Example</b>	<pre>switch (config) # logging receive switch (config) # show logging Local logging level: info Default remote logging level: notice No remote syslog servers configured. Allow receiving of messages from remote hosts: yes Number of archived log files to keep: 10 Log rotation size threshold: 5.000% of partition (43 megabytes) Log format: standard Subsecond timestamp field: disabled Levels at which messages are logged:     CLI commands: notice     Audit messages: notice switch (config) #</pre>
<b>Related Commands</b>	<code>show logging</code> <code>logging local</code> <code>logging local override</code>
<b>Notes</b>	<ul style="list-style-type: none"><li>This does not log to the console TTY port</li><li>In-band management should be enabled in order to open a channel from the host to the CPU</li><li>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</li></ul>

## 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.

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

## show logging

### show logging

Displays the logging configurations.

<b>Syntax Description</b>	N/A
<b>Default</b>	N/A
<b>Configuration Mode</b>	Any Command Mode
<b>History</b>	3.1.0000
<b>Role</b>	admin
<b>Example</b>	<pre>switch (config) # show logging Local logging level: info     Override for class mgmt-front: warning Default remote logging level: notice No remote syslog servers configured. Allow receiving of messages from remote hosts: no Number of archived log files to keep: 10 Log rotation size threshold: 5.000% of partition (43 megabytes) Log format: standard Subsecond timestamp field: enabled Subsecond timestamp precision: 1 whole digit; 3 fractional digits Levels at which messages are logged:     CLI commands: info     Audit messages: notice switch (config) #</pre>
<b>Related Commands</b>	<a href="#">logging fields</a> <a href="#">logging files rotation</a> <a href="#">logging level</a> <a href="#">logging local</a> <a href="#">logging receive</a> <a href="#">logging &lt;syslog IPv4 address/hostname&gt;</a>
<b>Notes</b>	

## show log

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

Displays the log file with optional filter criteria.

<b>Syntax Description</b>	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.
<b>Default</b>	N/A	
<b>Configuration Mode</b>	Any Command Mode	
<b>History</b>	3.1.0000	
	3.3.4402	Updated example and added note
<b>Role</b>	admin	
<b>Example</b>	<pre>switch (config) # show log matching "Executing Action" Jan 19 10:55:38 arc-switch14 cli28202: [cli.NOTICE]: user admin: Executing command: en Jan 19 11:19:32 arc-switch14 cli28202: [cli.NOTICE]: user admin: Executing command: image install image-SX_PPC_M460EX-ppc-m460ex-20140119-115026.img Jan 19 11:19:32 arc-switch14 mgmtd4064: [mgmtd.NOTICE]: Action ID 326: requested by: user admin (System Administrator) via CLI Jan 19 11:19:32 arc-switch14 mgmtd4064: [mgmtd.NOTICE]: Action ID 326: descr: install system software image Jan 19 11:19:32 arc-switch14 mgmtd4064: [mgmtd.NOTICE]: Action ID 326: param: image file- name: image-SX_PPC_M460EX-ppc-m460ex-20140119-115026.img, version: SX_PPC_M460EX 3.0.0000-dev-master-HA 2014-01-19 11:50:26 ppc Jan 19 11:19:32 arc-switch14 mgmtd4064: [mgmtd.NOTICE]: Action ID 326: param: switch next boot location after install: no switch (config) #</pre>	

---

**Related Commands**

logging fields  
logging files rotation  
logging level  
logging local  
logging receive  
logging <syslog IPv4 address/hostname>  
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.
-

## 4.7 Debugging

- *To use the debugging logs feature:*

**Step 1.** Enable debugging. Run:

```
switch (config) # debug ethernet all
```

**Step 2.** Display the debug level set. Run:

```
switch (config) # show debug ethernet
```

**Step 3.** Display the logs. Run:

```
switch (config) # show log debug {match|continue}
```

## 4.7.1 Commands

### debug ethernet all

**debug ethernet all**  
**no debug ethernet all**

Enables debug traces for Ethernet modules.

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

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

## debug ethernet dcbx

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

Configures the trace level for DCBX.

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

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

## debug ethernet ip igmp-snooping

```
debug ethernet ip igmp-snooping {all | forward-db-messages | group-info | init-shut | packet-dump | query | source-info | system-resources-management | timer | vlan-info}
```

```
no debug ethernet ip igmp-snooping {all | forward-db-messages | group-info | init-shut | packet-dump | query | source-info | system-resources-management | timer | vlan-info}
```

Configures the trace level for IGMP snooping.

The no form of the command disables tracking a specified level.

<b>Syntax Description</b>	all	Enable track traces
	forward-db-messages	Forwarding database messages
	group-info	Group information messages
	init-shut	Init and shutdown messages
	packet-dump	Packet dump messages
	query	Query related messages
	source-info	Source information messages
	system-resources-management	System resources management messages
	timer	Timer messages
	vlan-info	VLAN information messages
<b>Default</b>	N/A	
<b>Configuration Mode</b>	Config	
<b>History</b>	3.3.4150	
<b>Role</b>	admin	
<b>Example</b>	<pre>switch (config) # debug ethernet ip igmp-snooping all switch (config) #</pre>	
<b>Related Commands</b>		
<b>Notes</b>		

## debug ethernet ip interface

```
debug ethernet ip interface {all | arp-packet-dump | buffer | enet-packet-dump | error | fail-all | filter | trace-error | trace-event}
no debug ethernet ip interface {all | arp-packet-dump | buffer | enet-packet-dump | error | fail-all | filter | trace-error | trace-event}
```

Configures the trace level for interface.

The no form of the command disables tracking a specified level.

<b>Syntax Description</b>	all	Enable track traces
	arp-packet-dump	ARP packet dump trace
	buffer	Buffer trace
	enet-packet-dump	ENET packet dump trace
	error	Trace error messages
	fail-all	All failures including Packet Validation Trace
	filter	Lower layer traces
	trace-error	Trace error messages
	trace-event	Trace event messages
<b>Default</b>	N/A	
<b>Configuration Mode</b>	Config	
<b>History</b>	3.3.4150	
<b>Role</b>	admin	
<b>Example</b>	<pre>switch (config) # debug ethernet ip interface all switch (config) #</pre>	
<b>Related Commands</b>		
<b>Notes</b>		

## debug ethernet lacp

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

Configures the trace level for LACP.

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

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

## debug ethernet lldp

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

Configures the trace level for LLDP.

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

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

## debug ethernet port

### debug ethernet port all

Configures the trace level for port.

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

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

## debug ethernet qos

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

Configures the trace level for QoS.

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

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

## debug ethernet spanning-tree

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

Configures the trace level for spanning-tree.

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

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

---

**Example**

---

```
switch (config) # debug ethernet spanning-tree all
switch (config) #
```

---

**Related Commands**

---

---

**Notes**

---

## debug ethernet vlan

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

Configures the trace level for VLAN.

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

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

## show debug ethernet

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

Displays debug level configuration on a specific switch.

<b>Syntax Description</b>	dcbx	Displays the trace level for spanning tree.
	ip	Displays debug trace level for ethernet routing module. <ul style="list-style-type: none"><li>• arp</li><li>• dhcp-relay</li><li>• igmp-snooping</li><li>• interface</li><li>• ospf</li></ul>
	lacp	Displays the trace level for LACP.
	lldp	Displays the trace level for LLDP.
	port	Displays the trace level for port.
	qos	Displays the trace level for QoS.
	spanning-tree	Displays the trace level for spanning tree.
	vlan	Displays the trace level for VLAN.
<b>Default</b>	N/A	
<b>Configuration Mode</b>	Any Command Mode	
<b>History</b>	3.3.4150	
<b>Role</b>	admin	
<b>Example</b>	<pre>switch (config) # show debug ethernet dcbx dcbx protocol :     management is ON     fail-all is ON     control-panel is ON     tlv is ON switch (config) #</pre>	
<b>Related Commands</b>		
<b>Notes</b>		

## show log debug

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

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

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

## 4.8 Link Diagnostic Per Port

### 4.8.1 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.

### 4.8.2 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

### 4.8.3 Commands

#### show interfaces ib link-diagnostics

**show interfaces ib [device/port] link-diagnostics**

Displays a specific InfiniBand module/port or all InfiniBand ports.

<b>Syntax Description</b>	N/A	
<b>Default</b>	N/A	
<b>Configuration Mode</b>	Config	
<b>History</b>	3.6.4000	
<b>Role</b>	admin	
<b>Example</b>	<pre>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..</pre>	

---

**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.

<b>Syntax Description</b>	N/A		
<b>Default</b>	N/A		
<b>Configuration Mode</b>	Config		
<b>History</b>	3.6.4000		
<b>Role</b>	admin		
<b>Example</b>	<pre>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</pre>		
<b>Related Commands</b>			
<b>Notes</b>			

## show interfaces ib internal spine link-diagnostics

**show interfaces ib internal spine <module/port> link-diagnostics**

Displays a specific InfiniBand internal spine module/port.

<b>Syntax Description</b>	N/A
<b>Default</b>	N/A
<b>Configuration Mode</b>	Config
<b>History</b>	3.6.4000
<b>Role</b>	admin
<b>Example</b>	<pre>switch (config) # show interfaces ib internal spine 3/1/1 link-diagnos-tics ----- Interface          Code      Status ----- IB3/1/1            0         No issue was observed</pre>
<b>Related Commands</b>	
<b>Notes</b>	

## show interfaces ethernet link-diagnostics

**show interfaces ethernet [<interface>] link-diagnostics**

Displays a specific Ethernet module/port or all Ethernet ports.

<b>Syntax Description</b>	N/A	
<b>Default</b>	N/A	
<b>Configuration Mode</b>	Config	
<b>History</b>	3.6.4006	
	3.6.4110	Updated command input.
<b>Role</b>	admin	
<b>Example</b>	<pre>switch (config) # show interfaces ethernet link-diagnostics -----       Interface   Code      Status -----       Eth1/1     1024      Cable is unplugged       Eth1/2     1024      Cable is unplugged       Eth1/3     1024      Cable is unplugged       Eth1/4     1024      Cable is unplugged       Eth1/5     1024      Cable is unplugged       Eth1/6     1024      Cable is unplugged       Eth1/7     1024      Cable is unplugged       Eth1/8     1024      Cable is unplugged       Eth1/9     1024      Cable is unplugged       Eth1/10    1024      Cable is unplugged       Eth1/11    1024      Cable is unplugged       Eth1/12    1024      Cable is unplugged       Eth1/13    1024      Cable is unplugged       Eth1/14    1024      Cable is unplugged       Eth1/15    1024      Cable is unplugged       Eth1/16    1024      Cable is unplugged       Eth1/17    1024      Cable is unplugged       Eth1/18    1024      Cable is unplugged       Eth1/19    1024      Cable is unplugged       Eth1/20    1024      Cable is unplugged       Eth1/21    1024      Cable is unplugged       Eth1/22    1024      Cable is unplugged       Eth1/23    1024      Cable is unplugged       Eth1/24    1024      Cable is unplugged       Eth1/25    1024      Cable is unplugged       Eth1/26    1024      Cable is unplugged       Eth1/27    1024      Cable is unplugged       Eth1/28    1024      Cable is unplugged       Eth1/29    1024      Cable is unplugged       Eth1/30    1024      Cable is unplugged       Eth1/31    0          No issue was observed       Eth1/32    0          No issue was observed</pre>	

---

**Related Commands**

---

**Notes**

---

## 4.9 Signal Degradation Monitoring



This section is relevant only for Spectrum™ based switch systems.

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 MAC 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.

### 4.9.1 Effective-BER Monitoring

Effective-BER is the BER that the MAC/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 MAC layer. The Effective BER for FEC links is monitored using the FEC decoder uncorrectable codewords data.

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.

### 4.9.2 Configuring Signal Degradation Monitoring

**Step 1.** Enable signal degradation monitoring. Run:

```
switch (config) # interface ethernet 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) # interface ethernet 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 4.17.1.6, “Configuring an SNMP Notification,” on page 513 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 4.10.3, “Email Notifications,” on page 328 for a general explanation on how to enable email notifications for specific events.

## 4.9.3 Commands

### interface ethernet signal-degrade

[no] interface ethernet <slot>/<port> signal-degrade [no-shutdown]

Enables signal degradation operation per interface.

<b>Syntax Description</b>	no-shutdown	Does not shutdown an affected interface
<b>Default</b>	Disabled	
<b>Configuration Mode</b>	Config	
<b>History</b>	3.6.4110	
<b>Role</b>	admin	
<b>Example</b>	switch (config) #interface ethernet 1/1 signal-degrade	
<b>Related Commands</b>		
<b>Notes</b>		

## show interfaces ethernet signal-degrade

**show interfaces ethernet [<slot>/<port>] signal-degrade**

Displays signal degradation information.

<b>Syntax Description</b>	N/A
<b>Default</b>	N/A
<b>Configuration Mode</b>	Config
<b>History</b>	3.6.4110
<b>Role</b>	admin
<b>Example</b>	<pre>switch (config) # show interfaces ethernet signal-degrade ----- Interface      Admin state          Monitoring     Action        FEC type ----- Eth1/1         Enabled             Disabled       Shutdown     no-fec/post-fec Eth1/2         Enabled             Disabled       Shutdown     no-fec/post-fec Eth1/3         Enabled             Disabled       Shutdown     no-fec/post-fec Eth1/4         Enabled             Disabled       Shutdown     no-fec/post-fec Eth1/5         Enabled             Disabled       Shutdown     no-fec/post-fec ... ...</pre>
<b>Related Commands</b>	
<b>Notes</b>	

## 4.10 Event Notifications

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

### 4.10.1 Supported Events

Table 27 presents the supported events and maps them to their relevant MIB OID.

**Table 27 - 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
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
interface-down	An interface's link state has changed to DOWN	RFC1213: linkdown (SNMPv1)	Supported for Ethernet, and management interfaces for 1U and blade systems
interface-up	An interface's link state has changed to UP	RFC1213: linkup (SNMPv1)	Supported for Ethernet, and management interfaces for 1U and blade systems
internal-bus-error	Internal bus (I <sup>2</sup> C) error	Mellanox-EFM-MIB: internalBusError	N/A
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

**Table 27 - Supported Event Notifications and MIB Mapping**

Event Name	Event Description	MIB OID	Comments
new_root	Local bridge became a root bridge	Bridge-MIB: newRoot	Supported for Ethernet
paging-high	Paging activity has risen too high	N/A	Not supported
power-redundancy-mismatch	Power redundancy mismatch	Mellanox-EFM-MIB: powerRedundancyMismatch	Supported only for director switch systems
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
snmp-authtrap	An SNMPv3 request has failed authentication	Not implemented	N/A
topology_change	Topology change triggered by a local bridge	Bridge-MIB: topology-Change	Supported for Ethernet
unexpected-shutdown	Unexpected system shutdown	Mellanox-EFM-MIB: unexpectedShutdown	N/A
To send, use the CLI command <code>snmp-server notify send-test</code>	Send a testing event	testTrap	N/A
N/A	Reset occurred due to over-heating of ASIC	Mellanox-EFM-MIB: asicOverTempReset	Not supported
temperature-too-high	Temperature is too high	Mellanox-EFM-MIB: asicOverTemp	N/A

#### 4.10.2 Terminal Notifications

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

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

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

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

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

#### 4.10.3 Email Notifications

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

**Step 1.** Enter to Config mode. Run:

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

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

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

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

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

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

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

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

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

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

.
.
.

switch (config) #
```

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

```
switch # email send-test
```

The last command should generate the following email:

-----Original Message-----

From: Admin User [mailto:do-not-reply@switch.]  
Sent: Sunday, May 01, 2011 11:17 AM  
To: <name>  
Subject: System event on switch: Test email for event notification  
  
===== System information:  
Hostname: switch  
Version: <version> 2011-05-01 14:56:31

```
...
Date:      2011/05/01 08:17:29
Uptime:    17h 8m 28.060s
```

```
This is a test email.
===== Done.
```

## 4.10.4 Commands

### 4.10.4.1 Email Notification

#### email autosupport enable

**email autosupport enable**  
**no email autosupport enable**

Sends automatic support notifications via email.

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

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

## 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	
		<ul style="list-style-type: none"><li>• process-crash – a process has crashed</li><li>• process-exit – a process unexpectedly exited</li><li>• liveness-failure – a process has been detected as hung</li><li>• cpu-util-high – CPU utilization has risen too high</li><li>• cpu-util-ok – CPU utilization has fallen back to normal levels</li><li>• paging-high – paging activity has risen too high</li><li>• paging-ok – paging activity has fallen back to normal levels</li><li>• disk-space-low – filesystem free space has fallen too low</li><li>• disk-space-ok – filesystem free space is back in the normal range</li><li>• memusage-high – memory usage has risen too high</li><li>• memusage-ok – memory usage has fallen back to acceptable levels</li><li>• netusage-high – network utilization has risen too high</li><li>• netusage-ok – network utilization has fallen back to acceptable levels</li><li>• disk-io-high – disk I/O per second has risen too high</li><li>• disk-io-ok – disk I/O per second has fallen back to acceptable levels</li><li>• unexpected-cluster-join – node has unexpectedly joined the cluster</li><li>• unexpected-cluster-leave – node has unexpectedly left the cluster</li><li>• unexpected-cluster-size – the number of nodes in the cluster is unexpected</li><li>• unexpected-shutdown – unexpected system shutdown</li><li>• interface-up – an interface's link state has changed to up</li><li>• interface-down – an interface's link state has changed to down</li><li>• user-login – a user has logged into the system</li><li>• user-logout – a user has logged out of the system</li><li>• health-module-status – health module status</li><li>• temperature-too-high – temperature has risen too high</li><li>• low-power – low power supply</li><li>• low-power-recover – low power supply recover</li><li>• insufficient-power – insufficient power supply</li><li>• power-redundancy-mismatch – power redundancy mismatch</li><li>• insufficient-fans – insufficient amount of fans in system</li><li>• insufficient-fans-recover – insufficient amount of fans in system recovered</li></ul>

- 
- asic-chip-down – ASIC (chip) down
  - internal-bus-error – internal bus (I<sup>2</sup>C) error
  - internal-link-speed-mismatch – internal links speed mismatch
- 

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

---

## 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.

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

## 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.

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

## 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.

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

## 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.

<b>Syntax Description</b>	hostname or IP address	IP address.
<b>Default</b>	No email domain	
<b>Configuration Mode</b>	Config	
<b>History</b>	3.1.0000	
<b>Role</b>	admin	
<b>Example</b>	<pre>switch (config) # email domain mellanox switch (config) # show email Mail hub: 10.0.8.11 Mail hub port: 125 Domain: mellanox Return address: do-not-reply Include hostname in return address: yes ... switch (config) #</pre>	
<b>Related Commands</b>	show emails	
<b>Notes</b>		

## 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.

<b>Syntax Description</b>	hostname or IP address	Hostname or IP address.
<b>Default</b>	N/A	
<b>Configuration Mode</b>	Config	
<b>History</b>	3.1.0000	
<b>Role</b>	admin	
<b>Example</b>	<pre>switch (config) # email mailhub 10.0.8.11 switch (config) # show email Mail hub: 10.0.8.11 Mail hub port: 25 Domain: (not specified) Return address: do-not-reply Include hostname in return address: yes ... switch (config) #</pre>	
<b>Related Commands</b>	show email [events]	
<b>Notes</b>		

## 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.

<b>Syntax Description</b>	hostname or IP address	hostname or IP address.
<b>Default</b>	25	
<b>Configuration Mode</b>	Config	
<b>History</b>	3.1.0000	
<b>Role</b>	admin	
<b>Example</b>	<pre>switch (config) # email mailhub-port 125 switch (config) # show email Mail hub: 10.0.8.11 Mail hub port: 125 Domain: (system domain name) Return address: do-not-reply Include hostname in return address: yes ... switch (config) #</pre>	
<b>Related Commands</b>	show email	
<b>Notes</b>		

## 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.

<b>Syntax Description</b>	event name	Example event names would include “process-crash” and “cpu-util-high”.
<b>Default</b>	No events are enabled	
<b>Configuration Mode</b>	Config	
<b>History</b>	3.1.0000	
<b>Role</b>	admin	
<b>Example</b>	<pre>switch (config) # email notify event process-crash switch (config) # show email events Failure events for which emails will be sent: process-crash: A process in the system has crashed unexpected-shutdown: Unexpected system shutdown  Informational events for which emails will be sent: liveness-failure: A process in the system was detected as hung process-exit: A process in the system unexpectedly exited cpu-util-ok: CPU utilization has fallen back to normal levels cpu-util-high: CPU utilization has risen too high disk-io-ok: Disk I/O per second has fallen back to acceptable levels ... temperature-too-high: Temperature has risen too high  All events for which autosupport emails will be sent: process-crash: A process in the system has crashed liveness-failure: A process in the system was detected as hung switch (config) # switch (config) #</pre>	
<b>Related Commands</b>	show email	
<b>Notes</b>	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.

<b>Syntax Description</b>	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.
<b>Default</b>	No recipients are added
<b>Configuration Mode</b>	Config
<b>History</b>	3.1.0000
<b>Role</b>	admin
<b>Example</b>	<pre>switch (config) # email notify recipient user2@autosupport.mellanox.com switch (config) # show email Mail hub: Mail hub port: 25 Domain: (not specified) Return address: user1 Include hostname in return address: no Dead letter settings: Save dead.letter files: yes Dead letter max age: (none) Email notification recipients: user2@autosupport.mellanox.com (all events, in detail) Autosupport emails Enabled: no Recipient: autosupport@autosupport.mellanox.com Mail hub: autosupport.mellanox.com switch (config) #</pre>
<b>Related Commands</b>	show email
<b>Notes</b>	

## 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.

<b>Syntax Description</b>	username	Username.
<b>Default</b>	do-not-reply	
<b>Configuration Mode</b>	Config	
<b>History</b>	3.1.0000	
<b>Role</b>	admin	
<b>Example</b>	<pre>switch (config) # email return-addr user1 switch (config) # show email Mail hub: Mail hub port: 25 Domain: (not specified) Return address: user1 Include hostname in return address: yes ... switch (config) #</pre>	
<b>Related Commands</b>	show email	
<b>Notes</b>		

## 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.

<b>Syntax Description</b>	N/A
<b>Default</b>	No return host
<b>Configuration Mode</b>	Config
<b>History</b>	3.1.0000
<b>Role</b>	admin
<b>Example</b>	<pre>switch (config) # no email return-host switch (config) # show email Mail hub: Mail hub port:      25 Domain:            (system domain name) Return address:    my-address Include hostname in return address: no  Current reply address: host@localdomain  Dead letter settings:   Save dead.letter files: yes   Dead letter max age:    5 days  No recipients configured.  Autosupport emails   Enabled:        no   Recipient:     autosupport@autosupport.mellanox.com   Mail hub:       autosupport.mellanox.com switch (config) #</pre>
<b>Related Commands</b>	show email
<b>Notes</b>	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.

<b>Syntax Description</b>	N/A
<b>Default</b>	N/A
<b>Configuration Mode</b>	Config
<b>History</b>	3.1.0000
<b>Role</b>	admin
<b>Example</b>	<code>switch (config) # email send-test</code>
<b>Related Commands</b>	<code>show email [events]</code>
<b>Notes</b>	

## 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.

<b>Syntax Description</b>	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.
<b>Default</b>	default-cert	
<b>Configuration Mode</b>	Config	
<b>History</b>	3.2.3000	
<b>Role</b>	admin	
<b>Example</b>	switch (config) # email ssl mode tls-none	
<b>Related Commands</b>	N/A	
<b>Notes</b>		

## 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.

<b>Syntax Description</b>	N/A
<b>Default</b>	N/A
<b>Configuration Mode</b>	Config
<b>History</b>	3.2.3000
<b>Role</b>	admin
<b>Example</b>	switch (config) # email ssl cert-verify
<b>Related Commands</b>	N/A
<b>Notes</b>	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.

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

## show email

### show email [events]

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

<b>Syntax Description</b>	events	show event list
<b>Default</b>	N/A	
<b>Configuration Mode</b>	Any Command Mode	
<b>History</b>	3.1.0000	
<b>Role</b>	admin	
<b>Example</b>	<pre>switch (config) # show email Mail hub:   Mail hub port:      25   Domain:            (system domain name)   Return address:    my-address   Include hostname in return address: no    Current reply address: host@localdomain    Dead letter settings:     Save dead.letter files: yes     Dead letter max age:    5 days    No recipients configured.    Autosupport emails     Enabled:        no     Recipient:     autosupport@autosupport.mellanox.com     Mail hub:       autosupport.mellanox.com switch (config) #</pre>	
<b>Related Commands</b>	<a href="#">show email</a>	
<b>Notes</b>		

## 4.11 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 following mechanisms to perform those 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 is a record of the most active flows which cause an excessive usage of the port buffers. 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.

## 4.11.1 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.

<b>Syntax Description</b>	N/A
<b>Default</b>	Disabled
<b>Configuration Mode</b>	Config
<b>History</b>	3.6.3004
<b>Role</b>	admin
<b>Example</b>	<pre>switch (config) # telemetry shutdown switch (config) # no telemetry shutdown</pre>
<b>Related Commands</b>	
<b>Notes</b>	

## 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
<b>Default</b>	1000 msec.	
<b>Configuration Mode</b>	Config	
<b>History</b>	3.6.3004	
<b>Role</b>	admin	
<b>Example</b>		switch (config) # telemetry sampling log 1000 switch (config) # no telemetry sampling log
<b>Related Commands</b>		
<b>Notes</b>		

## 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).

<b>Syntax Description</b>	N/A
<b>Default</b>	N/A
<b>Configuration Mode</b>	Config Interface IB
<b>History</b>	3.6.3004
<b>Role</b>	admin
<b>Example</b>	switch (config interface ib 1/1) # telemetry sampling
<b>Related Commands</b>	
<b>Notes</b>	

## telemetry sampling tc

```
telemetry sampling tc <0-7> [mcast | ucast]
no telemetry sampling tc <tc_id> [mcast | ucast]
```

Enables multicast sampling (histogram fetching) on a traffic class for a particular Ethernet interface.

The no form of the command disables multicast sampling on a TC for a particular Ethernet interface.

<b>Syntax Description</b>	mcast	Multicast traffic
	ucast	Unicast traffic
<b>Default</b>	N/A	
<b>Configuration Mode</b>	Config Interface Ethernet Config Interface Port Channel Config Interface MLAG Port Channel	
<b>History</b>	3.6.3004	
<b>Role</b>	admin	
<b>Example</b>	switch (config interface ethernet 1/2) # telemetry sampling tc 3 mcast	
<b>Related Commands</b>		
<b>Notes</b>		

## telemetry threshold

```
telemetry threshold tc <0-7> [ucast | mcast]
no telemetry threshold tc <0-7> [ucast | mcast]
```

Enables threshold in hardware for a particular traffic class.  
The no form of the command disables threshold in hardware for a particular traffic class.

Syntax Description	ucast mcast	Unicast traffic Multicast traffic
Default	Disabled	
Configuration Mode	Config Interface Ethernet Config Interface Port Channel Config Interface MLAG Port Channel	
History	3.6.5000	
Role	admin	
Example	switch (config interface ethernet 1/12) # telemetry threshold tc 0 ucast	
Related Commands		
Notes		

## telemetry threshold level

**telemetry threshold level <level>**  
**no telemetry threshold level <level>**

Configures the threshold level in the hardware per port.  
The no form of the command resets the parameter to its default.

<b>Syntax Description</b>	level	Range: 96-1,000,000 Level is set in bytes and in increments of 96
<b>Default</b>	69984	
<b>Configuration Mode</b>	Config Interface Ethernet Config Interface Port Channel Config Interface MLAG Port Channel	
<b>History</b>	3.6.5000	
<b>Role</b>	admin	
<b>Example</b>	switch (config interface ethernet 1/12) # telemetry threshold level 288	
<b>Related Commands</b>		
<b>Notes</b>		

## clear telemetry

```
clear telemetry {threshold | sampling} [interface <type> <port-id>] [tc <0-7> [ucast | mcast]]
```

Clears telemetry data.

<b>Syntax Description</b>	type	<ul style="list-style-type: none"><li>• ethernet</li><li>• port-channel</li><li>• mlag-port-channel</li></ul>
	tc	Traffic class
	mcast	Multicast traffic
	ucast	Unicast traffic
<b>Default</b>	N/A	
<b>Configuration Mode</b>		Config Interface Ethernet Config Interface Port Channel Config Interface MLAG Port Channel
<b>History</b>	3.6.5000	
<b>Role</b>	admin	
<b>Example</b>		switch (config interface ethernet 1/12) # clear telemetry threshold level 288
<b>Related Commands</b>		
<b>Notes</b>		

## show telemetry sampling interface ethernet tc ucast

```
show telemetry sampling interface ethernet <slot>/<port>[/<subport>] tc
<tc_id> ucast
```

Displays fetched unicast histogram details for a given TC ID of the Ethernet interface.

<b>Syntax Description</b>	slot/port	Ethernet port number																																												
	subport	Ethernet subport number to be used in case of split port																																												
	tc_id	Input range: 0-7																																												
<b>Default</b>	N/A																																													
<b>Configuration Mode</b>	Any Command Mode																																													
<b>History</b>	3.6.3004																																													
<b>Role</b>	admin																																													
<b>Example</b>	<pre>switch (config) # show telemetry sampling interface ethernet 1/2 tc 6 ucast</pre> ----- <pre>Telemetry histogram: Eth1/2 traffic-class 6 - ucast Time                                Bin sizes (nsec buffer was occupied in bytes range) -----</pre> <table border="1"> <thead> <tr> <th>Time</th> <th>2976&lt;</th> <th>27552</th> <th>52128</th> <th>76704</th> <th>101280</th> <th>125856</th> <th>150432</th> <th>175008</th> <th>199584</th> <th>199584&gt;</th> </tr> </thead> <tbody> <tr> <td>01/13/17 08:18:09.67745</td> <td>1000000000</td> <td>0</td> <td>0</td> <td>0</td> <td>0</td> <td>0</td> <td>0</td> <td>0</td> <td>0</td> <td>0</td> </tr> <tr> <td>08:18:10.67850</td> <td>1000000000</td> <td>0</td> <td>0</td> <td>0</td> <td>0</td> <td>0</td> <td>0</td> <td>0</td> <td>0</td> <td>0</td> </tr> <tr> <td>08:18:11.67953</td> <td>1000000000</td> <td>0</td> <td>0</td> <td>0</td> <td>0</td> <td>0</td> <td>0</td> <td>0</td> <td>0</td> <td>0</td> </tr> </tbody> </table>		Time	2976<	27552	52128	76704	101280	125856	150432	175008	199584	199584>	01/13/17 08:18:09.67745	1000000000	0	0	0	0	0	0	0	0	0	08:18:10.67850	1000000000	0	0	0	0	0	0	0	0	0	08:18:11.67953	1000000000	0	0	0	0	0	0	0	0	0
Time	2976<	27552	52128	76704	101280	125856	150432	175008	199584	199584>																																				
01/13/17 08:18:09.67745	1000000000	0	0	0	0	0	0	0	0	0																																				
08:18:10.67850	1000000000	0	0	0	0	0	0	0	0	0																																				
08:18:11.67953	1000000000	0	0	0	0	0	0	0	0	0																																				
<b>Related Commands</b>																																														
<b>Notes</b>																																														

## show telemetry sampling interface ethernet tc mcast

```
show telemetry sampling interface ethernet <slot>/<port>[/<subport>] tc
<tc_id> mcast
```

Displays fetched multicast histogram details for a given tc\_id of the Ethernet interface.

<b>Syntax Description</b>	slot/port	Ethernet port number																																																																		
	subport	Ethernet subport number to be used in case of split port																																																																		
	tc_id	Input range: 0-7																																																																		
<b>Default</b>	N/A																																																																			
<b>Configuration Mode</b>	Any Command Mode																																																																			
<b>History</b>	3.6.3004																																																																			
<b>Role</b>	admin																																																																			
<b>Example</b>	<pre>switch (config) # show telemetry sampling interface ethernet 1/2 tc 3 mcast</pre> ----- <pre>Telemetry histogram: Eth1/2 traffic-class 3 - mcast Time                                Bin sizes (nsec buffer was occupied in bytes range) -----</pre> <table border="1"> <thead> <tr> <th>Time</th> <th>2976&lt;</th> <th>27552</th> <th>52128</th> <th>76704</th> <th>101280</th> <th>125856</th> <th>150432</th> <th>175008</th> <th>199584</th> <th>199584&gt;</th> </tr> </thead> <tbody> <tr> <td>01/16/17 04:09:07.79936</td> <td>1000000000</td> <td>0</td> <td>0</td> <td>0</td> <td>0</td> <td>0</td> <td>0</td> <td>0</td> <td>0</td> <td>0</td> </tr> <tr> <td>04:09:08.80096</td> <td>1000000000</td> <td>0</td> <td>0</td> <td>0</td> <td>0</td> <td>0</td> <td>0</td> <td>0</td> <td>0</td> <td>0</td> </tr> <tr> <td>04:09:09.80355</td> <td>1000000000</td> <td>0</td> <td>0</td> <td>0</td> <td>0</td> <td>0</td> <td>0</td> <td>0</td> <td>0</td> <td>0</td> </tr> <tr> <td>04:09:10.80518</td> <td>1000000000</td> <td>0</td> <td>0</td> <td>0</td> <td>0</td> <td>0</td> <td>0</td> <td>0</td> <td>0</td> <td>0</td> </tr> <tr> <td>04:09:11.80682</td> <td>1000000000</td> <td>0</td> <td>0</td> <td>0</td> <td>0</td> <td>0</td> <td>0</td> <td>0</td> <td>0</td> <td>0</td> </tr> </tbody> </table>	Time	2976<	27552	52128	76704	101280	125856	150432	175008	199584	199584>	01/16/17 04:09:07.79936	1000000000	0	0	0	0	0	0	0	0	0	04:09:08.80096	1000000000	0	0	0	0	0	0	0	0	0	04:09:09.80355	1000000000	0	0	0	0	0	0	0	0	0	04:09:10.80518	1000000000	0	0	0	0	0	0	0	0	0	04:09:11.80682	1000000000	0	0	0	0	0	0	0	0	0	
Time	2976<	27552	52128	76704	101280	125856	150432	175008	199584	199584>																																																										
01/16/17 04:09:07.79936	1000000000	0	0	0	0	0	0	0	0	0																																																										
04:09:08.80096	1000000000	0	0	0	0	0	0	0	0	0																																																										
04:09:09.80355	1000000000	0	0	0	0	0	0	0	0	0																																																										
04:09:10.80518	1000000000	0	0	0	0	0	0	0	0	0																																																										
04:09:11.80682	1000000000	0	0	0	0	0	0	0	0	0																																																										
<b>Related Commands</b>																																																																				
<b>Notes</b>																																																																				

## show telemetry sampling interface ethernet tc ucast last

**show telemetry sampling interface ethernet <slot>/<port>[/<subport>] tc <tc\_id> ucast last <num\_of\_entries>**

Displays last num of fetched unicast histogram details for the given tc\_id of the ethernet interface.

<b>Syntax Description</b>	slot/port	Ethernet port number																																												
	subport	Ethernet subport number to be used in case of split port																																												
	tc_id	Input range: 0-7																																												
	num_of_entries	Input range: 0-1000																																												
<b>Default</b>	N/A																																													
<b>Configuration Mode</b>	Any Command Mode																																													
<b>History</b>	3.6.3004																																													
<b>Role</b>	admin																																													
<b>Example</b>	<pre>switch (config) # show telemetry sampling interface ethernet 1/2 tc 3 ucast last 3 ----- Telemetry histogram: Eth1/2 traffic-class 3 - ucast Time   Bin sizes (msec buffer was occupied in bytes range) -----</pre> <table border="1"> <thead> <tr> <th>Time</th> <th>2976&lt;</th> <th>27552</th> <th>52128</th> <th>76704</th> <th>101280</th> <th>125856</th> <th>150432</th> <th>175008</th> <th>199584</th> <th>199584&gt;</th> </tr> </thead> <tbody> <tr> <td>01/16/17 04:28:39.81351</td> <td>1000000000</td> <td>0</td> <td>0</td> <td>0</td> <td>0</td> <td>0</td> <td>0</td> <td>0</td> <td>0</td> <td>0</td> </tr> <tr> <td>04:28:40.81512</td> <td>1000000000</td> <td>0</td> <td>0</td> <td>0</td> <td>0</td> <td>0</td> <td>0</td> <td>0</td> <td>0</td> <td>0</td> </tr> <tr> <td>04:28:41.81708</td> <td>1000000000</td> <td>0</td> <td>0</td> <td>0</td> <td>0</td> <td>0</td> <td>0</td> <td>0</td> <td>0</td> <td>0</td> </tr> </tbody> </table>		Time	2976<	27552	52128	76704	101280	125856	150432	175008	199584	199584>	01/16/17 04:28:39.81351	1000000000	0	0	0	0	0	0	0	0	0	04:28:40.81512	1000000000	0	0	0	0	0	0	0	0	0	04:28:41.81708	1000000000	0	0	0	0	0	0	0	0	0
Time	2976<	27552	52128	76704	101280	125856	150432	175008	199584	199584>																																				
01/16/17 04:28:39.81351	1000000000	0	0	0	0	0	0	0	0	0																																				
04:28:40.81512	1000000000	0	0	0	0	0	0	0	0	0																																				
04:28:41.81708	1000000000	0	0	0	0	0	0	0	0	0																																				
<b>Related Commands</b>																																														
<b>Notes</b>	In case requested entries are more than what the DB contains it will print the amount in the table.																																													

## show telemetry sampling interface ethernet tc mcast last

**show telemetry sampling interface ethernet <slot>/<port>[/<subport>] tc <tc\_id> mcast last <num\_of\_entries>**

Displays last num of fetched multicast histogram details for the given tc\_id of the ethernet interface.

<b>Syntax Description</b>	slot/port subport tc_id num_of_entries	Ethernet port number Ethernet subport number to be used in case of split port Input range: 0-7 Input range: 0-1000																																																																		
<b>Default</b>	N/A																																																																			
<b>Configuration Mode</b>	Any Command Mode																																																																			
<b>History</b>	3.6.3004																																																																			
<b>Role</b>	admin																																																																			
<b>Example</b>	<pre>switch (config) # show telemetry sampling interface ethernet 1/2 tc 3 mcast last 4 ----- Telemetry histogram: Eth1/2 traffic-class 3 - mcast Time   Bin sizes (msec buffer was occupied in bytes range) -----</pre> <table border="1"> <thead> <tr> <th>Time</th> <th>2976&lt;</th> <th>27552</th> <th>52128</th> <th>76704</th> <th>101280</th> <th>125856</th> <th>150432</th> <th>175008</th> <th>199584</th> <th>199584&gt;</th> </tr> </thead> <tbody> <tr> <td>01:16:17</td> <td>2976&lt;</td> <td>27552</td> <td>52128</td> <td>76704</td> <td>101280</td> <td>125856</td> <td>150432</td> <td>175008</td> <td>199584</td> <td>199584&gt;</td> </tr> <tr> <td>04:23:38.28864</td> <td>1000000000</td> <td>0</td> <td>0</td> <td>0</td> <td>0</td> <td>0</td> <td>0</td> <td>0</td> <td>0</td> <td>0</td> </tr> <tr> <td>04:23:39.28977</td> <td>1000000000</td> <td>0</td> <td>0</td> <td>0</td> <td>0</td> <td>0</td> <td>0</td> <td>0</td> <td>0</td> <td>0</td> </tr> <tr> <td>04:23:40.29111</td> <td>1000000000</td> <td>0</td> <td>0</td> <td>0</td> <td>0</td> <td>0</td> <td>0</td> <td>0</td> <td>0</td> <td>0</td> </tr> <tr> <td>04:23:41.29259</td> <td>1000000000</td> <td>0</td> <td>0</td> <td>0</td> <td>0</td> <td>0</td> <td>0</td> <td>0</td> <td>0</td> <td>0</td> </tr> </tbody> </table>	Time	2976<	27552	52128	76704	101280	125856	150432	175008	199584	199584>	01:16:17	2976<	27552	52128	76704	101280	125856	150432	175008	199584	199584>	04:23:38.28864	1000000000	0	0	0	0	0	0	0	0	0	04:23:39.28977	1000000000	0	0	0	0	0	0	0	0	0	04:23:40.29111	1000000000	0	0	0	0	0	0	0	0	0	04:23:41.29259	1000000000	0	0	0	0	0	0	0	0	0	
Time	2976<	27552	52128	76704	101280	125856	150432	175008	199584	199584>																																																										
01:16:17	2976<	27552	52128	76704	101280	125856	150432	175008	199584	199584>																																																										
04:23:38.28864	1000000000	0	0	0	0	0	0	0	0	0																																																										
04:23:39.28977	1000000000	0	0	0	0	0	0	0	0	0																																																										
04:23:40.29111	1000000000	0	0	0	0	0	0	0	0	0																																																										
04:23:41.29259	1000000000	0	0	0	0	0	0	0	0	0																																																										
<b>Related Commands</b>																																																																				
<b>Notes</b>	In case requested entries are more than what the DB contains it will print the amount in the table.																																																																			

## show telemetry threshold

**show telemetry threshold [interface <type> <port-id>] [tc <0-7> [ucast | mcast]]**

Displays the threshold data for either all interfaces or single interface or per interface per traffic class.

<b>Syntax Description</b>	type	<ul style="list-style-type: none"> <li>• ethernet</li> <li>• port-channel</li> <li>• mlag-port-channel</li> </ul>
	tc	Traffic class
	mcast	Multicast traffic
	ucast	Unicast traffic
<b>Default</b>	N/A	
<b>Configuration Mode</b>	Any Command Mode	
<b>History</b>	3.6.5000	
<b>Role</b>	admin	
<b>Example</b>	<pre>switch (config) # show telemetry threshold interface ethernet 1/10-1/13 ----- Date      Time       Port      TC      Level      Duration(100 usec)    Repeated ----- 09/21/17  10:11:48  Eth 1/10   0       100       102497.61          1 09/21/17  10:12:06  Eth 1/10   3       100       85714.76          1  switch (config) # show telemetry threshold interface port-channel 20 tc 2 mcast ----- Date      Time       Port      TC      Level      Duration(100 usec)    Repeated ----- 09/21/17  10:11:48  Po20 (Eth 1/1) 2 (mcast) 100       102497.61          1 09/21/17  10:12:06  Po20 (Eth 1/1) 2 (mcast) 100       85714.76          1</pre>	

### Related Commands

### Notes

## 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.

<b>Syntax Description</b>	slot/port	Infiniband port number																																												
		num_of_entries																																												
<b>Default</b>	N/A																																													
<b>Configuration Mode</b>	Any Command Mode																																													
<b>History</b>	3.6.3004																																													
<b>Role</b>	admin																																													
<b>Example</b>	<pre>switch (config) # show telemetry sampling interface ethernet 1/2 to 6 ucast</pre> <hr/> <pre>Telemetry histogram: Eth1/2 traffic-class 6 - ucast Time                                Bin sizes (nsec buffer was occupied in bytes range) -----</pre> <table border="1"> <thead> <tr> <th>Time</th> <th>2976&lt;</th> <th>27552</th> <th>52128</th> <th>76704</th> <th>101280</th> <th>125856</th> <th>150432</th> <th>175008</th> <th>199584</th> <th>199584&gt;</th> </tr> </thead> <tbody> <tr> <td>08:18:09.67745</td> <td>976563</td> <td>0</td> <td>0</td> <td>0</td> <td>0</td> <td>0</td> <td>0</td> <td>0</td> <td>0</td> <td>0</td> </tr> <tr> <td>08:18:10.67850</td> <td>976563</td> <td>0</td> <td>0</td> <td>0</td> <td>0</td> <td>0</td> <td>0</td> <td>0</td> <td>0</td> <td>0</td> </tr> <tr> <td>08:18:11.67953</td> <td>976563</td> <td>0</td> <td>0</td> <td>0</td> <td>0</td> <td>0</td> <td>0</td> <td>0</td> <td>0</td> <td>0</td> </tr> </tbody> </table>		Time	2976<	27552	52128	76704	101280	125856	150432	175008	199584	199584>	08:18:09.67745	976563	0	0	0	0	0	0	0	0	0	08:18:10.67850	976563	0	0	0	0	0	0	0	0	0	08:18:11.67953	976563	0	0	0	0	0	0	0	0	0
Time	2976<	27552	52128	76704	101280	125856	150432	175008	199584	199584>																																				
08:18:09.67745	976563	0	0	0	0	0	0	0	0	0																																				
08:18:10.67850	976563	0	0	0	0	0	0	0	0	0																																				
08:18:11.67953	976563	0	0	0	0	0	0	0	0	0																																				
<b>Related Commands</b>																																														
<b>Notes</b>	In case requested entries are more than what the DB contains it will print the amount in the table.																																													

## stats export csv telemetry

```
stats export csv telemetry <slot>/<port>[/<subport>]<tc>-[mcast | ucast] [file-name *] [after * *] [before * *]
```

Exports histograms collected by stats to a csv file.

<b>Syntax Description</b>	slot/port	Ethernet InfiniBand port number
	subport	Ethernet InfiniBand subport number to be used in case of split port
<b>Default</b>	N/A	
<b>Configuration Mode</b>	Any Command Mode	
<b>History</b>	3.6.3004	
<b>Role</b>	admin	
<b>Example</b>		switch (config) # stats export csv telemetry 1/1 Generated report file: telemetry-20170119-102715.csv
<b>Related Commands</b>		
<b>Notes</b>		

## 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 files stats telemetry

**show files stats telemetry [filename]**

Displays all files created by command stats export csv telemetry unless a filename is given.

<b>Syntax Description</b>	N/A
<b>Default</b>	N/A
<b>Configuration Mode</b>	Any Command Mode
<b>History</b>	3.6.3004
<b>Role</b>	admin
<b>Example</b>	<pre>switch (config) # show files stats telemetry telemetry-20170119-102715.csv</pre>
<b>Related Commands</b>	
<b>Notes</b>	

## telemetry threshold

[interface-id] telemetry threshold  
no [interface-id] telemetry threshold

The command enables threshold on hardware.  
The no form of the command disables threshold.

<b>Syntax Description</b>	[interface-id]	Input range: 1-3600		
<b>Default</b>	false			
<b>Configuration Mode</b>	Config Interface IB			
<b>History</b>	3.6.4006			
<b>Role</b>	admin			
<b>Example</b>	switch (config) # interface ib 1/1 switch (config interface ib 1/1) # telemetry threshold			
<b>Related Commands</b>				
<b>Notes</b>				

## 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 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.

<b>Syntax Description</b>	time	Max rate per hour. Input range: 1-3600
<b>Default</b>	100	
<b>Configuration Mode</b>	Config	
<b>History</b>	3.6.4006	
<b>Role</b>	admin	
<b>Example</b>	switch (config) # telemetry threshold syslog 400	
<b>Related Commands</b>		
<b>Notes</b>		

## telemetry threshold level

[interface-id] telemetry threshold level  
no [interface-id] telemetry threshold level

The command 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)
<b>Default</b>	69984	
<b>Configuration Mode</b>	Config Interface IB	
<b>History</b>	3.6.4006	
<b>Role</b>	admin	
<b>Example</b>		switch (config) # interface ib 1/1 switch (config interface ib 1/1) # telemetry threshold level 288
<b>Related Commands</b>		
<b>Notes</b>		

## 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) : 256
S/W Sampling Interval(ms) : 1000
Threshold Logging : Disabled
Threshold Logging(rate per hour) : 100
```

---

**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 28 - User Roles (Accounts) and Default Passwords**

User Role	Default Password
admin	admin
monitor	monitor
xmldadmin	xmldadmin
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 MLNX-OS switch. The MLNX-OS switch supports Remote Access Dial-In User Service (RADIUS) or Terminal Access Controller Access Control device Plus (TACACS+) protocols.

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

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

#### 4.12.2.1 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 ciphers. 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.

<b>Syntax Description</b>	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. <ul style="list-style-type: none"> <li>• admin - full administrative capabilities</li> <li>• monitor - read only capabilities, can not change the running configuration</li> <li>• unpriv – can only query the most basic information, and cannot take any actions or change any configuration</li> <li>• v_admin – basic administrator capabilities</li> </ul>
	disable [login   password]	<ul style="list-style-type: none"> <li>• Disable - disable this account</li> <li>• Disable login - disable all logins to this account</li> <li>• Disable password - disable login to this account using a local password</li> </ul>
	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	<ul style="list-style-type: none"> <li>• 0: specifies a login password in cleartext</li> <li>• 7: specifies a login password in encrypted text</li> </ul>
	password	Specifies a password for the user in string form. If [0   7] was not specified then the password is in cleartext.
<b>Default</b>	The following usernames are available by default:	
	<ul style="list-style-type: none"> <li>• admin</li> <li>• monitor</li> <li>• xmladmin</li> <li>• xmluser</li> </ul>	
<b>Configuration Mode</b>	Config	
<b>History</b>	3.1.0000	
	3.4.0000	Updated Example

	3.4.1100	Updated Example
	3.6.2002	Added “disconnect” parameter
<b>Role</b>	admin	
<b>Example</b>	<pre>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) #</pre>	
<b>Related Commands</b>	<a href="#">show usernames</a> <a href="#">show users</a>	
<b>Notes</b>	<ul style="list-style-type: none"><li>• To enable a user account, just set a password on it (or use the command <code>username &lt;user&gt; nopassword</code> to enable it with no password required for login)</li><li>• Removing a user account does not terminate any current sessions that user has open; it just prevents new sessions from being established</li><li>• Encrypted password is useful for the command <code>show configuration</code>, since the cleartext password cannot be recovered after it is set</li></ul>	

## show usernames

### show usernames

Displays list of users and their capabilities.

<b>Syntax Description</b>	N/A
<b>Default</b>	N/A
<b>Configuration Mode</b>	Any Command Mode
<b>History</b>	3.1.0000
<b>Role</b>	admin
<b>Example</b>	<pre>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) #</pre>
<b>Related Commands</b>	<a href="#">username</a> <a href="#">show users</a>
<b>Notes</b>	

## show users

### show users [history]

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

<b>Syntax Description</b>	history	Displays current and historical sessions.
<b>Default</b>	N/A	
<b>Configuration Mode</b>	Any Command Mode	
<b>History</b>	3.1.0000	
<b>Role</b>	admin	
<b>Example</b>	<pre>switch (config) # show users USERNAME    FULL NAME          LINE   HOST           IDLE admin      System Administrator pts/0  172.22.237.174  0d0h34m4s admin      System Administrator pts/1  172.30.0.127   1d3h30m49s admin      System Administrator pts/3  172.22.237.34  0d0h0m0s switch (config) #show users history admin     pts/3 172.22.237.34   Wed Feb  1 11:56  still logged in admin     pts/3 172.22.237.34   Wed Feb  1 11:42 - 11:46 (00:04)  wtmp begins Wed Feb  1 11:38:10 2012 switch (config) #</pre>	
<b>Related Commands</b>	<a href="#">username</a> <a href="#">show usernames</a>	
<b>Notes</b>		

## show whoami

### show whoami

Displays username and capabilities of user currently logged in.

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

#### 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.

<b>Syntax Description</b>	N/A
<b>Default</b>	N/A
<b>Configuration Mode</b>	Config
<b>History</b>	3.1.0000
	3.2.3000    Removed ‘time’ parameter from the command.
<b>Role</b>	admin
<b>Example</b>	<pre>switch (config) # aaa accounting changes default stop-only tacacs+ switch (config) # show aaa AAA authorization:     Default User: admin     Map Order: local-only Authentication method(s):     local     radius     tacacs+     ldap Accounting method(s):     tacacs+ switch (config) # show aaa</pre>
<b>Related Commands</b>	show aaa
<b>Notes</b>	<ul style="list-style-type: none"> <li>• TACACS+ is presently the only accounting service method supported</li> <li>• 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</li> <li>• 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</li> <li>• 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</li> </ul>

## 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.

<b>Syntax Description</b>	auth-method	<ul style="list-style-type: none"> <li>• local</li> <li>• radius</li> <li>• tacacs+</li> <li>• ldap</li> </ul>
<b>Default</b>	local	
<b>Configuration Mode</b>	Any Command Mode	
<b>History</b>	3.1.0000	
<b>Role</b>	admin	
<b>Example</b>	<pre>switch (config) # aaa authentication login default local radius tacacs+ ldap switch (config) # show aaa AAA authorization:     Default User: admin     Map Order: local-only Authentication method(s):     local     radius     tacacs+     ldap Accounting method(s):     tacacs+ switch (config) #</pre>	
<b>Related Commands</b>	show aaa	
<b>Notes</b>	<p>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.</p>	

## 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
<b>Default</b>	0	
<b>Configuration Mode</b>	Config	
<b>History</b>	3.5.0200	
<b>Role</b>	admin	
<b>Example</b>		switch (config) # aaa authentication attempts fail-delay 1
<b>Related Commands</b>	N/A	
<b>Notes</b>		

## 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.

<b>Syntax Description</b>	downcase	Does not convert all usernames to lowercase (for authentication failure tracking purposes only).
	enable	Disables tracking of failed authentication attempts
<b>Default</b>	N/A	
<b>Configuration Mode</b>	Config	
<b>History</b>	3.2.3000	
<b>Role</b>	admin	
<b>Example</b>	switch (config) # aaa authentication attempts track enable	
<b>Related Commands</b>	N/A	
<b>Notes</b>	<ul style="list-style-type: none"><li>This is required for the lockout functionality described below, but can also be used on its own for informational purposes.</li><li>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.</li></ul>	

## 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.

---

<b>Syntax Description</b>	enable	<p>Enables locking out of user accounts based on authentication failures.</p> <p>This both suspends enforcement of any existing lock-outs, 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.</p> <p>Lockouts only work if tracking is enabled. Enabling lockouts automatically enables tracking. Disabling tracking automatically disables lockouts.</p>
	lock-time	<p>Sets maximum permitted consecutive authentication failures before locking out users.</p> <p>Unlike the “max-fail” setting, this does take effect immediately for all accounts</p> <p>If both unlock-time and lock-time are set, the unlock-time must be greater than the lock-time</p> <p>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</p>
	max-fail	<p>Sets maximum permitted consecutive authentication failures before locking out users.</p> <p>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.</p>
	unlock-time	<p>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.</p> <p>Unlike the “max-fail” setting, this does take effect immediately for all accounts.</p> <p>If both unlock-time and lock-time are set, the unlock-time must be greater than the lock-time.</p> <p>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.</p>

---

<b>Default</b>	N/A
<b>Configuration Mode</b>	Config
<b>History</b>	3.2.3000
<b>Role</b>	admin
<b>Example</b>	<pre>switch (config) # aaa authentication attempts lockout enable</pre>
<b>Related Commands</b>	N/A
<b>Notes</b>	

## 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.

<b>Syntax Description</b>	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: <ul style="list-style-type: none"> <li>• Real remote usernames which simply failed authentication</li> <li>• Mis-typed remote usernames</li> <li>• Passwords accidentally entered as usernames</li> <li>• Bogus usernames made up as part of an attack on the system</li> </ul>
	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).
<b>Default</b>	N/A	
<b>Configuration Mode</b>	Config	
<b>History</b>	3.2.3000	
<b>Role</b>	admin	
<b>Example</b>	switch (config) # aaa authentication attempts class-override admin no-lockout	
<b>Related Commands</b>	N/A	
<b>Notes</b>		

## 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.

<b>Syntax Description</b>	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.
<b>Default</b>	N/A	
<b>Configuration Mode</b>	Config	
<b>History</b>	3.2.3000	
<b>Role</b>	admin	
<b>Example</b>	switch (config) # aaa authentication attempts reset user admin all	
<b>Related Commands</b>	N/A	
<b>Notes</b>		

## 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

<b>Syntax Description</b>	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.
<b>Default</b>	N/A	
<b>Configuration Mode</b>	Config	
<b>History</b>	3.2.3000	
<b>Role</b>	admin	
<b>Example</b>	switch (config) # aaa authentication attempts reset user admin no-clear-history	
<b>Related Commands</b>	N/A	
<b>Notes</b>		

## aaa authorization

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

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

<b>Syntax Description</b>	<table border="0"> <tr> <td>username</td><td>Specifies what local account the authenticated user will be logged on as when a user is authenticated (via RADIUS or TACACS+) and does not have a local account. If the username is local, this mapping is ignored.</td></tr> <tr> <td>order &lt;policy&gt;</td><td> Sets the user mapping behavior when authenticating users via RADIUS or TACACS+ to one of three choices. The order determines how the remote user mapping behaves. If the authenticated username is valid locally, no mapping is performed. The setting has the following three possible behaviors: <ul style="list-style-type: none"> <li>• 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.</li> <li>• 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.</li> <li>• local-only – maps all remote users to the user specified by the “aaa authorization map default-user &lt;user name&gt;” command. Any vendor attributes received by an authentication server are ignored.</li> </ul> </td></tr> </table>	username	Specifies what local account the authenticated user will be logged on as when a user is authenticated (via RADIUS or TACACS+) and does not have a local account. If the username is local, this mapping is ignored.	order <policy>	Sets the user mapping behavior when authenticating users via RADIUS or TACACS+ to one of three choices. The order determines how the remote user mapping behaves. If the authenticated username is valid locally, no mapping is performed. The setting has the following three possible behaviors: <ul style="list-style-type: none"> <li>• 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.</li> <li>• 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.</li> <li>• local-only – maps all remote users to the user specified by the “aaa authorization map default-user &lt;user name&gt;” command. Any vendor attributes received by an authentication server are ignored.</li> </ul>
username	Specifies what local account the authenticated user will be logged on as when a user is authenticated (via RADIUS or TACACS+) and does not have a local account. If the username is local, this mapping is ignored.				
order <policy>	Sets the user mapping behavior when authenticating users via RADIUS or TACACS+ to one of three choices. The order determines how the remote user mapping behaves. If the authenticated username is valid locally, no mapping is performed. The setting has the following three possible behaviors: <ul style="list-style-type: none"> <li>• 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.</li> <li>• 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.</li> <li>• local-only – maps all remote users to the user specified by the “aaa authorization map default-user &lt;user name&gt;” command. Any vendor attributes received by an authentication server are ignored.</li> </ul>				

<b>Default</b>	Default user - admin Map order - remote-first
<b>Configuration Mode</b>	Config
<b>History</b>	3.1.0000
<b>Role</b>	admin
<b>Example</b>	<pre>switch (config) # aaa authorization map default-user admin switch (config) # show aaa AAA authorization:     Default User: admin     Map Order: remote-first Authentication method(s):     local Accounting method(s):     tacacs+ switch (config) #</pre>

<b>Related Commands</b>	show aaa username
<b>Notes</b>	<ul style="list-style-type: none"><li>• 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.</li><li>• 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.</li><li>• The user must be careful when setting AAA authorization to “remote-only” because if the remote server happens to be configured incorrectly, then the user may lock themselves out.</li></ul>

## show aaa

### show aaa

Displays the AAA configuration.

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

## show aaa authentication attempts

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

Shows the current authentication, authorization and accounting settings.

<b>Syntax Description</b>	authentication attempts configured status user	Displays configuration and history of authentication failures. Displays configuration of authentication failure tracking. Displays status of authentication failure tracking and lockouts for specific user.												
<b>Default</b>	N/A													
<b>Configuration Mode</b>	Any Command Mode													
<b>History</b>	3.2.1000 3.5.0200	Updated Example												
<b>Role</b>	admin													
<b>Example</b>	<pre>switch (config) # show aaa authentication attempts Configuration for authentication failure tracking and locking:   Track authentication failures: yes   Lock accounts based on authentication failures: yes   Override treatment of 'admin' user: (none)   Override treatment of unknown usernames: hash-usernames   Convert usernames to lowercase for tracking: no   Delay after each auth failure (fail delay): none</pre> <pre>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</pre> <table> <thead> <tr> <th>Username</th> <th>Known</th> <th>Locked</th> <th>Failures</th> <th>Last fail time</th> <th>Last fail from</th> </tr> </thead> <tbody> <tr> <td>0Q72B43EHBKT8CB5AF5PGRX3U3B3TUL4CYJP93N(*)</td> <td>no</td> <td>no</td> <td>1</td> <td>2012/08/20 14:29:19</td> <td>ttyS0</td> </tr> </tbody> </table> <p>(*) Hashed for security reasons</p> <pre>switch-627d3c [standalone: master] (config) # switch (config) #</pre>		Username	Known	Locked	Failures	Last fail time	Last fail from	0Q72B43EHBKT8CB5AF5PGRX3U3B3TUL4CYJP93N(*)	no	no	1	2012/08/20 14:29:19	ttyS0
Username	Known	Locked	Failures	Last fail time	Last fail from									
0Q72B43EHBKT8CB5AF5PGRX3U3B3TUL4CYJP93N(*)	no	no	1	2012/08/20 14:29:19	ttyS0									
<b>Related Commands</b>	N/A													
<b>Notes</b>														

#### 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.

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

<b>Syntax Description</b>	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)
<b>Default</b>	3 seconds, 1 retry Default UDP port is 1812	
<b>Configuration Mode</b>	Config	
<b>History</b>	3.1.0000	
<b>Role</b>	admin	
<b>Example</b>	<pre>switch (config) # radius-server host 40.40.40.40 switch (config) # show radius RADIUS defaults:     Key:          3333     Timeout:      3     Retransmit:   1 RADIUS servers:     40.40.40.40:1812         Enabled:     yes         Key:          3333 (default)         Timeout:      3 (default)         Retransmit:   1 (default) switch (config) #</pre>	

**Related Commands**

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.

<b>Syntax Description</b>	N/A
<b>Default</b>	N/A
<b>Configuration Mode</b>	Any Command Mode
<b>History</b>	3.1.0000
<b>Role</b>	admin
<b>Example</b>	<pre>switch (config) # show radius RADIUS defaults:     Key:          3333     Timeout:      3     Retransmit:   1 RADIUS servers:     40.40.40.40:1812         Enabled:     yes         Key:          3333 (default)         Timeout:      3 (default)         Retransmit:   1 (default) switch (config) #</pre>
<b>Related Commands</b>	<a href="#">aaa authorization</a> <a href="#">radius-server</a> <a href="#">radius-server host</a>
<b>Notes</b>	

#### 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.

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

<b>Syntax Description</b>	
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)
<b>Default</b>	3 seconds, 1 retry Default TCP port is 49 Default auth-type is PAP
<b>Configuration Mode</b>	Config
<b>History</b>	3.1.0000
<b>Role</b>	admin

**Example**

```
switch (config) # tacacs-server host 40.40.40.40
switch (config) # show tacacs
TACACS+ defaults:
    Key:          3333
    Timeout:      3
    Retransmit:   1
TACACS+ servers:
    40.40.40.40:49
        Enabled:     yes
        Auth-type:   PAP
        Key:         3333 (default)
        Timeout:     3 (default)
        Retransmit:  1 (default)
switch (config) #
```

**Related Commands**

aaa authorization  
show tacacs  
tacacs-server

**Notes**

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

## show tacacs

### show tacacs

Displays TACACS+ configurations.

<b>Syntax Description</b>	N/A
<b>Default</b>	N/A
<b>Configuration Mode</b>	Any Command Mode
<b>History</b>	3.1.0000
<b>Role</b>	admin
<b>Example</b>	<pre>switch (config) # show tacacs TACACS+ defaults:     Key:          3333     Timeout:      3     Retransmit:   1 TACACS+ servers:     40.40.40.40:49         Enabled:     yes         Auth-type:   PAP         Key:         3333 (default)         Timeout:     3 (default)         Retransmit:  1 (default) switch (config) #</pre>
<b>Related Commands</b>	<a href="#">aaa authorization</a> <a href="#">tacacs-server</a> <a href="#">tacacs-server host</a>
<b>Notes</b>	

#### 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.

<b>Syntax Description</b>	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
<b>Default</b>	ou=users,dc=example,dc=com	
<b>Configuration Mode</b>	Config	
<b>History</b>	3.1.0000	
	3.4.0000	Updated Example
<b>Role</b>	admin	
<b>Example</b>	<pre>switch (config) # ldap base-dn ou=department,dc=example,dc=com switch (config) # show ldap User base DN      : ou=department,dc=example,dc=com User search scope : subtree Login attribute   : sAMAccountName Bind DN          : Bind password    : Group base DN    : Group attribute   : member LDAP version     : 3 Referrals        : yes Server port      : 389 Search Timeout   : 5 Bind Timeout     : 5 SSL mode         : none Server SSL port  : 636 (not active) SSL ciphers      : TLS1.2 (not active) SSL cert verify  : yes SSL ca-list       : default-ca-list  LDAP servers:  1: 10.10.10.10  2: 10.10.10.12 switch (config) #</pre>	

---

**Related Commands** show ldap

---

**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.

<b>Syntax Description</b>	string	A case-sensitive string that specifies distinguished name or password to bind to on the LDAP server.
<b>Default</b>	""	
<b>Configuration Mode</b>	Config	
<b>History</b>	3.1.0000	
	3.4.0000	Updated Example
<b>Role</b>	admin	
<b>Example</b>	<pre>switch (config) # ldap bind-dn my-dn switch (config) # ldap bind-password my-password switch (config) # show ldap User base DN      : ou=department,dc=example,dc=com User search scope : subtree Login attribute   : sAMAccountName Bind DN          : my-dn Bind password    : my-password Group base DN    : Group attribute  : member LDAP version     : 3 Referrals        : yes Server port      : 389 Search Timeout   : 5 Bind Timeout     : 5 SSL mode         : none Server SSL port  : 636 (not active) SSL ciphers      : TLS1.2 (not active) SSL cert verify  : yes SSL ca-list       : default-ca-list  LDAP servers:   1: 10.10.10.10   2: 10.10.10.12 switch (config) #</pre>	
<b>Related Commands</b>	show ldap	
<b>Notes</b>	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.

<b>Syntax Description</b>	group-att member uniqueMember group-dn	Specifies a custom attribute name. groupOfNames or group membership attribute. groupOfUniqueNames membership attribute. DN of group required for authorization.
<b>Default</b>	group-att: member group-dn: “”	
<b>Configuration Mode</b>	Config	
<b>History</b>	3.1.0000 3.4.0000	Updated Example
<b>Role</b>	admin	
<b>Example</b>	<pre>switch (config) # ldap group-attribute member switch (config) # ldap group-dn my-group-dn switch (config) # show ldap User base DN      : ou=department,dc=example,dc=com User search scope : subtree Login attribute   : sAMAccountName Bind DN          : my-dn Bind password    : my-password Group base DN    : my-group-dn Group attribute   : member LDAP version     : 3 Referrals        : yes Server port      : 389 Search Timeout   : 5 Bind Timeout     : 5 SSL mode         : none Server SSL port  : 636 (not active) SSL ciphers      : TLS1.2 (not active) SSL cert verify  : yes SSL ca-list       : default-ca-list  LDAP servers:  1: 10.10.10.10  2: 10.10.10.12 switch (config) #</pre>	

**Related Commands**

show ldap

**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.

<b>Syntax Description</b>	IP Address number last	IPv4 or IPv6 address. The order of the LDAP server. The LDAP server will be added in the last location.
<b>Default</b>	No hosts configured	
<b>Configuration Mode</b>	Config	
<b>History</b>	3.1.0000 3.4.0000	Updated Example
<b>Role</b>	admin	
<b>Example</b>	<pre>switch (config) # ldap host 10.10.10.10 switch (config) # show ldap User base DN      : ou=department,dc=example,dc=com User search scope : subtree Login attribute   : sAMAccountName Bind DN          : my-dn Bind password    : my-password Group base DN    : my-group-dn Group attribute   : member LDAP version     : 3 Referrals         : yes Server port       : 389 Search Timeout   : 5 Bind Timeout     : 5 SSL mode          : none Server SSL port  : 636 (not active) SSL ciphers       : TLS1.2 (not active) SSL cert verify   : yes SSL ca-list       : default-ca-list  LDAP servers:   1: 10.10.10.10   2: 10.10.10.12 switch (config) #</pre>	
<b>Related Commands</b>	<a href="#">show aaa</a> <a href="#">show ldap</a>	
<b>Notes</b>	<ul style="list-style-type: none"> <li>The system will select the LDAP host to try according to its order</li> <li>New servers are by default added at the end of the list of servers</li> </ul>	

## 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.

<b>Syntax Description</b>	string uid sAMAccountName	Custom attribute name. LDAP login name is taken from the user login user-name. SAM Account name, active directory login name.
<b>Default</b>	sAMAccountName	
<b>Configuration Mode</b>	Config	
<b>History</b>	3.1.0000 3.4.0000	Updated Example
<b>Role</b>	admin	
<b>Example</b>	<pre>switch (config) # ldap login-attribute uid switch (config) # show ldap User base DN      : ou=department,dc=example,dc=com User search scope : subtree Login attribute   : uid Bind DN          : my-dn Bind password    : my-password Group base DN    : my-group-dn Group attribute   : member LDAP version     : 3 Referrals        : yes Server port      : 389 Search Timeout   : 5 Bind Timeout     : 5 SSL mode         : none Server SSL port  : 636 (not active) SSL ciphers      : TLS1.2 (not active) SSL cert verify  : yes SSL ca-list       : default-ca-list  LDAP servers:  1: 10.10.10.10  2: 10.10.10.12 switch (config) #</pre>	
<b>Related Commands</b>	show aaa show ldap	
<b>Notes</b>		

## 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.

<b>Syntax Description</b>	port	TCP port number.
<b>Default</b>	389	
<b>Configuration Mode</b>	Config	
<b>History</b>	3.1.0000	
	3.4.0000	Updated Example
<b>Role</b>	admin	
<b>Example</b>	<pre>switch (config) # ldap port 1111 switch (config) # show ldap User base DN      : ou=department,dc=example,dc=com User search scope : subtree Login attribute   : uid Bind DN          : my-dn Bind password    : my-password Group base DN    : my-group-dn Group attribute   : member LDAP version     : 3 Referrals        : yes Server port       : 1111 Search Timeout   : 5 Bind Timeout     : 5 SSL mode         : none Server SSL port  : 636 (not active) SSL ciphers      : TLS1.2 (not active) SSL cert verify  : yes SSL ca-list       : default-ca-list  LDAP servers:  1: 10.10.10.10  2: 10.10.10.12 switch (config) #</pre>	
<b>Related Commands</b>	<a href="#">show aaa</a> <a href="#">show ldap</a>	
<b>Notes</b>		

## ldap referrals

**ldap referrals**  
**no ldap referrals**

Enables LDAP referrals.  
The no form of the command disables LDAP referrals.

<b>Syntax Description</b>	N/A
<b>Default</b>	LDAP referrals are enabled
<b>Configuration Mode</b>	Config
<b>History</b>	3.1.0000
	3.4.0000 Updated Example
<b>Role</b>	admin
<b>Example</b>	<pre>switch (config) # no ldap referrals switch (config) # show ldap User base DN      : ou=department,dc=example,dc=com User search scope : subtree Login attribute   : uid Bind DN          : my-dn Bind password    : my-password Group base DN    : my-group-dn Group attribute   : member LDAP version     : 3 Referrals        : no Server port       : 1111 Search Timeout   : 5 Bind Timeout     : 5 SSL mode         : none Server SSL port  : 636 (not active) SSL ciphers      : TLS1.2 (not active) SSL cert verify  : yes SSL ca-list       : default-ca-list  LDAP servers:  1: 10.10.10.10  2: 10.10.10.12 switch (config) #</pre>
<b>Related Commands</b>	<a href="#">show aaa</a> <a href="#">show ldap</a>
<b>Notes</b>	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.

<b>Syntax Description</b>	scope	<ul style="list-style-type: none"> <li>one-level - searches the immediate children of the base dn</li> <li>subtree - searches at the base DN and all its children</li> </ul>
<b>Default</b>	subtree	
<b>Configuration Mode</b>	Config	
<b>History</b>	3.1.0000	
	3.4.0000	Updated Example
<b>Role</b>	admin	
<b>Example</b>	<pre>switch (config) # ldap scope subtree switch (config) # show ldap User base DN      : ou=department,dc=example,dc=com User search scope : subtree Login attribute   : uid Bind DN           : my-dn Bind password    : my-password Group base DN    : my-group-dn Group attribute   : member LDAP version     : 3 Referrals         : no Server port       : 1111 Search Timeout    : 5 Bind Timeout      : 5 SSL mode          : none Server SSL port   : 636 (not active) SSL ciphers       : TLS1.2 (not active) SSL cert verify   : yes SSL ca-list        : default-ca-list  LDAP servers:  1: 10.10.10.10  2: 10.10.10.12 switch (config) #</pre>	
<b>Related Commands</b>	<a href="#">show aaa</a> <a href="#">show ldap</a>	
<b>Notes</b>		

## ldap ssl

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

Sets SSL parameter for LDAP.

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

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



## 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.

<b>Syntax Description</b>	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.
<b>Default</b>	5 seconds	
<b>Configuration Mode</b>	Config	
<b>History</b>	3.1.0000	
	3.4.0000	Updated Example
<b>Role</b>	admin	
<b>Example</b>	<pre>switch (config) # ldap timeout-bind 10 switch (config) # show ldap User base DN      : ou=department,dc=example,dc=com User search scope : subtree Login attribute   : uid Bind DN           : my-dn Bind password     : my-password Group base DN    : my-group-dn Group attribute   : member LDAP version      : 3 Referrals         : no Server port       : 1111 Search Timeout    : 5 Bind Timeout      : 10 SSL mode          : none Server SSL port   : 636 (not active) SSL ciphers       : TLS1.2 (not active) SSL cert verify   : yes SSL ca-list        : default-ca-list  LDAP servers:  1: 10.10.10.10  2: 10.10.10.12 switch (config) #</pre>	

---

**Related Commands**

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.

<b>Syntax Description</b>	version	Sets the LDAP version. Values: 2 and 3.
<b>Default</b>	3	
<b>Configuration Mode</b>	Config	
<b>History</b>	3.1.0000	
	3.4.0000	Updated Example
<b>Role</b>	admin	
<b>Example</b>	<pre>switch (config) # ldap version 3 switch (config) # show ldap User base DN      : ou=department,dc=example,dc=com User search scope : subtree Login attribute   : uid Bind DN           : my-dn Bind password    : my-password Group base DN    : my-group-dn Group attribute   : member LDAP version     : 3 Referrals         : no Server port       : 1111 Search Timeout   : 5 Bind Timeout     : 10 SSL mode          : none Server SSL port  : 636 (not active) SSL ciphers       : TLS1.2 (not active) SSL cert verify  : yes SSL ca-list       : default-ca-list  LDAP servers:  1: 10.10.10.10  2: 10.10.10.12 switch (config) #</pre>	
<b>Related Commands</b>	<a href="#">show aaa</a> <a href="#">show ldap</a>	
<b>Notes</b>		

## show ldap

### show ldap

Displays LDAP configurations.

<b>Syntax Description</b>	N/A
<b>Default</b>	N/A
<b>Configuration Mode</b>	Any Command Mode
<b>History</b>	3.1.0000
	3.4.0000 Updated Example
<b>Role</b>	admin
<b>Example</b>	<pre>switch (config) # show ldap User base DN      : ou=department,dc=example,dc=com User search scope : subtree Login attribute   : uid Bind DN          : my-dn Bind password    : my-password Group base DN    : my-group-dn Group attribute   : member LDAP version     : 3 Referrals        : no Server port      : 1111 Search Timeout   : 5 Bind Timeout     : 10 SSL mode         : none Server SSL port  : 636 (not active) SSL ciphers      : TLS1.2 (not active) SSL cert verify  : yes SSL ca-list       : default-ca-list  LDAP servers:  1: 10.10.10.10  2: 10.10.10.12 switch (config) #</pre>
<b>Related Commands</b>	<a href="#">show aaa</a> <a href="#">show ldap</a>
<b>Notes</b>	

#### 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.

<b>Syntax Description</b>	N/A
<b>Default</b>	Disabled
<b>Configuration Mode</b>	Config
<b>History</b>	3.5.0200
<b>Role</b>	admin
<b>Example</b>	<pre>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</pre>
<b>Related Commands</b>	<pre>user &lt;username&gt; password &lt;password&gt; ssh server min-version ssh server security strict snmp-server user no neighbor &lt;ip-address&gt; password ntp server disable ntp server keyID router bgp neighbor password router bgp peer-group password</pre>
<b>Notes</b>	<p>Before enabling secure mode, the command performs the following configuration checks:</p> <ul style="list-style-type: none"> <li>• NTP Key ID cannot be MD5 when secure mode is enabled</li> <li>• SSH min-version cannot be 1 when enabling secure mode</li> <li>• SSH security must be set to strict security</li> <li>• SNMPv3 user auth cannot be md5 when enabling secure mode</li> <li>• SNMPv3 user priv cannot be des when enabling secure mode</li> <li>• SNMPv3 trap auth cannot be md5 when enabling secure mode</li> <li>• SNMPv3 trap priv cannot be des when enabling secure mode</li> <li>• Router BGP neighbor password cannot be set when enabling secure mode</li> <li>• Router BGP peer-group password cannot be set when enabling with secure mode</li> <li>• User password hash cannot be MD5 when secure mode is enabled</li> </ul> <p>Only if the check passes, secure mode is enabled on the switch system.</p>

## show system secure-mode

### show system secure-mode

Displays the security mode of the switch system.

<b>Syntax Description</b>	N/A
<b>Default</b>	N/A
<b>Configuration Mode</b>	Any Command Mode
<b>History</b>	3.4.2300
<b>Role</b>	admin
<b>Example</b>	<pre>switch (config) # show system secure-mode  Secure mode configured: yes Secure mode enabled : yes switch (config) #</pre>
<b>Related Commands</b>	system secure-mode enable
<b>Notes</b>	<p>“Secure mode configuration” describes the user configuration “Secure mode enabled” describes the system state</p>

## 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
- 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.

<b>Syntax Description</b>	key-location	Configures where to store the encryption key: <ul style="list-style-type: none"> <li>• local – Stores the key locally</li> <li>• usb – Stores the key on a USB device</li> </ul>
	key	Configures a key
<b>Default</b>	N/A	
<b>Configuration Mode</b>	Config	
<b>History</b>	3.6.1002	
<b>Role</b>	admin	
<b>Example</b>	<pre>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</pre>	
<b>Related Commands</b>		
<b>Notes</b>	<ul style="list-style-type: none"> <li>• It is recommended to store the encryption password on a USB device rather than locally</li> <li>• Enabling encryption may slightly slow system performance</li> <li>• 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.</li> </ul>	

## 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

<b>Syntax Description</b>	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)
<b>Default</b>	N/A	
<b>Configuration Mode</b>	Config	
<b>History</b>	3.2.3000	
<b>Role</b>	admin	
<b>Example</b>	<pre>switch (config)# crypto ipsec ike restart switch (config)#</pre>	
<b>Related Commands</b>	N/A	
<b>Notes</b>		

## **crypto ipsec peer local**

```
crypto ipsec peer <IPv4 or IPv6 address> local <IPv4 or IPv6 address> {enable |  
keying {ike [auth {hmac-md5 | hmac-sha1 | hmac-sha256 | null} | dh-group | dis-  
able | encrypt | exchange-mode | lifetime | local | mode | peer-identity | pfs-group |  
preshared-key | prompt-preshared-key | transform-set] | manual [auth | disable |  
encrypt | local-spi | mode | remote-spi]}{}}
```

Configures ipsec in the system.

Syntax Description	enable	Enables IPSec peering.
ike		<p>Configures IPSec peering using IKE ISAKMP to manage SA keys. It has the following optional parameters:</p> <ul style="list-style-type: none"> <li>• auth: Configures the authentication algorithm for IPSec peering</li> <li>• dh-group: Configures the phase1 Diffie-Hellman group proposed for secure IKE key exchange</li> <li>• disable: Configures this IPSec peering administratively disabled</li> <li>• encrypt: Configures the encryption algorithm for IPSec peering</li> <li>• exchange-mode: Configures the IKE key exchange mode to propose for peering</li> <li>• lifetime: Configures the SA lifetime to propose for this IPSec peering</li> <li>• local-identity: Configures the ISAKMP payload identification value to send as local endpoint's identity</li> <li>• mode: Configures the peering mode for this IPSec peering</li> <li>• peer-identity: Configures the identification value to match against the peer's ISAKMP payload identification</li> <li>• pfs-group: Configures the phase2 PFS (Perfect Forwarding Secrecy) group to propose for Diffie-Hellman exchange for this IPSec peering</li> <li>• preshared-key: Configures the IKE pre-shared key for the IPSec peering</li> <li>• prompt-preshared-key: Prompts for the pre-shared key, rather than entering it on the command line</li> <li>• transform-set: Configures transform proposal parameters</li> </ul>
keying		<p>Configures key management for this IPSec peering:</p> <ul style="list-style-type: none"> <li>• auth: Configures the authentication algorithm for this IPSec peering</li> <li>• disable: Configures this IPSec peering administratively disabled</li> <li>• encrypt: Configures the encryption algorithm for this IPSec peering</li> <li>• local-spi: Configures the local SPI for this manual IPSec peering</li> <li>• mode: Configures the peering mode for this IPSec peering</li> <li>• remote-spi: Configures the remote SPI for this manual IPSec peering</li> </ul>
manual		Configures IPSec peering using manual keys.
<b>Default</b>	N/A	

<b>Configuration Mode</b>	Config
<b>History</b>	3.2.3000
<b>Role</b>	admin
<b>Example</b>	<pre>switch (config)# crypto ipsec peer 10.10.10.10 local 10.7.34.139 enable</pre> <pre>switch (config)#</pre>
<b>Related Commands</b>	N/A
<b>Notes</b>	

## 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.

<b>Syntax Description</b>	cert-name	The name of the certificate.
<b>Default</b>	N/A	
<b>Configuration Mode</b>	Config	
<b>History</b>	3.2.3000	
<b>Role</b>	admin	
<b>Example</b>	switch (config) # crypto certificate default-cert name test	
<b>Related Commands</b>	N/A	
<b>Notes</b>	<ul style="list-style-type: none"><li>Two certificates with the same subject and issuer fields cannot both be placed onto the CA list</li><li>The no form of the command does not delete the certificate from the certificate database</li><li>Unless specified otherwise, applications that use CA certificates will still consult the well-known certificate bundle before looking at the default-ca-list</li></ul>	

## 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).

<b>Syntax Description</b>	cert-name	The name of the certificate.
<b>Default</b>	N/A	
<b>Configuration Mode</b>	Config	
<b>History</b>	3.2.3000	
<b>Role</b>	admin	
<b>Example</b>	switch (config) # crypto certificate default-cert name test	
<b>Related Commands</b>	N/A	
<b>Notes</b>	<ul style="list-style-type: none"><li>• A certificate must already be defined before it can be configured in the default-cert role</li><li>• 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</li></ul>	

## 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.

<b>Syntax Description</b>	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.
<b>Default</b>	N/A	
<b>Configuration Mode</b>	Config	
<b>History</b>	3.2.1000	
	3.3.4350	Added “hash-algorithm” parameter
	3.6.4000	Added “days-valid” parameter
<b>Role</b>	admin	
<b>Example</b>	switch (config) # crypto certificate generation default hash-algorithm sha256	
<b>Related Commands</b>	N/A	
<b>Notes</b>	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	<p>Generates certificates. This option has the following parameters which may be entered sequentially in any order:</p> <ul style="list-style-type: none"> <li>• comment: Specifies a certificate comment (free string)</li> <li>• common-name: Specifies the common name of the issuer and subject (e.g. a domain name)</li> <li>• country-code: Specifies the country codwo-alpha-numeric-character country code, or “--” for none)</li> <li>• days-valid: Specifies the number of days the certificate is valid</li> <li>• email-addr: Specifies the email address</li> <li>• hash-algorithm: Specifies the hashing function used for signature algorithm. Default value is SHA256.</li> <li>• 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)</li> <li>• locality: Specifies the locality name</li> <li>• org-unit: Specifies the organizational unit name</li> <li>• organization: Specifies the organization name</li> <li>• serial-num: Specifies the serial number for the certificate (a lower-case hexadecimal serial number prefixed with “0x”)</li> <li>• state-or-prov: Specifies the state or province name</li> </ul>
	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.
<b>Default</b>	N/A	
<b>Configuration Mode</b>	Config	
<b>History</b>	3.2.3000	
	3.3.4402	Added “hash-algorithm” parameter
	3.6.4000	Added “hash-algorithm” parameter
<b>Role</b>	admin	
<b>Example</b>	<pre>switch (config) # crypto certificate name system-self-signed generate self-signed hash-algorithm sha256</pre>	

---

**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.

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

## 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.

<b>Syntax Description</b>	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
<b>Default</b>	N/A	
<b>Configuration Mode</b>	Config	
<b>History</b>	3.2.1000	
<b>Role</b>	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.

<b>Syntax Description</b>	N/A
<b>Default</b>	N/A
<b>Configuration Mode</b>	Config
<b>History</b>	3.6.1002
<b>Role</b>	admin
<b>Example</b>	<pre>switch (config)# show crypto encrypt-data Sensitive files encryption:     Status:          enabled     Key location:   usb     Cipher:         aes256 switch (config)#+</pre>
<b>Related Commands</b>	N/A
<b>Notes</b>	

## show crypto ipsec

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

Displays information ipsec configuration.

<b>Syntax Description</b>	N/A
<b>Default</b>	N/A
<b>Configuration Mode</b>	Config
<b>History</b>	3.2.1000
<b>Role</b>	admin
<b>Example</b>	<pre>switch (config)# show crypto ipsec IPSec Summary ----- Crypto IKE is using pluto (Openswan) daemon. Daemon process state is stopped.  No IPSec peers configured.  IPSec IKE Peering State ----- Crypto IKE is using pluto (Openswan) daemon. Daemon process state is stopped.  No active IPSec IKE peers.  IPSec Policy State ----- No active IPSec policies.  IPSec Security Association State ----- No active IPSec security associations. switch (config)# </pre>
<b>Related Commands</b>	N/A
<b>Notes</b>	

## 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.

<b>Syntax Description</b>	job ID	An integer.
<b>Default</b>	N/A	
<b>Configuration Mode</b>	Config	
<b>History</b>	3.1.0000	
<b>Role</b>	admin	
<b>Example</b>	<pre>switch (config) # job 100 switch (config job 100) #</pre>	
<b>Related Commands</b>	show jobs	
<b>Notes</b>	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.

<b>Syntax Description</b>	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.
<b>Default</b>	N/A	
<b>Configuration Mode</b>	Config job	
<b>History</b>	3.1.0000	
<b>Role</b>	admin	
<b>Example</b>	<pre>switch (config)# job 100 switch (config job 100) # command 10 "show power" switch (config job 100) #</pre>	
<b>Related Commands</b>	show jobs	
<b>Notes</b>	<ul style="list-style-type: none"><li>• The command must be defined with inverted commas (")</li><li>• 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 &lt;type&gt; &lt;number&gt; description my-description".</li></ul>	

## comment

**comment <comment>**  
**no comment**

Adds a comment to the job.  
The no form of the command deletes the comment.

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

## enable

**enable**  
**no enable**

Enables the specified job.

The no form of the command disables the specified job.

<b>Syntax Description</b>	N/A
<b>Default</b>	N/A
<b>Configuration Mode</b>	Config job
<b>History</b>	3.1.0000
<b>Role</b>	admin
<b>Example</b>	<pre>switch (config)# job 100 switch (config job 100) # enable switch (config job 100) #</pre>
<b>Related Commands</b>	show jobs
<b>Notes</b>	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.

<b>Syntax Description</b>	N/A
<b>Default</b>	N/A
<b>Configuration Mode</b>	Config job
<b>History</b>	3.1.0000
<b>Role</b>	admin
<b>Example</b>	<pre>switch (config)# job 100 switch (config job 100) # execute switch (config job 100) #</pre>
<b>Related Commands</b>	show jobs
<b>Notes</b>	<ul style="list-style-type: none"><li>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</li><li>The job will not be run if not currently enabled</li></ul>

## 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.

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

**name**

**name <job name>**  
**no name**

Configures a name for this job.  
The no form of the command resets the name to its default.

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

## 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.

<b>Syntax Description</b>	recurrence type	The available schedule types are: <ul style="list-style-type: none"><li>• daily - the job is executed every day at a specified time</li><li>• weekly - the job is executed on a weekly basis</li><li>• monthly - the job is executed every month on a specified day of the month</li><li>• once - the job is executed once at a single specified date and time</li><li>• periodic - the job is executed on a specified fixed time interval, starting from a fixed point in time.</li></ul>
<b>Default</b>	once	
<b>Configuration Mode</b>	Config job	
<b>History</b>	3.1.0000	
<b>Role</b>	admin	
<b>Example</b>	<pre>switch (config)# job 100 switch (config job 100) # schedule type once switch (config job 100) #</pre>	
<b>Related Commands</b>	show jobs	
<b>Notes</b>	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.

<b>Syntax Description</b>	recurrence type	The available schedule types are: <ul style="list-style-type: none"> <li>• daily - the job is executed every day at a specified time</li> <li>• weekly - the job is executed on a weekly basis</li> <li>• monthly - the job is executed every month on a specified day of the month</li> <li>• once - the job is executed once at a single specified date and time</li> <li>• periodic - the job is executed on a specified fixed time interval, starting from a fixed point in time.</li> </ul>
<b>Default</b>	once	interval and date
<b>Configuration Mode</b>	Config job	Interval and date, per recurrence type.
<b>History</b>	3.1.0000	
<b>Role</b>	admin	
<b>Example</b>	<pre>switch (config)# job 100 switch (config job 100) # schedule monthly interval 10 switch (config job 100) #</pre>	
<b>Related Commands</b>	show jobs	
<b>Notes</b>	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.

<b>Syntax Description</b>	job-id	Job ID.
<b>Default</b>	N/A	
<b>Configuration Mode</b>	Config	
<b>History</b>	3.1.0000	
<b>Role</b>	admin	
<b>Example</b>	<pre>switch (config) # show jobs 10 Job 10:     Status:           inactive     Enabled:          yes     Continue on failure: no     Schedule Type:   once     Time and date:   1970/01/01 00:00:00 +0000     Last Exec Time:  Thu 2012/04/05 13:11:42 +0000     Next Exec Time:  N/A     Commands:         Command 10: show power     Last Output: ===== Module      Status ===== PS1         OK PS2         NOT PRESENT  switch (config) #</pre>	
<b>Related Commands</b>	<a href="#">show jobs</a>	
<b>Notes</b>		

## 4.15 Statistics and Alarms

### 4.15.1 Commands

#### stats alarm <alarm-id> clear

```
stats alarm <alarm ID> clear
```

Clears alarm state.

<b>Syntax Description</b>	alarm ID	Alarms supported by the system, for example: <ul style="list-style-type: none"><li>• cpu_util_indiv - Average CPU utilization too high: percent utilization</li><li>• disk_io - Operating System Disk I/O per second too high: kilobytes per second</li><li>• fs_mnt - Free filesystem space too low: percent of disk space free</li><li>• intf_util - Network utilization too high: bytes per second</li><li>• memory_pct_used - Too much memory in use: percent of physical memory used</li><li>• paging - Paging activity too high: page faults</li><li>• temperature - Temperature is too high: degrees</li></ul>
<b>Default</b>	N/A	
<b>Configuration Mode</b>	Config	
<b>History</b>	3.1.0000	
<b>Role</b>	admin	
<b>Example</b>		<pre>switch (config) # stats alarm cpu_util_indiv clear switch (config) #</pre>
<b>Related Commands</b>	show stats alarm	
<b>Notes</b>		

## 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.

<b>Syntax Description</b>	alarm ID	Alarms supported by the system, for example: <ul style="list-style-type: none"><li>• cpu_util_indiv - Average CPU utilization too high: percent utilization</li><li>• disk_io - Operating System Disk I/O per second too high: kilobytes per second</li><li>• fs_mnt - Free filesystem space too low: percent of disk space free</li><li>• intf_util - Network utilization too high: bytes per second</li><li>• memory_pct_used - Too much memory in use: percent of physical memory used</li><li>• paging - Paging activity too high: page faults</li><li>• temperature - Temperature is too high: degrees</li></ul>
<b>Default</b>	The default is different per alarm-id	
<b>Configuration Mode</b>	Config	
<b>History</b>	3.1.0000	
<b>Role</b>	admin	
<b>Example</b>		<pre>switch (config) # stats alarm cpu_util_indiv enable switch (config) #</pre>
<b>Related Commands</b>	show stats alarm	
<b>Notes</b>		

## **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.

<b>Syntax Description</b>	alarm ID	Alarms supported by the system, for example: <ul style="list-style-type: none"> <li>• cpu_util_indiv - Average CPU utilization too high: percent utilization</li> <li>• disk_io - Operating System Disk I/O per second too high: kilobytes per second</li> <li>• fs_mnt - Free filesystem space too low: percent of disk space free</li> <li>• intf_util - Network utilization too high: bytes per second</li> <li>• memory_pct_used - Too much memory in use: percent of physical memory used</li> <li>• paging - Paging activity too high: page faults</li> <li>• temperature - Temperature is too high: degrees</li> </ul>
	single	Does not repeat events: only sends one event whenever the alarm changes state.
	while-not-cleared	Repeats error events until the alarm clears.
<b>Default</b>	single	
<b>Configuration Mode</b>	Config	
<b>History</b>	3.1.0000	
<b>Role</b>	monitor/admin	
<b>Example</b>	<pre>switch (config) # stats alarm cpu_util_indiv event-repeat single switch (config) #</pre>	
<b>Related Commands</b>	show stats alarm	
<b>Notes</b>		

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

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

Configure alarms thresholds.

<b>Syntax Description</b>	alarm ID	Alarms supported by the system, for example: <ul style="list-style-type: none"> <li>• cpu_util_indiv - Average CPU utilization too high: percent utilization</li> <li>• disk_io - Operating System Disk I/O per second too high: kilobytes per second</li> <li>• fs_mnt - Free filesystem space too low: percent of disk space free</li> <li>• intf_util - Network utilization too high: bytes per second</li> <li>• memory_pct_used - Too much memory in use: percent of physical memory used</li> <li>• paging - Paging activity too high: page faults</li> <li>• temperature - Temperature is too high: degrees</li> </ul>
	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.
<b>Default</b>	Default is different per alarm-id	
<b>Configuration Mode</b>	Config	
<b>History</b>	3.1.0000	
<b>Role</b>	admin	
<b>Example</b>	<pre>switch (config) # stats alarm cpu_util_indiv falling clear-threshold 10 switch (config) #</pre>	
<b>Related Commands</b>	show stats alarm	
<b>Notes</b>	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.

<b>Syntax Description</b>	alarm ID	Alarms supported by the system, for example: <ul style="list-style-type: none"> <li>• cpu_util_indiv - Average CPU utilization too high: percent utilization</li> <li>• disk_io - Operating System Disk I/O per second too high: kilobytes per second</li> <li>• fs_mnt - Free filesystem space too low: percent of disk space free</li> <li>• intf_util - Network utilization too high: bytes per second</li> <li>• memory_pct_used - Too much memory in use: percent of physical memory used</li> <li>• paging - Paging activity too high: page faults</li> <li>• temperature - Temperature is too high: degrees</li> </ul>
	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.
<b>Default</b>		Short window: 5 alarms in 1 hour Medium window: 20 alarms in 1 day Long window: 50 alarms in 7 days
<b>Configuration Mode</b>		Config
<b>History</b>		3.1.0000
<b>Role</b>		monitor/admin
<b>Example</b>		<pre>switch (config) # stats alarm paging rate-limit window long 2000 switch (config) #</pre>
<b>Related Commands</b>		show stats alarm
<b>Notes</b>		

## **stats chd <chd-id> clear**

**stats chd <CHD ID> clear**

Clears CHD counters.

<b>Syntax Description</b>	CHD ID	CHD supported by the system, for example: <ul style="list-style-type: none"> <li>• cpu_util - CPU utilization: percentage of time spent</li> <li>• cpu_util_ave - CPU utilization average: percentage of time spent</li> <li>• cpu_util_day - CPU utilization average: percentage of time spent</li> <li>• disk_device_io_hour - Storage device I/O read/write statistics for the last hour: bytes</li> <li>• disk_io - Operating system aggregate disk I/O average (KB/sec)</li> <li>• eth_day</li> <li>• eth_hour</li> <li>• eth_ip_day</li> <li>• eth_ip_hour</li> <li>• fs_mnt_day - Filesystem system usage average: bytes</li> <li>• fs_mnt_month - Filesystem system usage average: bytes</li> <li>• fs_mnt_week - Filesystem system usage average: bytes</li> <li>• ib_day</li> <li>• ib_hour</li> <li>• intf_day - Network interface statistics aggregation: bytes</li> <li>• intf_hour - Network interface statistics (same as “interface” sample)</li> <li>• intf_util - Aggregate network utilization across all interfaces</li> <li>• memory_day - Average physical memory usage: bytes</li> <li>• memory_pct - Average physical memory usage</li> <li>• paging - Paging activity: page faults</li> <li>• paging_day - Paging activity: page faults</li> </ul>
<b>Default</b>	N/A	
<b>Configuration Mode</b>	Config	
<b>History</b>	3.1.0000	
<b>Role</b>	admin	
<b>Example</b>	<pre>switch (config) # stats chd memory_day clear switch (config) #</pre>	

---

**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.

---

<b>Syntax Description</b>	chd-id	CHD supported by the system, for example:
		<ul style="list-style-type: none"> <li>• cpu_util - CPU utilization: percentage of time spent</li> <li>• cpu_util_ave - CPU utilization average: percentage of time spent</li> <li>• cpu_util_day - CPU utilization average: percentage of time spent</li> <li>• disk_device_io_hour - Storage device I/O read/write statistics for the last hour: bytes</li> <li>• disk_io - Operating system aggregate disk I/O average: KB/sec</li> <li>• eth_day</li> <li>• eth_hour</li> <li>• fs_mnt_day - Filesystem system usage average: bytes</li> <li>• fs_mnt_month - Filesystem system usage average: bytes</li> <li>• fs_mnt_week - Filesystem system usage average: bytes</li> <li>• ib_day</li> <li>• ib_hour</li> <li>• intf_day - Network interface statistics aggregation: bytes</li> <li>• intf_hour - Network interface statistics (same as “interface” sample)</li> <li>• intf_util - Aggregate network utilization across all interfaces</li> <li>• memory_day - Average physical memory usage: bytes</li> <li>• memory_pct - Average physical memory usage</li> <li>• paging - Paging activity: page faults</li> <li>• paging_day - Paging activity: page faults</li> </ul>
<b>Default</b>	Enabled	
<b>Configuration Mode</b>	Config	
<b>History</b>	3.1.0000	
<b>Role</b>	monitor/admin	
<b>Example</b>	<pre>switch (config) # stats chd memory_day enable switch (config) #</pre>	

---

---

**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.

<b>Syntax Description</b>	CHD ID	Possible IDs: <ul style="list-style-type: none"> <li>• cpu_util - CPU utilization: percentage of time spent</li> <li>• cpu_util_ave - CPU utilization average: percentage of time spent</li> <li>• cpu_util_day - CPU utilization average: percentage of time spent</li> <li>• disk_device_io_hour - Storage device I/O read/write statistics for the last hour: bytes</li> <li>• disk_io - Operating system aggregate disk I/O average: KB/sec</li> <li>• eth_day</li> <li>• eth_hour</li> <li>• fs_mnt_day - Filesystem system usage average: bytes</li> <li>• fs_mnt_month - Filesystem system usage average: bytes</li> <li>• fs_mnt_week - Filesystem system usage average: bytes</li> <li>• ib_day</li> <li>• ib_hour</li> <li>• intf_day - Network interface statistics aggregation: bytes</li> <li>• intf_hour - Network interface statistics (same as “interface” sample)</li> <li>• intf_util - Aggregate network utilization across all interfaces</li> <li>• memory_day - Average physical memory usage: bytes</li> <li>• memory_pct - Average physical memory usage</li> <li>• paging - Paging activity: page faults</li> <li>• paging_day - Paging activity: page faults</li> </ul>
	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.
<b>Default</b>	Different per CHD	
<b>Configuration Mode</b>	Config	
<b>History</b>	3.1.0000	
<b>Role</b>	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.

<b>Syntax Description</b>	sample ID	Possible sample IDs are: <ul style="list-style-type: none"> <li>• congested</li> <li>• cpu_util - CPU utilization: milliseconds of time spent</li> <li>• disk_device_io - Storage device I/O statistics</li> <li>• disk_io - Operating system aggregate disk I/O: KB/sec</li> <li>• eth</li> <li>• eth-abs</li> <li>• eth_ip</li> <li>• fan - Fan speed</li> <li>• fs_mnt_bytes - Filesystem usage: bytes</li> <li>• fs_mnt_inodes - Filesystem usage: inodes</li> <li>• ib</li> <li>• interface - Network interface statistics</li> <li>• intf_util - Network interface utilization: bytes</li> <li>• memory - System memory utilization: bytes</li> <li>• paging - Paging activity: page faults</li> <li>• power - Power supply usage</li> <li>• power-consumption</li> <li>• temperature - Modules temperature</li> </ul>
<b>Default</b>	N/A	
<b>Configuration Mode</b>	Config	
<b>History</b>	3.1.0000	
<b>Role</b>	admin	
<b>Example</b>	switch (config) # stats sample temperature clear switch (config) #	
<b>Related Commands</b>	show stats sample	
<b>Notes</b>		

## **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.

<b>Syntax Description</b>	sample ID	Possible sample IDs are: <ul style="list-style-type: none"> <li>• congested</li> <li>• cpu_util - CPU utilization: milliseconds of time spent</li> <li>• disk_device_io - Storage device I/O statistics</li> <li>• disk_io - Operating system aggregate disk I/O: KB/sec</li> <li>• eth</li> <li>• fan - Fan speed</li> <li>• fs_mnt_bytes - Filesystem usage: bytes</li> <li>• fs_mnt_inodes - Filesystem usage: inodes</li> <li>• ib</li> <li>• interface - Network interface statistics</li> <li>• intf_util - Network interface utilization: bytes</li> <li>• memory - System memory utilization: bytes</li> <li>• paging - Paging activity: page faults</li> <li>• power - Power supply usage</li> <li>• power-consumption</li> <li>• temperature - Modules temperature</li> </ul>
	number of seconds	Interval in seconds.
<b>Default</b>	Different per sample	
<b>Configuration Mode</b>	Config	
<b>History</b>	3.1.0000	
<b>Role</b>	admin	
<b>Example</b>	<pre>switch (config) # stats sample temperature interval 1 switch (config) # show stats sample temperature Sample "temperature" (Modules temperature):     Enabled:          yes     Sampling interval: 1 second switch (config) #</pre>	
<b>Related Commands</b>	show stats sample	
<b>Notes</b>		

## stats clear-all

**stats clear all**

Clears data for all samples, CHDs, and status for all alarms.

<b>Syntax Description</b>	N/A
<b>Default</b>	N/A
<b>Configuration Mode</b>	Config
<b>History</b>	3.1.0000
<b>Role</b>	admin
<b>Example</b>	<pre>switch (config) # stats clear-all switch (config) #</pre>
<b>Related Commands</b>	N/A
<b>Notes</b>	

## stats export

```
stats export <format> <report name> [{after | before} <yyyy/mm/dd>
<hh:mm:ss>] [filename <filename>]
```

Exports statistics to a file.

<b>Syntax Description</b>	format	Currently the only supported value for <format> is “csv” (comma-separated value).
	report name	Determines dataset to be exported. Possible report names are: <ul style="list-style-type: none"> <li>• memory - Memory utilization</li> <li>• paging - Paging I/O</li> <li>• cpu_util - CPU utilization</li> </ul>
	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.
<b>Default</b>	N/A	
<b>Configuration Mode</b>	Config	
<b>History</b>	3.1.0000	
<b>Role</b>	admin	
<b>Example</b>	<pre>switch (config) # stats export csv memory filename mellanoxexample before 2000/08/14 15:59:50 after 2000/08/14 15:01:50 Generated report file: mellanoxexample.csv switch (config) # show files stats mellanoxexample.csv switch (config) #</pre>	
<b>Related Commands</b>	show files stats	
<b>Notes</b>		

## show stats alarm

**show stats alarm [<Alarm ID> [rate-limit]]**

Displays status of all alarms or the specified alarm.

<b>Syntax Description</b>	Alarm ID	May be: <ul style="list-style-type: none"> <li>• cpu_util_indiv - Average CPU utilization too high: percent utilization</li> <li>• disk_io - Operating System Disk I/O per second too high: kilobytes per second</li> <li>• fs_mnt - Free filesystem space too low: percent of disk space free</li> <li>• intf_util - Network utilization too high: bytes per second</li> <li>• memory_pct_used - Too much memory in use: percent of physical memory used</li> <li>• paging - Paging activity too high: page faults</li> <li>• temperature - Temperature is too high: degrees</li> </ul>
	rate-limit	Displays rate limit parameters.
<b>Default</b>	N/A	
<b>Configuration Mode</b>	Config	
<b>History</b>	3.1.0000	
<b>Role</b>	admin	
<b>Example</b>	<pre>switch (config) # show stats alarm Alarm cpu_util_indiv (Average CPU utilization too high): ok Alarm disk_io (Operating System Disk I/O per second too high): (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) #</pre>	
<b>Related Commands</b>	stats alarm	
<b>Notes</b>		

## show stats chd

**show stats chd [<CHD ID>]**

Displays configuration of all statistics CHDs.

<b>Syntax Description</b>	CHD ID	May be: <ul style="list-style-type: none"> <li>• cpu_util_indiv - Average CPU utilization too high: percent utilization</li> <li>• disk_io - Operating System Disk I/O per second too high: kilobytes per second</li> <li>• fs_mnt - Free filesystem space too low: percent of disk space free</li> <li>• intf_util - Network utilization too high: bytes per second</li> <li>• memory_pct_used - Too much memory in use: percent of physical memory used</li> <li>• paging - Paging activity too high: page faults</li> <li>• temperature - Temperature is too high: degrees</li> </ul>
<b>Default</b>	N/A	
<b>Configuration Mode</b>	Config	
<b>History</b>	3.1.0000	
<b>Role</b>	admin	
<b>Example</b>	<pre>switch (config) # show stats chd disk_device_io_hour  CHD "disk_device_io_hour" (Storage device I/O read/write statistics for the last hour: bytes):     Enabled:      yes     Source dataset: sample "disk_device_io"     Computation basis: data points     Interval:       1 data point(s)     Range:          1 data point(s)  switch (config) #</pre>	
<b>Related Commands</b>	<a href="#">stats chd</a>	
<b>Notes</b>		

## 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

<b>Syntax Description</b>	N/A
<b>Default</b>	N/A
<b>Configuration Mode</b>	Config
<b>History</b>	3.1.0000
<b>Role</b>	admin
<b>Example</b>	<pre>switch (config) # show stats cpu  CPU 0     Utilization:          6%     Peak Utilization Last Hour: 16% at 2012/02/28 08:47:32     Avg. Utilization Last Hour: 8% switch (config) #</pre>
<b>Related Commands</b>	N/A
<b>Notes</b>	

## show stats sample

**show stats sample [<sample ID>]**

Displays sampling interval for all samples, or the specified one.

<b>Syntax Description</b>	sample ID	Possible sample IDs are: <ul style="list-style-type: none"> <li>• congested</li> <li>• cpu_util - CPU utilization: milliseconds of time spent</li> <li>• disk_device_io - Storage device I/O statistics</li> <li>• disk_io - Operating system aggregate disk I/O: KB/sec</li> <li>• eth</li> <li>• fan - Fan speed</li> <li>• fs_mnt_bytes - Filesystem usage: bytes</li> <li>• fs_mnt_inodes - Filesystem usage: inodes</li> <li>• ib</li> <li>• interface - Network interface statistics</li> <li>• intf_util - Network interface utilization: bytes</li> <li>• memory - System memory utilization: bytes</li> <li>• paging - Paging activity: page faults</li> <li>• power - Power supply usage</li> <li>• power-consumption</li> <li>• temperature - Modules temperature</li> </ul>
<b>Default</b>	N/A	
<b>Configuration Mode</b>	Config	
<b>History</b>	3.1.0000	
<b>Role</b>	admin	
<b>Example</b>	<pre>switch (config) # show stats sample fan Sample "fan" (Fan speed):     Enabled:          yes     Sampling interval: 1 minute 11 seconds switch (config) #</pre>	
<b>Related Commands</b>	N/A	
<b>Notes</b>		

## 4.16 Chassis Management

The chassis manager provides the user access to the following information:

**Table 29 - 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 30 - System Health Monitor Alerts Scenarios (Sheet 1 of 6)**

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 30 - System Health Monitor Alerts Scenarios (Sheet 2 of 6)**

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 SwitchX 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	“SwitchX temperature is back to normal”
BBU Health Monitoring				
“BBU <num> active alarms: Under-temperature during discharge (UTD)”	Under-temperature during discharge	Email, system status LED set red, log alert, SNMP	Check ambient temperature. Replace BBU if the problem persist.	“Module BBU <num> has been restored to its normal state”
“BBU <num> active alarms: Under-temperature during charge (UTC)”	Under-temperature during charge	Email, system status LED set red, log alert, SNMP	Check ambient temperature. Replace BBU if the problem persist.	“Module BBU <num> has been restored to its normal state”

**Table 30 - System Health Monitor Alerts Scenarios (Sheet 3 of 6)**

Alert Message	Scenario	Notification Indicator	Recovery Action	Recovery Message
“BBU <num> active alarms: Over pre-charge current (PCHGC)”	Over pre-charge current	Email, system status LED set red, log alert, SNMP	Replace BBU if the problem persists.	“Module BBU <num> has been restored to its normal state”
“BBU <num> active alarms: Overcharging voltage (CHGV)”	Overcharging voltage	Email, system status LED set red, log alert, SNMP	Replace BBU if the problem persists.	“Module BBU <num> has been restored to its normal state”
“BBU <num> active alarms: Overcharging current (CHGC)”	Overcharging current	Email, system status LED set red, log alert, SNMP	Replace BBU if the problem persists.	“Module BBU <num> has been restored to its normal state”
“BBU <num> active alarms: Overcharge (OC)”	Overcharged BBU	Email, system status LED set red, log alert, SNMP	Replace BBU if the problem persists.	“Module BBU <num> has been restored to its normal state”
“BBU <num> active alarms: Charge timeout suspend (CTOS)”	Charge timeout suspend	Email, system status LED set red, log alert, SNMP	N/A	“Module BBU <num> has been restored to its normal state”
“BBU <num> active alarms: Charge timeout (CTO)”	Charge timeout	Email, system status LED set red, log alert, SNMP	N/A	“Module BBU <num> has been restored to its normal state”
“BBU <num> active alarms: Pre-charge time-out suspend (PTOS)”	Pre-charge timeout suspend	Email, system status LED set red, log alert, SNMP	N/A	“Module BBU <num> has been restored to its normal state”
“BBU <num> active alarms: Pre-charge time-out (PTO)”	Pre-charge timeout	Email, system status LED set red, log alert, SNMP	N/A	“Module BBU <num> has been restored to its normal state”
“BBU <num> active alarms: Over-temperature FET (OTF)”	Over-temperature FET	Email, system status LED set red, log alert, SNMP	N/A	“Module BBU <num> has been restored to its normal state”

**Table 30 - System Health Monitor Alerts Scenarios (Sheet 4 of 6)**

Alert Message	Scenario	Notification Indicator	Recovery Action	Recovery Message
“BBU <num> active alarms: Cell under-voltage compensated (CUVC)”	Cell under-voltage compensated	Email, system status LED set red, log alert, SNMP	Replace BBU if the problem persists.	“Module BBU <num> has been restored to its normal state”
“BBU <num> active alarms: Over-temperature during discharge (OTD)”	Over-temperature during discharge	Email, system status LED set red, log alert, SNMP	Replace BBU if the problem persists.	“Module BBU <num> has been restored to its normal state”
“BBU <num> active alarms: Over-temperature during charge (OTC)”	Over-temperature during charge	Email, system status LED set red, log alert, SNMP	Check ambient temperature. Replace BBU if the problem persists.	“Module BBU <num> has been restored to its normal state”
“BBU <num> active alarms: Short-circuit during discharge latch (ASCDL)”	Short-circuit during discharge latch	Email, system status LED set red, log alert, SNMP	Replace BBU	N/A
“BBU <num> active alarms: Short-circuit during discharge (ASCL)”	Short-circuit during discharge	Email, system status LED set red, log alert, SNMP	Replace BBU if the problem persists.	“Module BBU <num> has been restored to its normal state”
“BBU <num> active alarms: Short-circuit during charge latch (ASCCL)”	Short-circuit during charge latch	Email, system status LED set red, log alert, SNMP	Replace BBU	N/A
“BBU <num> active alarms: Short-circuit during charge (ASCC)”	Short-circuit during charge	Email, system status LED set red, log alert, SNMP	Replace BBU if the problem persists.	“Module BBU <num> has been restored to its normal state”
“BBU <num> active alarms: Overload during discharge latch (AOLDL)”	Overload during discharge latch	Email, system status LED set red, log alert, SNMP	Replace BBU	N/A
“BBU <num> active alarms: Overload during discharge (AOLD)”	Overload during discharge	Email, system status LED set red, log alert, SNMP	Replace BBU if the problem persists.	“Module BBU <num> has been restored to its normal state”

**Table 30 - System Health Monitor Alerts Scenarios (Sheet 5 of 6)**

Alert Message	Scenario	Notification Indicator	Recovery Action	Recovery Message
“BBU <num> active alarms: Over-current during discharge 1 (OCD1)”	Over-current during discharge	Email, system status LED set red, log alert, SNMP	Replace BBU if the problem persists.	“Module BBU <num> has been restored to its normal state”
“BBU <num> active alarms: Over-current during discharge 2 (OCD2)”	Over-current during discharge	Email, system status LED set red, log alert, SNMP	Replace BBU if the problem persists.	“Module BBU <num> has been restored to its normal state”
“BBU <num> active alarms: Over-current during charge 1 (OCC1)”	Over-current during charge	Email, system status LED set red, log alert, SNMP	Replace BBU if the problem persists.	“Module BBU <num> has been restored to its normal state”
“BBU <num> active alarms: Over-current during charge 2 (OCC2)”	Over-current during charge	Email, system status LED set red, log alert, SNMP	Replace BBU if the problem persists.	“Module BBU <num> has been restored to its normal state”
“BBU <num> active alarms: Cell over-voltage (COV)”	Cell over-voltage	Email, system status LED set red, log alert, SNMP	Replace BBU if the problem persists (may take up to 48 hours if BBU was in storage).	“Module BBU <num> has been restored to its normal state”
“BBU <num> active alarms: Cell under-voltage (CUV)”	Cell under-voltage	Email, system status LED set red, log alert, SNMP	Replace BBU if the problem persists.	“Module BBU <num> has been restored to its normal state”
“Module BBU <num> voltage is out of range”	Cell over-voltage	Email, system status LED set red, log alert, SNMP	Replace BBU if the problem persists (may take up to 48 hours if BBU was in storage).	“Module BBU <num> voltage is back in range”
“Module BBU <num> current is too high”	Over-current during charge	Email, system status LED set red, log alert, SNMP	Replace BBU if the problem persists.	“BBU <num> has been restored to its normal state”
“Module BBU <num> current is too high”	Over-current during discharge	Email, system status LED set red, log alert, SNMP	Replace BBU if the problem persists.	“BBU <num> has been restored to its normal state”

**Table 30 - System Health Monitor Alerts Scenarios (Sheet 6 of 6)**

Alert Message	Scenario	Notification Indicator	Recovery Action	Recovery Message
“Module BBU <num> temperature is too hot”	Over-temperature during charge	Email, system status LED set red, log alert, SNMP	Check ambient temperature. Replace BBU if the problem persist.	“Module BBU <num> temperature is back to normal”
“Module BBU <num> temperature is too hot”	Over-temperature during discharge	Email, system status LED set red, log alert, SNMP	Check ambient temperature. Replace BBU if the problem persist.	“Module BBU <num> temperature is back to normal”

## 4.16.2 Power Management

### 4.16.2.1 Width Reduction Power Saving

Link width reduction (LWR) is a Mellanox proprietary power saving feature to be utilized to economize the power usage of the fabric. LWR may be used to manually or automatically configure a certain connection between Mellanox switch systems to lower the width of a link from 4X operation to 1X based on the traffic flow.

LWR is relevant only for 40GbE 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 484.

**Table 31 - LWR Configuration Behavior**

Switch-A Configuration	Switch-B Configuration	Behavior
Disable	Disable	LWR is disabled.

**Table 31 - LWR Configuration Behavior**

Switch-A Configuration	Switch-B Configuration	Behavior
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

#### 4.16.3 Monitoring Environmental Conditions

Step 1. Display module's temperature. Run:

```
switch (config) # show temperature
=====
Module    Sensor          CurTemp   Status
                    (Celsius)
=====
MGMT     CPU_BOARD_MONITOR  40.00    OK
L01      BOARD_MONITOR     27.00    OK
L01      QSFP_TEMP1        24.00    OK
L01      QSFP_TEMP2        22.00    OK
L01      QSFP_TEMP3        21.00    OK
L01      SX                 38.00    OK
L02      BOARD_MONITOR      27.00    OK
L02      QSFP_TEMP1         24.50    OK
L02      QSFP_TEMP2         22.50    OK
L02      QSFP_TEMP3         21.50    OK
L02      SX                 32.00    OK
PS2      PS_MONITOR         24.66    OK
PS3      PS_MONITOR         31.04    OK
PS4      PS_MONITOR         28.06    OK
S01      BOARD_MONITOR      23.00    OK
S01      SX                 34.00    OK
S01      SX_AMBIENT_TEMP   22.50    OK
S02      BOARD_MONITOR      24.00    OK
S02      SX                 49.00    OK
S02      SX_AMBIENT_TEMP   24.00    OK
switch (config) #
```

**Step 2.** Display measured voltage levels of power supplies. Run:

```
switch (config) # show voltage
=====
Module  Power Meter      Reg  Expected  Actual   Status
          Voltage      Voltage
=====
PS2     PS_MONITOR      V1   48.00    46.88   OK
PS3     PS_MONITOR      V1   48.00    48.29   OK
PS4     PS_MONITOR      V1   48.00    48.29   OK
MGMT   CPU_BOARD_MONITOR V1   12.00    11.92   OK
MGMT   CPU_BOARD_MONITOR V2   2.50     2.48    OK
MGMT   CPU_BOARD_MONITOR V3   3.30     3.31    OK
MGMT   CPU_BOARD_MONITOR V4   3.30     3.30    OK
MGMT   CPU_BOARD_MONITOR V5   1.80     1.81    OK
MGMT   CPU_BOARD_MONITOR V6   1.20     1.26    OK
S01    BOARD_MONITOR    V1   3.30     3.33    OK
S01    BOARD_MONITOR    V2   2.27     2.15    OK
S01    BOARD_MONITOR    V3   1.80     1.76    OK
S01    BOARD_MONITOR    V4   3.30     3.30    OK
S01    BOARD_MONITOR    V5   0.90     0.93    OK
S01    BOARD_MONITOR    V6   1.20     1.19    OK
S02    BOARD_MONITOR    V1   3.30     3.26    OK
S02    BOARD_MONITOR    V2   2.27     2.16    OK
S02    BOARD_MONITOR    V3   1.80     1.79    OK
S02    BOARD_MONITOR    V4   3.30     3.31    OK
S02    BOARD_MONITOR    V5   0.90     0.95    OK
S02    BOARD_MONITOR    V6   1.20     1.20    OK
L01    BOARD_MONITOR    V1   3.30     3.33    OK
L01    BOARD_MONITOR    V2   2.27     2.16    OK
L01    BOARD_MONITOR    V3   1.80     1.76    OK
L01    BOARD_MONITOR    V4   3.30     3.30    OK
L01    BOARD_MONITOR    V5   0.90     0.93    OK
L01    BOARD_MONITOR    V6   1.20     1.19    OK
L02    BOARD_MONITOR    V1   3.30     3.26    OK
L02    BOARD_MONITOR    V2   2.27     2.17    OK
L02    BOARD_MONITOR    V3   1.80     1.79    OK
L02    BOARD_MONITOR    V4   3.30     3.30    OK
L02    BOARD_MONITOR    V5   0.90     0.89    OK
L02    BOARD_MONITOR    V6   1.20     1.19    OK
switch (config) #
```

**Step 3.** Display the fan speed and status. Run:

```
switch (config) # show fan
=====
Module      Device      Fan  Speed      Status
          (RPM)
=====
FAN1        FAN        F1   6994.00   OK
FAN2        FAN        F1   6792.00   OK
FAN3        FAN        F1   6870.00   OK
FAN4        FAN        F1   6818.00   OK
S01         FAN        F1   7800.00   OK
S01         FAN        F2   8130.00   OK
S02         FAN        F1   8130.00   OK
S02         FAN        F2   8490.00   OK
S03         FAN        -    -          NOT PRESENT
S04         FAN        -    -          NOT PRESENT
S05         FAN        -    -          NOT PRESENT
S06         FAN        -    -          NOT PRESENT
switch (config) #
```

**Step 4.** Display the voltage current and status of each module in the system. Run:

```
switch (config) # show power consumers
=====
Module      Power      Voltage     Current     Status
          (Watts)    (Amp)
=====
FAN1        15.55     48.00      0.32       OK
FAN2        16.26     48.00      0.34       OK
FAN3        15.30     48.00      0.32       OK
FAN4        14.98     48.00      0.31       OK
L01         32.45     48.00      0.68       OK
L02         28.75     48.00      0.60       OK
MGMT        16.08     48.00      0.34       OK
S01         37.34     48.00      0.78       OK
S02         35.09     48.00      0.73       OK

Total power used : 211.79 W
Max power : 686.00 W
switch (config) #
```

#### 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/usbl/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/usbl/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    UID          Blue
```

- **To deactivate the UID LED on a switch system, run:**

```
switch (config) # led MGMT uid off
```

## 4.16.6 System Reboot

### 4.16.6.1 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 Commands

### 4.16.7.1 Chassis Management

#### clear counters

**clear counters [all | interface <type> <number>] [ethernet|port-channel]**

Clears switch counters.

<b>Syntax Description</b>	all	Clears all switch counters.
	type	A specific interface type
	number	The interface number.
<b>Default</b>	N/A	
<b>Configuration Mode</b>	Config Interface Port Channel	
<b>History</b>	3.2.3000	
	3.6.4000	Added note
<b>Role</b>	admin	
<b>Example</b>	switch (config) # clear counters	
<b>Related Commands</b>		
<b>Notes</b>	The command also clears storm-control counters.	

## health

**health {max-report-len <length> | re-notif-cntr <counter> | report-clear}**

Configures health daemon settings.

<b>Syntax Description</b>	max-report-len <length> re-notif-cntr <counter> report-clear	Sets the length of the health report - number of line entries. Range: 10-2048. Health control changes notification counter, in seconds. Range: 120-7200 seconds. Clears the health report.
<b>Default</b>	max-report-len: 50 re-notif-cntr:	
<b>Configuration Mode</b>	Config	
<b>History</b>	3.1.0000	
<b>Role</b>	admin	
<b>Example</b>	switch (config) # health re-notif-cntr 125 switch (config) #	
<b>Related Commands</b>	show health-report	
<b>Notes</b>		

## led uid

**led <module> uid <on | off>**

Configures the UID LED.

<b>Syntax Description</b>	module on off	Specifies the module whose UID LED to configure Turns on UID LED Turns off UID LED
<b>Default</b>	N/A	
<b>Configuration Mode</b>	Config	
<b>History</b>	3.6.1002	
<b>Role</b>	admin	
<b>Example</b>		switch (config) # led MGMT uid on switch (config) #
<b>Related Commands</b>	N/A	
<b>Notes</b>		•

## 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.

<b>Syntax Description</b>	auto	Allows the system to automatically decide whether to work in power-saving mode or not.
	force	Forces power-saving mode on the port.
<b>Default</b>	Disabled	
<b>Configuration Mode</b>	Config Interface Ethernet	
<b>History</b>	3.3.4000	
<b>Role</b>	admin	
<b>Example</b>	switch (config interface ethernet 1/1) # power-management width auto	
<b>Related Commands</b>	show interface	
<b>Notes</b>		

## usb eject

### usb eject

Gracefully turns off the USB interface.

<b>Syntax Description</b>	N/A
<b>Default</b>	N/A
<b>Configuration Mode</b>	Config
<b>History</b>	3.1.0000
<b>Role</b>	admin
<b>Example</b>	<pre>switch (config) # usb eject switch (config) #</pre>
<b>Related Commands</b>	N/A
<b>Notes</b>	Applicable only for systems with USB interface.

## show asic-version

### show asic-version

Displays firmware ASIC version.

<b>Syntax Description</b>	N/A
<b>Default</b>	N/A
<b>Configuration Mode</b>	Any Command Mode
<b>History</b>	3.1.0000 3.4.2008                          Updated Example
<b>Role</b>	admin
<b>Example</b>	<pre>switch (config) # show asic-version ===== Module      Device      Version ===== MGMT        SX          9.2.9160</pre>
<b>Related Commands</b>	N/A
<b>Notes</b>	

## show bios

### show bios

Displays the BIOS version information.

<b>Syntax Description</b>	N/A
<b>Default</b>	N/A
<b>Configuration Mode</b>	Any Command Mode
<b>History</b>	3.3.4150
<b>Role</b>	admin
<b>Example</b>	<pre>switch (config) # show bios BIOS version : 4.6.5 BIOS subversion : Official AMI Release BIOS release date : 07/02/2013 switch (config) #</pre>
<b>Related Commands</b>	
<b>Notes</b>	The command is available only on x86 systems

## show cpld

### show cpld

Displays status of all CPLDs in the system.

<b>Syntax Description</b>	N/A	
<b>Default</b>	N/A	
<b>Configuration Mode</b>	Any Command Mode	
<b>History</b>	3.1.0000 3.3.4302                          Updated example	
<b>Role</b>	admin	
<b>Example</b>	<pre>switch (config) # show cpld ===== Name          Type           Version ===== Cpld1        CPLD_TOR       4 Cpld2        CPLD_PORT1     2 Cpld3        CPLD_PORT2     2 Cpld4        CPLD_MEZZ      3 switch (config) #</pre>	
<b>Related Commands</b>	N/A	
<b>Notes</b>		

## show fan

### show fan

Displays fans status.

<b>Syntax Description</b>	N/A
<b>Default</b>	N/A
<b>Configuration Mode</b>	Any Command Mode
<b>History</b>	3.1.0000
<b>Role</b>	admin
<b>Example</b>	<pre>switch (config) # show fan switch (config) # show fan ===== Module          Device          Fan   Speed      Status                   (RPM) ===== FAN            FAN           F1    5340.00   OK FAN            FAN           F2    5340.00   OK FAN            FAN           F3    5640.00   OK FAN            FAN           F4    5640.00   OK PS1            FAN           F1    5730.00   OK PS2            FAN           -     -         NOT PRESENT switch (config) #</pre>
<b>Related Commands</b>	N/A
<b>Notes</b>	

## show health-report

### show health-report

Displays health report.

<b>Syntax Description</b>	N/A	
<b>Default</b>	N/A	
<b>Configuration Mode</b>	Any Command Mode	
<b>History</b>	3.1.0000	
	3.3.0000	Output update
<b>Role</b>	admin	
<b>Example</b>	<pre>switch (config) # show health-report =====   ALERTS CONFIGURATION   ===== Re-notification counter (sec):[3600] Report max counter: [50] =====   HEALTH REPORT   ===== No Health issues file switch (config) #</pre>	
<b>Related Commands</b>	N/A	
<b>Notes</b>	Problems with the power supply cannot be monitored on SX1016 switch systems.	

## show inventory

### show inventory

Displays system inventory.

<b>Syntax Description</b>	N/A																													
<b>Default</b>	N/A																													
<b>Configuration Mode</b>	Any Command Mode																													
<b>History</b>	3.1.0000																													
	3.4.1604	Removed CPU module output from Example																												
	3.5.1000	Removed Type column from Example																												
	3.6.1002	Updated output																												
<b>Role</b>	admin																													
<b>Example</b>	<pre>switch (config) # show inventory</pre> <hr/> <table><thead><tr><th>Module</th><th>Part number</th><th>Serial Number</th><th>Asic Rev.</th><th>HW Rev.</th></tr></thead><tbody><tr><td>CHASSIS</td><td>MSX1036B-1SFR</td><td>MT1205X01549</td><td>N/A</td><td>A1</td></tr><tr><td>MGMT</td><td>MSX1036B-1SFR</td><td>MT1205X01549</td><td>0</td><td>A1</td></tr><tr><td>FAN</td><td>MSX60-FF</td><td>MT1206X07209</td><td>N/A</td><td>A3</td></tr><tr><td>PS1</td><td>MSX60-PF</td><td>MT1206X06697</td><td>N/A</td><td>A2</td></tr></tbody></table> <pre>switch (config) #</pre>					Module	Part number	Serial Number	Asic Rev.	HW Rev.	CHASSIS	MSX1036B-1SFR	MT1205X01549	N/A	A1	MGMT	MSX1036B-1SFR	MT1205X01549	0	A1	FAN	MSX60-FF	MT1206X07209	N/A	A3	PS1	MSX60-PF	MT1206X06697	N/A	A2
Module	Part number	Serial Number	Asic Rev.	HW Rev.																										
CHASSIS	MSX1036B-1SFR	MT1205X01549	N/A	A1																										
MGMT	MSX1036B-1SFR	MT1205X01549	0	A1																										
FAN	MSX60-FF	MT1206X07209	N/A	A3																										
PS1	MSX60-PF	MT1206X06697	N/A	A2																										
<b>Related Commands</b>	N/A																													
<b>Notes</b>																														

## show leds

**show leds [<module>]**

Displays the LED status of the switch system.

<b>Syntax Description</b>	module	Specifies the module whose LED status to display																														
<b>Default</b>	N/A																															
<b>Configuration Mode</b>	Config																															
<b>History</b>	3.6.1002																															
	3.6.2002	Updated output																														
<b>Role</b>	admin																															
<b>Example</b>	<pre>switch (config) # show leds Module      LED                  Status -----</pre> <table><thead><tr><th>Module</th><th>LED</th><th>Status</th></tr></thead><tbody><tr><td>MGMT</td><td>STATUS</td><td>Green</td></tr><tr><td>MGMT</td><td>FAN1</td><td>Green</td></tr><tr><td>MGMT</td><td>FAN2</td><td>Green</td></tr><tr><td>MGMT</td><td>FAN3</td><td>Green</td></tr><tr><td>MGMT</td><td>FAN4</td><td>Green</td></tr><tr><td>MGMT</td><td>PS_STATUS</td><td>Green</td></tr><tr><td>MGMT</td><td>PS1</td><td>Green</td></tr><tr><td>MGMT</td><td>PS2</td><td>Green</td></tr><tr><td>MGMT</td><td>UID</td><td>Blue</td></tr></tbody></table>		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
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																														
<b>Related Commands</b>	N/A																															
<b>Notes</b>																																

## show memory

**show memory**

Displays memory status.

<b>Syntax Description</b>	N/A
<b>Default</b>	N/A
<b>Configuration Mode</b>	Any Command Mode
<b>History</b>	3.1.0000
<b>Role</b>	admin
<b>Example</b>	<pre>switch (config) # show memory Total          Used         Free        Used+B/C   Free-B/C Physical      2027 MB      761 MB     1266 MB    1214 MB     813 MB Swap           0 MB        0 MB       0 MB       0 MB  Physical Memory Borrowed for System Buffers and Cache:   Buffers:                      0 MB   Cache:                        452 MB   Total Buffers/Cache:          452 MB switch (config) #</pre>
<b>Related Commands</b>	N/A
<b>Notes</b>	

## show module

### show module

Displays modules status.

<b>Syntax Description</b>	N/A								
<b>Default</b>	N/A								
<b>Configuration Mode</b>	Any Command Mode								
<b>History</b>	<table><tr><td>3.1.0000</td><td></td></tr><tr><td>3.3.0000</td><td>Added “Is Fatal” column</td></tr><tr><td>3.4.2008</td><td>Updated command output</td></tr><tr><td>3.4.3000</td><td>Updated command output and added note</td></tr></table>	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
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								
<b>Role</b>	admin								
<b>Example</b>	<pre>switch (config) # show module ===== Module      Status ===== MGMT      ready FAN1      ready FAN2      ready PS1       ready PS2       not-present switch (config) #</pre>								
<b>Related Commands</b>	N/A								
<b>Notes</b>	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.

<b>Syntax Description</b>	N/A
<b>Default</b>	N/A
<b>Configuration Mode</b>	Any Command Mode
<b>History</b>	3.1.0000 3.5.1000 Updated Example
<b>Role</b>	admin
<b>Example</b>	<pre>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) #</pre>
<b>Related Commands</b>	N/A
<b>Notes</b>	

## show power consumers

### show power consumers

Displays power consumption information.

<b>Syntax Description</b>	N/A
<b>Default</b>	N/A
<b>Configuration Mode</b>	Any Command Mode
<b>History</b>	3.1.0000 3.5.1000                          Updated Example
<b>Role</b>	admin
<b>Example</b>	<pre>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) #</pre>
<b>Related Commands</b>	N/A
<b>Notes</b>	

## show protocols

### show protocols

Displays all protocols enabled in the system.

<b>Syntax Description</b>	N/A	
<b>Default</b>	N/A	
<b>Configuration Mode</b>	Any Command Mode	
<b>History</b>	3.2.3000 3.3.4550                      Updated Example 3.6.1002                      Updated Example	
<b>Role</b>	admin	
<b>Example</b>	<pre>switch (config) # show protocols  Ethernet           enabled spanning-tree      rst lacp               disabled lldp               disabled igmp-snooping     disabled ets                enabled priority-flow-control disabled sflow              disabled openflow           disabled mlag               disabled dot1x              disabled isolation-group   disabled  IP routing         disabled bgp                disabled pim                disabled vrrp               disabled ospf               disabled magp               disabled dhcp-relay         disabled  Infiniband         enabled sm                disabled router             disabled</pre>	
<b>Related Commands</b>	N/A	
<b>Notes</b>		

## show resources

### show resources

Displays system resources.

<b>Syntax Description</b>	N/A
<b>Default</b>	N/A
<b>Configuration Mode</b>	Any Command Mode
<b>History</b>	3.1.0000
<b>Role</b>	admin
<b>Example</b>	<pre>switch (config) # show resources Total          Used          Free Physical    2027 MB      761 MB    1266 MB Swap           0 MB         0 MB       0 MB  Number of CPUs:      1 CPU load averages: 0.11 / 0.23 / 0.23  CPU 1 Utilization:          5% Peak Utilization Last Hour: 19% at 2012/02/15 13:26:19 Avg. Utilization Last Hour: 7% switch (config) #</pre>
<b>Related Commands</b>	N/A
<b>Notes</b>	

## show system capabilities

### show system capabilities

Displays system capabilities.

<b>Syntax Description</b>	N/A	
<b>Default</b>	N/A	
<b>Configuration Mode</b>	Any Command Mode	
<b>History</b>	3.1.0000 3.3.0000                          Added gateway support 3.6.1002                          Updated output	
<b>Role</b>	admin	
<b>Example</b>	<pre>switch (config) # show system capabilities Ethernet: Supported, L2, L3 Ethernet Max licensed speed: 56Gb</pre>	
<b>Related Commands</b>	show system profile	
<b>Notes</b>		

## show system mac

### show system mac

Displays system MAC address.

<b>Syntax Description</b>	N/A
<b>Default</b>	N/A
<b>Configuration Mode</b>	Any Command Mode
<b>History</b>	3.1.0000
<b>Role</b>	admin
<b>Example</b>	<pre>switch (config) # show system mac 00:02:C9:5E:AF:18 switch (config) #</pre>
<b>Related Commands</b>	N/A
<b>Notes</b>	

## show system profile

### show system profile

Displays system profile.

<b>Syntax Description</b>	N/A
<b>Default</b>	N/A
<b>Configuration Mode</b>	Any Command Mode
<b>History</b>	3.2.0000
<b>Role</b>	admin
<b>Example</b>	<pre>switch (config) # show system profile eth-single-switch switch (config) #</pre>
<b>Related Commands</b>	system profile
<b>Notes</b>	

## 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
SX1036
switch (config) #
```

---

**Related Commands**

---

**Notes**

## show temperature

### show temperature

Displays system temperature sensors status.

<b>Syntax Description</b>	N/A
<b>Default</b>	N/A
<b>Configuration Mode</b>	Any Command Mode
<b>History</b>	3.1.0000
<b>Role</b>	admin
<b>Example</b>	<pre>switch (config) # show temperature ===== Module      Component          Reg  CurTemp   Status               (Celsius) ===== MGMT       BOARD_MONITOR      T1   25.00    OK MGMT       CPU_BOARD_MONITOR  T1   26.00    OK MGMT       CPU_BOARD_MONITOR  T2   41.00    OK MGMT       QSFP_TEMP1        T1   23.00    OK MGMT       QSFP_TEMP2        T1   22.50    OK MGMT       QSFP_TEMP3        T1   23.00    OK MGMT       SX                 T1   37.00    OK switch (config) #</pre>
<b>Related Commands</b>	N/A
<b>Notes</b>	

## show uboot

### show uboot

Displays u-boot version.

<b>Syntax Description</b>	N/A
<b>Default</b>	N/A
<b>Configuration Mode</b>	Any Command Mode
<b>History</b>	3.3.5006 3.4.1110 Updated Example
<b>Role</b>	admin
<b>Example</b>	<pre>switch (config) # show uboot UBOOT version : U-Boot 2009.01 SX_PPC_M460EX 3.2.0330-82 ppc (Dec 20 2012 - 17:53:54) switch (config) #</pre>
<b>Related Commands</b>	N/A
<b>Notes</b>	This command is available only on PPC based systems

## show version

### show version

Displays version information for the currently running system image.

<b>Syntax Description</b>	N/A
<b>Default</b>	N/A
<b>Configuration Mode</b>	Any Command Mode
<b>History</b>	3.1.0000
<b>Role</b>	admin
<b>Example</b>	<pre>switch (config) # show version Product name:      MLNX-OS Product release:   3.1.0000 Build ID:          #1-dev Build date:        2012-02-26 08:47:51 Target arch:       ppc Target hw:         m460ex Built by:          root@r-fit16  Uptime:            1d 3h 32m 24.656s  Product model:    ppc Host ID:          0002c911a15e System memory:    110 MB used / 1917 MB free / 2027 MB total Swap:              0 MB used / 0 MB free / 0 MB total Number of CPUs:   1 CPU load averages: 0.18 / 0.19 / 0.16 switch (config) #</pre>
<b>Related Commands</b>	N/A
<b>Notes</b>	

## show version concise

### show version concise

Displays concise version information for the currently running system image.

<b>Syntax Description</b>	N/A
<b>Default</b>	N/A
<b>Configuration Mode</b>	Any Command Mode
<b>History</b>	3.1.0000
<b>Role</b>	admin
<b>Example</b>	<pre>switch (config) # show version concise PPC_M460EX 3.4.2000 2015-05-06 20:26:41 ppc switch (config) #</pre>
<b>Related Commands</b>	N/A
<b>Notes</b>	

## show voltage

### show voltage

Displays voltage level measurements on different sensors.

<b>Syntax Description</b>	N/A
<b>Default</b>	N/A
<b>Configuration Mode</b>	Any Command Mode
<b>History</b>	3.1.0000
	3.3.5006 Updated Example
<b>Role</b>	admin
<b>Example</b>	<pre>switch (config) # show voltage ===== Module    Power Meter          Reg           Expected   Actual   Status   High     Low                 Voltage        Voltage ===== 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) #</pre>
<b>Related Commands</b>	N/A
<b>Notes</b>	

## show chassis ha

### show chassis ha

Displays Chassis HA parameters and status.

<b>Syntax Description</b>	N/A
<b>Default</b>	N/A
<b>Configuration Mode</b>	Config
<b>History</b>	3.1.0000
<b>Role</b>	admin
<b>Example</b>	<pre>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) #</pre>
<b>Related Commands</b>	chassis ha
<b>Notes</b>	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 32 - 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		



Starting from version 3.4.1600, IB interfaces in interfaces tables (i.e. ifTable, ifxTable) have changed from SX<if>/<port> to IB/port.

**Table 33 - Standard MIBs – Chassis and Switch**

MIB	Standard	Comments
RFC1213-MIB	RFC 1213	
IF-MIB	RFC 2863	ifXTable only supported.
ENTITY-MIB	RFC 4133	
ENTITY-SENSOR-MIB	RFC 3433	Fan and temperature sensors
ENTITY-STATE-MIB	RFC 4268	Fan and temperature states

**Table 33 - Standard MIBs – Chassis and Switch**

MIB	Standard	Comments
Bridge MIB	RFC 4188	dot1dTpFdbGroup and dot1dStaticGroup are not supported in this MIB, it is supported as a part of Q-Bridge-MIB.
Q-Bridge MIB	RFC 4363	The following SNMP groups are not supported: <ul style="list-style-type: none"><li>• qBridgeVlanStatisticsGroup,</li><li>• qBridgeVlanStatisticsOverflowGroup ,</li><li>• qBridgeVlanHCStatisticsGroup,</li><li>• qBridgeLearningConstraintsGroup.</li></ul> The following SNMP tables are not supported: <ul style="list-style-type: none"><li>• dot1qTpGroupTable (dynamic MC MAC addresses)</li><li>• dot1qForwardAllTable (GMRP)</li><li>• dot1qForwardUnregisteredTable (GMRP)</li></ul> dot1qVlanCurrentTable (GVRP)
RSTP-MIB	RFC 4318	
LLDP-MIB	802.1AB-2005	
ENTITY-SENSOR-MIB	RFC 3433	<ul style="list-style-type: none"><li>• Port module transmit/receiver power sensors</li><li>• Fan, temperature sensors</li></ul>
BGP4-MIB	RFC 4273	Only supports the following tables: <ul style="list-style-type: none"><li>• bgpLocalAs</li><li>• bgpPeerLocalAddr</li><li>• bgpPeerState</li><li>• bgpIdentifier</li></ul>
OSPF-MIB	RFC 4750	

#### 4.17.1.2 Private MIB

**Table 34 - 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 Mellanox Private Traps

The following private traps are supported by MLNX-OS®.

**Table 35 - SNMP Traps**

Trap	Action Required
asicChipDown	Reboot the system.
asicOverTempReset	Check fans and environmental temperature.
asicOverTemp	Check fans and environmental temperature.
lowPower	Add/connect power supplies.
internalBusError	N/A
procCrash	Generate SysDump and contact Mellanox support.
cpuUtilHigh	N/A
procUnexpectedExit	Generate SysDump and contact Mellanox support.
diskSpaceLow	Clean images and sysDump files using the commands “image delete” and “file debug-dump delete”.
systemHealthStatus	Refer to Health Status table.

**Table 35 - SNMP 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 27, “Supported Event Notifications and MIB Mapping,” on page 326.

#### 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.

```
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 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

- priv type – des or aes-128
- Step 2.** Enter authentication password and its confirmation.
- Step 3.** Enter privacy password and its confirmation.

```
switch (config) # snmp-server user admin v3 prompt auth md5 priv des
Auth password: *****
Confirm: *****
Privacy password: *****
Confirm: *****
switch (config) #
```

To retrieve the system table, run the following SNMP command:

```
snmpwalk -v3 -l authPriv -a MD5 -u admin -A "<Authentication password>" -x DES -X
"<privacy password>" <system ip> SNMPv2-MIB::system
```

#### 4.17.1.6 Configuring an SNMP Notification

➤ *To set up the SNMP Notification (traps or informs):*

- Step 1.** Make sure SNMP and SNMP notification are enable. Run:

```
switch (config) # snmp-server enable
switch (config) # snmp-server enable notify
```

- 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
switch (config) #
```



To print event notifications to the terminal (SSH or CONSOLE) refer to [Section 4.6.1, “Monitor,”](#) on page 280.

#### 4.17.1.7 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.

##### 4.17.1.7.1 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
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 [548](#) 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 36 which are expanded upon in the following subsections.

**Table 36 - 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

**Table 36 - Supported SET OIDs**

MIB Name	OID Name	OID
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

#### 4.17.1.7.2 Sending 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 4.17.1.7.1, “Enabling SNMP SET,” on page 514](#).
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).

#### 4.17.1.7.3 Setting 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 165 for more information.

#### 4.17.1.7.4 Power Cycle with SNMP

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.

#### 4.17.1.7.5 Changing 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 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 `mellanoxConfigD`

BCmdUri 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 mellanoxConfigD-BCmdUri 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

#### 4.17.1.7.6 Upgrading 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 243.

- 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

#### 4.17.1.8 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.



The JSON API is available on x86 based systems only.

##### 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.



HTTP access to the web-based management console needs to be enabled using the command "web http enable" to allow POST requests.

The HTTP client must first be authenticated by sending a POST request to the following URL:

```
http://<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 HTTP requests in the system.

See Section 4.17.2.6, "JSON Examples," on page 525 for examples.

##### 4.17.2.2 Sending the Request

After successful authentication, the HTTP client can start sending JSON requests. All requests (POST and GET) should be sent to the following URL:

```
http://<switch-ip-address>/admin/launch?script=json
```

After the request is handled in the system the HTTP 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 520 for the CLI request format.

See Section 4.17.2.4, “JSON Response Format,” on page 522 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 530.

### 4.17.2.3 JSON Request Format

#### 4.17.2.3.1 JSON Execution Requests

JSON execution requests are HTTP 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 interface ethernet 1/1"  
}
```

Multiple command execution request format:

```
{  
    "commands": ["<CLI cmd 1>", "<CLI cmd 2>", ... , <CLI cmd n>]  
}
```

Example:

```
{  
    "commands": [  
        [  
            "show interface ethernet 1/1",  
            "show interface ethernet 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 525 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 556](#)”).

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 interface ethernet 1/1"  
}
```

See Section 4.17.2.6, “JSON Examples,” on page 525 for examples.

#### 4.17.2.3.2 JSON Query Requests

JSON Query requests are HTTP 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:

```
http://<switch-ip-address>/admin/launch?script=json&job_id=<job number>
```

See Section 4.17.2.6, “JSON Examples,” on page 525 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.

##### 4.17.2.4.1 Single Command Response Format

The HTTP 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 executionThe 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 interface ethernet 1/1  
    "status": "OK",  
    "status_message": "",  
    "data":  
    {  
        "speed": "40GbE",  
        "admin_state": "up"  
    }  
}
```

See Section 4.17.2.6, “JSON Examples,” on page 525 for more examples.

##### 4.17.2.4.2 Multiple Command Response Format

The HTTP 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 interface ethernet 1/1",
      "status": "OK",
      "status_message": "",
      "data": {"speed": "40GbE", "admin_state": "up"}
    },
    {
      "executed_command": "show interface ethernet 1/100",
      "status": "ERROR",
      "status_message": "wrong interface name",
      "data": ""
    },
    {
      "executed_command": "show interface ethernet 1/2",
      "status": "ABORTED",
      "status_message": "",
      "data": ""
    }
  ]
}
```

See Section 4.17.2.6, “JSON Examples,” on page 525 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 interface ethernet 1/1",  
    "status": "PENDING",  
    "status_message": "",  
    "data": ""  
}
```

See Section 4.17.2.6, “JSON Examples,” on page 525 for examples.

#### 4.17.2.4.4Asynchronous Response Format

Response to an asynchronous request is similar to the HTTP 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 525 for examples.

#### 4.17.2.5 Supported Commands

##### 4.17.2.5.1Set 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 of currently supported “show” commands, please refer to [Appendix B,“Show Commands Supported by JSON API,” on page 1424](#).

#### 4.17.2.6 JSON Examples

The following examples use curl (a common tool in Linux systems) to send HTTP POST requests to the system.

##### 4.17.2.6.1 Authentication Example

Before sending JSON HTTP 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"  
"http://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="http://10.10.10.10/admin/launch?script=rh&template=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 http 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 "http://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 "http://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 "http://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 http GET operation to the JSON URL with the “job\_id” parameter.

Send the request:

```
curl -b /tmp/cookie -X GET "http://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"  
                    }  
                ]  
            }  
        }  
    ]  
}
```

#### 4.17.2.6.5 Error 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 "http://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 "http://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 HTTP POST requests.

Login to the WebUI → Go to the “Setup” tab → Select “JSON API” from the left side menu.



This section is displayed only if JSON API is enabled using the command “json-gw enable”.

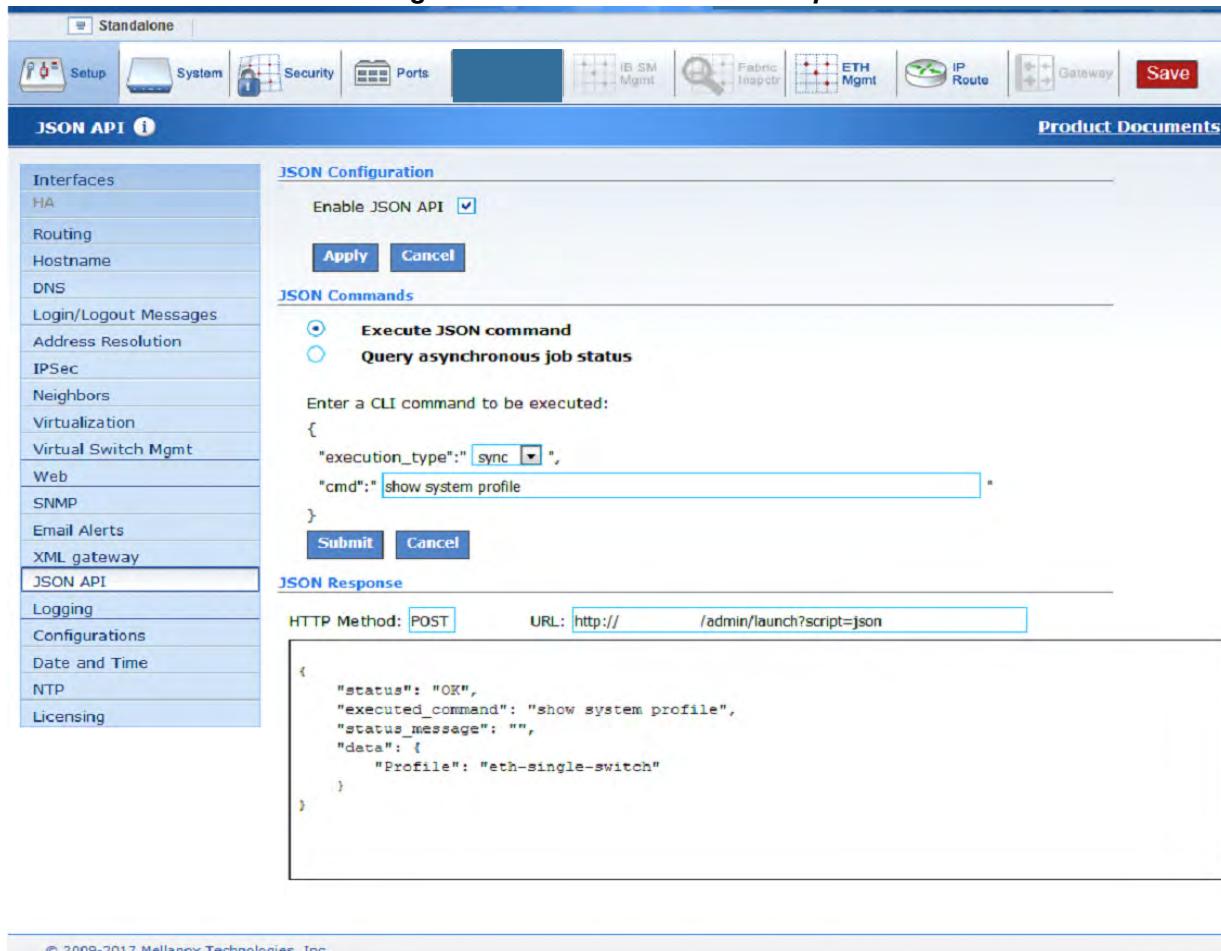
##### 4.17.2.7.1 To Execute a JSON Request

- Step 1.** Choose “Execute JSON command”
- Step 2.** Choose the “execution\_type” from the drop down list
- Step 3.** In the “cmd” field type the CLI command to execute
- Step 4.** Press “Submit”

The JSON response is then shown in the “JSON Response” box below.

The HTTP method (HTTP POST in this case) and the URL used to send the request will be displayed next to their respective field.

**Figure 14: JSON API WebUI Example**



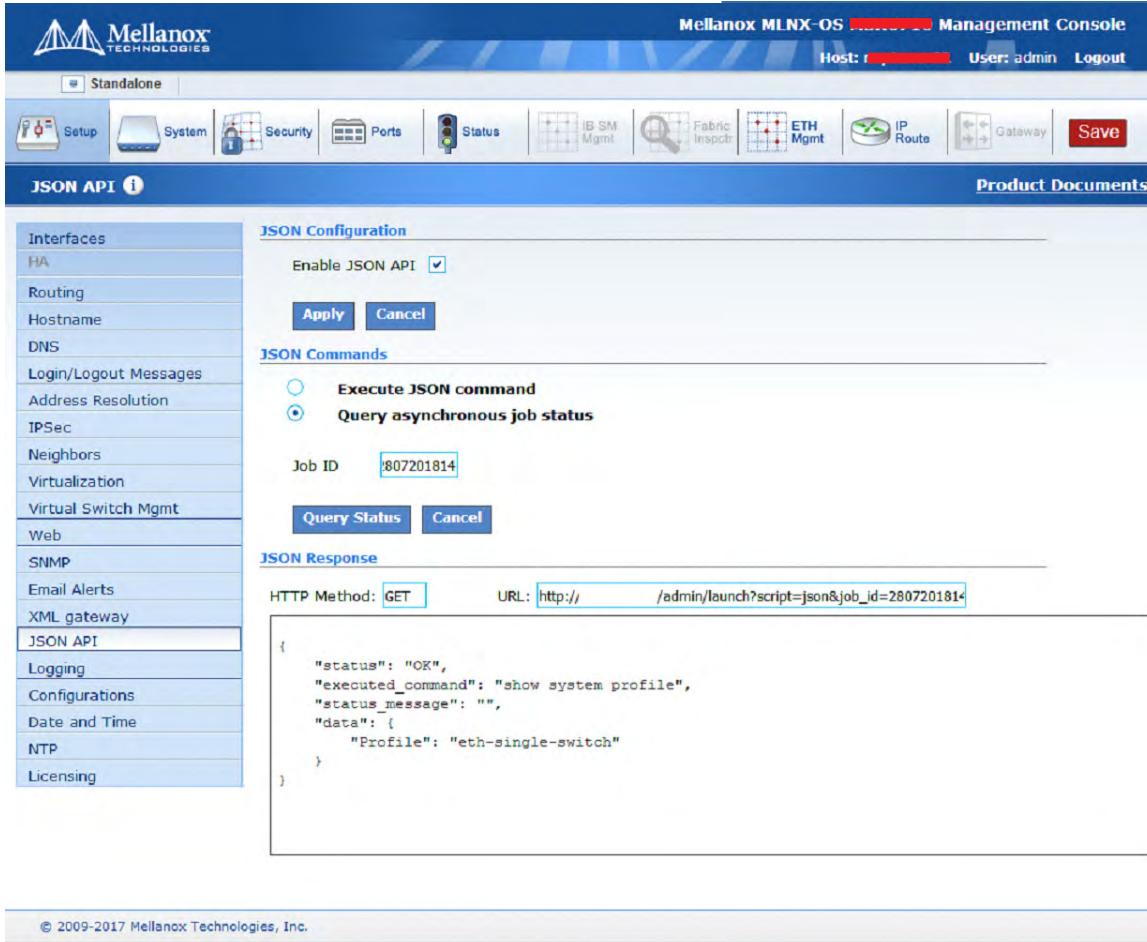
#### 4.17.2.7.2 To Query an Asynchronous JSON Request

- 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 HTTP method (HTTP GET in this case) and the URL used to send the request will be displayed next to the “HTTP Method” and “URL” field respectively.

**Figure 15: JSON API WebUI Example**



The screenshot shows the Mellanox MLNX-OS Management Console interface. The top navigation bar includes the Mellanox logo, host information (Host: 1.2.3.4), user (User: admin), and logout links. Below the navigation is a toolbar with various management icons: Setup, System, Security, Ports, Status, IB SM Mgmt, Fabric Insights, ETH Mgmt, IP Routes, and Gateway. A prominent red "Save" button is located on the right.

The main content area is titled "JSON API" and contains the following sections:

- JSON Configuration:** Includes an "Enable JSON API" checkbox (checked) and "Apply" and "Cancel" buttons.
- JSON Commands:** Shows two radio button options: "Execute JSON command" (unchecked) and "Query asynchronous job status" (checked). A "Job ID" field displays "807201814".
- Query Status:** Includes "Query Status" and "Cancel" buttons.
- JSON Response:** Displays an "HTTP Method: GET" dropdown set to "GET" and a URL input field containing "http://<host>/admin/launch?script=json&job\_id=2807201814". Below this is a code block showing the JSON response content:

```
{
  "status": "OK",
  "executed_command": "show system profile",
  "status_message": "",
  "data": {
    "Profile": "eth-single-switch"
  }
}
```

At the bottom of the page, a copyright notice reads: "© 2009-2017 Mellanox Technologies, Inc."

#### 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.

<b>Syntax Description</b>	enable	Enables SNMPD refresh mechanism.
	interval	Sets SNMPD refresh interval.
	time	In seconds. Range: 20-500.
<b>Default</b>	Enabled. Interval: 60 secs	
<b>Configuration Mode</b>	Config	
<b>History</b>	3.2.3000	
	3.4.1100	Added time parameter and updated notes
<b>Role</b>	admin	
<b>Example</b>	switch (config) # snmp-server auto-refresh interval 120	
<b>Related Commands</b>	show snmp	
<b>Notes</b>	<ul style="list-style-type: none"> <li>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".</li> <li>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.</li> </ul>	

## 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.

<b>Syntax Description</b>	<table border="0"> <tr> <td>community</td><td>Community name.</td></tr> <tr> <td>ro</td><td>Sets the read-only community string.</td></tr> <tr> <td>rw</td><td>Sets the read-write community string.</td></tr> </table>	community	Community name.	ro	Sets the read-only community string.	rw	Sets the read-write community string.
community	Community name.						
ro	Sets the read-only community string.						
rw	Sets the read-write community string.						
<b>Default</b>	Read-only community: “public” Read-write community: “”						
<b>Configuration Mode</b>	Config						
<b>History</b>	3.1.0000						
<b>Role</b>	admin						
<b>Example</b>	<pre>switch(config) # snmp-server community private rw switch (config) # show snmp SNMP enabled: yes SNMP port: 161 System contact: System location: Read-only community: public Read-write community: private  Interface listen enabled: yes No Listen Interfaces.  Traps enabled: yes Default trap community: public Default trap port: 162  No trap sinks configured. switch(config) #</pre>						
<b>Related Commands</b>	show snmp						
<b>Notes</b>	<ul style="list-style-type: none"> <li>If neither the “ro” or the “rw” parameters are specified, the read-only community is set as the default community</li> <li>If the read-only community is specified, only queries can be performed</li> <li>If the read-write community is specified, both queries and sets can be performed</li> </ul>						

## 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.

<b>Syntax Description</b>	contact name	Contact name.
<b>Default</b>	""	
<b>Configuration Mode</b>	Config	
<b>History</b>	3.1.0000	
<b>Role</b>	admin	
<b>Example</b>	<pre>switch (config) # snmp-server contact my-name switch (config) # show snmp SNMP enabled: yes SNMP port: 161 System contact: my-name System location: Read-only community: public Read-write community: private  Interface listen enabled: yes No Listen Interfaces.  Traps enabled: yes Default trap community: public Default trap port: 162  No trap sinks configured. switch (config) #</pre>	
<b>Related Commands</b>	<a href="#">show snmp</a>	
<b>Notes</b>		

## 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.

<b>Syntax Description</b>	N/A
<b>Default</b>	SNMP is enabled by default
<b>Configuration Mode</b>	Config
<b>History</b>	3.1.0000
<b>Role</b>	admin
<b>Example</b>	switch (config) # snmp-server enable
<b>Related Commands</b>	show snmp
<b>Notes</b>	

## snmp-server enable communities

**snmp-server enable communities**  
**no snmp-server enable communities**

Enables community-based authentication.  
The no form of the command disables community-based authentication.

<b>Syntax Description</b>	N/A
<b>Default</b>	SNMP server communities are enabled by default
<b>Configuration Mode</b>	Config
<b>History</b>	N/A
<b>Role</b>	admin
<b>Example</b>	switch (config) # snmp-server enable communities
<b>Related Commands</b>	show snmp
<b>Notes</b>	

## 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.

<b>Syntax Description</b>	N/A
<b>Default</b>	SNMP server multi-communities are disabled by default
<b>Configuration Mode</b>	Config
<b>History</b>	N/A
<b>Role</b>	admin
<b>Example</b>	switch (config) # snmp-server enable mult-communities
<b>Related Commands</b>	show snmp
<b>Notes</b>	

## 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.

<b>Syntax Description</b>	N/A
<b>Default</b>	SNMP notifies are enabled by default
<b>Configuration Mode</b>	Config
<b>History</b>	N/A
<b>Role</b>	admin
<b>Example</b>	switch (config) # snmp-server enable notify
<b>Related Commands</b>	show snmp
<b>Notes</b>	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.

<b>Syntax Description</b>	N/A
<b>Default</b>	SNMP MIBs are all given permission for SET requests by default
<b>Configuration Mode</b>	Config
<b>History</b>	3.6.3004
<b>Role</b>	admin
<b>Example</b>	switch (config) # snmp-server enable set-permission MELLANOX-SW-UPDATE
<b>Related Commands</b>	show snmp set-permission
<b>Notes</b>	

## snmp-server host

```
snmp-server host <IP address> {disable | {traps | informs} [<community> | <port> | version <snmp version>]}
no snmp-server host <IPv4 or IPv6 address> {disable | {traps| informs} [<community> | <port>]}
```

Configures hosts to which to send SNMP traps.

The no form of the commands removes a host from which SNMP traps should be sent.

<b>Syntax Description</b>	IP address	IPv4 or IPv6 address.
	disable	Temporarily disables sending of traps to this host.
	community	Specifies trap community string.
	port	Overrides default UDP port for this trap sink.
	snmp version	Specifies the SNMP version of traps to send to this host.
<b>Default</b>	No hosts are configured Default community is “public” Default UDP port is 162 Default SNMP version is 2c	
<b>Configuration Mode</b>	Config	
<b>History</b>	3.1.0000	
	3.2.1050	Add inform option
<b>Role</b>	admin	

**Example**

```
switch (config) # snmp-server host 10.10.10.10 traps version 1
switch (config) # show snmp
SNMP enabled: yes
SNMP port: 161
System contact:
System location:

Read-only communities:
public

Read-write communities:
(none)

Interface listen enabled: yes
No Listen Interfaces.

Traps enabled: yes
Default trap community: public
Default trap port: 162

Trap sinks:
10.10.10.10
    Enabled: yes
    Type: traps version 1
    Port: 162 (default)
    Community: public (default)
switch (config) #
```

**Related Commands**

show snmp  
snmp-server enable

**Notes**

This setting is only meaningful if traps are enabled, though the list of hosts may still be edited if traps are disabled. Refer to “snmp-server enable” command.

## snmp-server listen

```
snmp-server listen {enable | interface <ifName>}
no snmp-server listen {enable | interface <ifName> }
```

Configures SNMP server interface access restrictions.  
The no form of the command disables the listen interface restricted list for SNMP server.

<b>Syntax Description</b>	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”.
<b>Default</b>	N/A	
<b>Configuration Mode</b>	Config	
<b>History</b>	3.1.0000	
<b>Role</b>	admin	
<b>Example</b>	<pre>switch (config) # snmp listen enable switch (config) # show snmp SNMP enabled: yes SNMP port: 161 System contact: System location: Read-only community: public Read-write community: private  Interface listen enabled: yes No Listen Interfaces.  Traps enabled: yes Default trap community: public Default trap port: 162  Trap sinks: 10.10.10.10 Enabled: yes Type: traps version 1 Port: 3 Community: public (default) switch (config) #</pre>	
<b>Related Commands</b>	show snmp	
<b>Notes</b>	If enabled, and if at least one of the interfaces listed is eligible to be a listen interface, then SNMP requests will only be accepted on those interfaces. Otherwise, SNMP requests are accepted on any interface.	

## snmp-server location

**snmp-server location <system location>**  
**no snmp-server location**

Sets a value for the sysLocation variable in MIB-II.

The no form of the command clears the contents of the sysLocation variable.

<b>Syntax Description</b>	system location	String.
<b>Default</b>	""	
<b>Configuration Mode</b>	Config	
<b>History</b>	3.1.0000	
<b>Role</b>	admin	
<b>Example</b>	<pre>switch (config) # snmp-server location lab switch (config) # show snmp SNMP enabled: yes SNMP port: 161 System contact: my-name System location: lab Read-only community: public Read-write community: private  Interface listen enabled: yes No Listen Interfaces.  Traps enabled: yes Default trap community: public Default trap port: 162  No trap sinks configured. switch (config) #</pre>	
<b>Related Commands</b>	<a href="#">show snmp</a>	
<b>Notes</b>		

## 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.

<b>Syntax Description</b>	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.
<b>Default</b>	Community: public All informs and traps are enabled Port: 162	
<b>Configuration Mode</b>	Config	
<b>History</b>	3.1.0000  3.2.1050	Changed traps to notify
<b>Role</b>	admin	
<b>Example</b>	<pre>switch (config) # snmp-server community public switch (config) # show snmp SNMP enabled: yes SNMP port: 1000 System contact: my-name System location: lab Read-only community: public Read-write community: private  Interface listen enabled: yes No Listen Interfaces.  Traps enabled: yes Default trap community: public Default trap port: 162  No trap sinks configured. switch (config) #</pre>	

**Related Commands**

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.

<b>Syntax Description</b>	port	UDP port.
<b>Default</b>	161	
<b>Configuration Mode</b>	Config	
<b>History</b>	3.1.0000	
<b>Role</b>	admin	
<b>Example</b>	<pre>switch (config) # snmp-server port 1000 switch (config) # show snmp SNMP enabled: yes SNMP port: 1000 System contact: my-name System location: lab Read-only community: public Read-write community: private  Interface listen enabled: yes No Listen Interfaces.  Traps enabled: yes Default trap community: public Default trap port: 162  No trap sinks configured. switch (config) #</pre>	
<b>Related Commands</b>	<a href="#">show snmp</a>	
<b>Notes</b>		

## 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.

<b>Syntax Description</b>	v3	Configures SNMP v3 users
	auth	Configures SNMP v3 security parameters, specifying passwords in plaintext on the command line (note: passwords are always stored encrypted)
	capability	Sets capability level for SET requests
	enable	Enables SNMP v3 access for this user
	encrypted	Configures SNMP v3 security parameters, specifying passwords in encrypted form
	prompt	Configures SNMP v3 security parameters, specifying passwords securely in follow-up prompts, rather than on the command line
	require-privacy	Requires privacy (encryption) for requests from this user
<b>Default</b>	No SNMP v3 users defined	
<b>Configuration Mode</b>	Config	
<b>History</b>	3.1.0000	
<b>Role</b>	admin	
<b>Example</b>	<pre>switch (config) # snmp-server user admin v3 enable switch (config) # show snmp user User name: admin     Enabled overall:      yes     Authentication type: sha     Privacy type:        aes-128     Authentication password: (NOT SET; user disabled)     Privacy password:    (NOT SET; user disabled)     SET access:         Enabled:          yes         Capability level: admin switch (config) #</pre>	

**Related Commands**

show snmp user

**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.

## **show snmp**

**show snmp [auto-refresh | engineID | events | host | user]**

Displays SNMP-server configuration and status.

<b>Syntax Description</b>	auto-refresh	SNMP refreshed mechanism status.
	engineID	SNMP Engine ID.
	events	SNMP events.
	host	List of notification sinks.
	user	SNMP users.
<b>Default</b>	N/A	
<b>Configuration Mode</b>	Config	
<b>History</b>	3.1.0000	
<b>Role</b>	admin	
<b>Example</b>	<pre>switch (config) # show snmp user User name: Hendrix     Enabled overall:          yes     Authentication type:     sha     Privacy type:            des     Authentication password: (set)     Privacy password:        (set)     Require privacy:         yes     SET access:         Enabled:              yes         Capability level:     admin switch (config) #</pre>	
<b>Related Commands</b>	show snmp	
<b>Notes</b>		

## show snmp auto-refresh

### show snmp auto-refresh

Displays SNMPD refresh mechanism status.

<b>Syntax Description</b>	N/A
<b>Default</b>	N/A
<b>Configuration Mode</b>	Config
<b>History</b>	3.1.0000
<b>Role</b>	admin
<b>Example</b>	<pre>switch (config) # show snmp auto-refresh ===== SNMP auto refresh ===== Auto-refresh enabled:          yes Refresh interval (sec):       60  ===== Auto-Refreshed tables ===== entPhysicalTable ifTable ifXTable</pre>
<b>Related Commands</b>	<a href="#">snmp-server auto-refresh</a>
<b>Notes</b>	

## show snmp set-permission

### show snmp set-permission

Displays SNMP SET permission settings.

<b>Syntax Description</b>	N/A
<b>Default</b>	N/A
<b>Configuration Mode</b>	Config
<b>History</b>	3.6.3004
<b>Role</b>	admin
<b>Example</b>	<pre>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</pre>
<b>Related Commands</b>	<a href="#">snmp-server enable set-permission</a>
<b>Notes</b>	

#### 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.

<b>Syntax Description</b>	N/A
<b>Default</b>	XML Gateway is enabled
<b>Configuration Mode</b>	Config
<b>History</b>	3.1.0000
<b>Role</b>	admin
<b>Example</b>	<pre>switch (config) # xml-gw enable switch (config) # show xml-gw XML Gateway enabled: yes switch (config) #</pre>
<b>Related Commands</b>	<a href="#">show xml-gw</a>
<b>Notes</b>	

## show xml-gw

**show xml-gw**

Displays the XML gateway setting.

<b>Syntax Description</b>	N/A
<b>Default</b>	N/A
<b>Configuration Mode</b>	Any Command Mode
<b>History</b>	3.1.0000
<b>Role</b>	admin
<b>Example</b>	<pre>switch (config) # show xml-gw XML Gateway enabled: yes switch (config) #</pre>
<b>Related Commands</b>	<a href="#">xml-gw enable</a>
<b>Notes</b>	

#### 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.

<b>Syntax Description</b>	N/A
<b>Default</b>	JSON API is enabled
<b>Configuration Mode</b>	Config
<b>History</b>	3.6.3004
<b>Role</b>	admin
<b>Example</b>	<code>switch (config) # json-gw enable</code>
<b>Related Commands</b>	<code>show json-gw</code>
<b>Notes</b>	This command is available on x86 switch systems only.

## 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.

<b>Syntax Description</b>	N/A
<b>Default</b>	N/A
<b>Configuration Mode</b>	Any Command Mode
<b>History</b>	3.6.3004
	3.6.4000 Updated Example and Related Commands.
<b>Role</b>	admin
<b>Example</b>	<pre>switch (config) # show json-gw  JSON Gateway enabled: yes Synchronous request timeout: 30 JSON API version: 1.0</pre>
<b>Related Commands</b>	<code>json-gw enable</code> <code>json-gw synchronous-request-timeout &lt;time out value&gt;</code> <code>no json-gw synchronous-request-timeout</code>
<b>Notes</b>	This command is available on x86 switch systems only.

## show json-gw

### show json-gw

Displays the JSON API setting.

<b>Syntax Description</b>	N/A
<b>Default</b>	N/A
<b>Configuration Mode</b>	Any Command Mode
<b>History</b>	3.6.3004 3.6.4000 Updated Example and Related Commands.
<b>Role</b>	admin
<b>Example</b>	<pre>switch (config) # show json-gw  JSON Gateway enabled: yes Synchronous request timeout: 30 JSON API version: 1.0</pre>
<b>Related Commands</b>	<a href="#">json-gw enable</a> <a href="#">json-gw synchronous-request-timeout &lt;time out value&gt;</a> <a href="#">no json-gw synchronous-request-timeout</a>
<b>Notes</b>	This command is available on x86 switch systems only.

## 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 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 16: Accepting an Agent Request through the Console**

Pending node requests: 1

**Accept All** **Reject All** There are no accepted/rejected requests to clear

Name	Fingerprint	Action
switch-632476.mtr.labs.mlnx	29:9F:4B:1F...	<b>Accept</b> <b>Reject</b>

#### 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 Mellanoxswitch).

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 Writing Configuration Classes

➤ ***To write configuration classes:***

- Step 1.** Assigning Configuration Classes to a Node

Configuration files can be written and changed in the puppet server machine in the directory “`/etc/puppetlabs/puppet/manifests/`” (or “`/etc/puppet/manifests`” in case of an open source puppet server).

The file “/etc/puppetlabs/puppet/manifests/site.pp” is the main file for Puppet-classes-to-nodes association. To associate a configuration to a Puppet agent node, just append association lines as below:

```
import "netdev_vlan_example"
import "netdev_l2_vlan_example"
import "netdev_lag_example"
node 'switch-6375dc.mtr.labs.mlnx' {

    netdev_device { $hostname: }

    include vlan_example # Asserts a class vlan_example in one of the files
    include l2_interface_example

    include lag_example

}
```



If you have a puppet console, you may assign classes of configuration in the following way:

- Add the relevant classes (using the console add class button on the “nodes” page).
- Assign the classes to the relevant nodes/groups in the puppet server console (in the console node/group page -> edit -> Classes).

**Step 2.** Update VLAN.

Manifest example (located in “/etc/puppetlabs/puppet/manifests/netdev\_vlan\_example.pp”).

```
class vlan_example{

    $vlans = {
        'Vlan244' => {vlan_id => 244, ensure => present},
        'Vlan245' => {vlan_id => 245, ensure => present},
    }

    create_resources( netdev_vlan, $vlans )
}
```

**Step 3.** Update Layer 2 Interface.

Manifest example (located in “/etc/puppetlabs/puppet/manifests/netdev\_l2\_interface\_example.pp”)

```
class vlans_ensure_example{

  $vlans = {
    'Vlan347' => {vlan_id => 347, ensure => present},
    'Vlan348' => {vlan_id => 348, ensure => present},
    'Vlan349' => {vlan_id => 349, ensure => present},
  }

  create_resources( netdev_vlan, $vlans )
}

class l2_interface_example{

  include vlans_ensure_example #class to Ensure VLANs before assigning

  $l2_interfaces = {
    'ethernet 1/3' => {ensure => absent, vlan_tagging => disable}, #default
    'ethernet 1/4' => {ensure => present, vlan_tagging => enable,
    tagged_vlans => [Vlan348,Vlan347], untagged_vlan => Vlan349} #hybrid
  }

  create_resources( netdev_l2_interface, $l2_interfaces )
}
```

#### Step 4. Update LAG.

Manifest example (located in “/etc/puppetlabs/puppet/manifests/netdev\_lag\_example.pp”)

```
class lag_example{

  $lags = {
    'port-channel 101' => {ensure => present,
    links => ['ethernet 1/12', 'ethernet 1/13'], lacp => active},
    'port-channel 102' => {ensure => present,
    links => ['ethernet 1/6','ethernet 1/5'], lacp => disabled},
  }

  create_resources( netdev_lag, $lags )
}
```



You may add classes to ensure that all assigned links are with the same layer 1 and layer 2 configurations (similarly to the way we did in update l2\_interface section with vlans\_ensure\_example class).

## 4.18.5 Supported Configuration Capabilities

### 4.18.5.1 Ethernet, InfiniBand, and Port-Channel Interface Capabilities

**Table 37 - 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
admin	Disables/enables interface admin state.	up, down	admin => up
mtu	Configures the maximum transmission unit frame size for the interface.	Ethernet: 1518-9216	mtu => 1520
description	Sets the Ethernet and LAG description.	Text	description => "changed_by_puppet"

### 4.18.5.2 VLAN Capabilities

**Table 38 - VLAN Capabilities**

Field	Description	Values	Example
ensure	Creates or destroys the VLAN given as a resource ID	absent, present	ensure => present
vlan_id	The VLAN ID	1-4094 (integer)	vlan_id => 245

### 4.18.5.3 Layer 2 Ethernet Interface Capabilities

**Table 39 - L2 Ethernet and Port-Channel Interface Capabilities**

Field	Description	Values	Example
ensure	Sets the given values or restores the Layer 2 interface to default.	absent, present	ensure => present
vlan_tagging	VLAN tagging mode	enable, disable	vlan_tagging => enable
tagged_vlans	List of tagged (trunked) VLANs	2-4994 (range)	tagged_vlans => [Vlan348, Vlan347]
untagged_vlan	Untag (access) VLAN	<VLAN name>	untagged_vlan => Vlan349

#### 4.18.5.4 LAG (Port-Channel) Capabilities

**Table 40 - LAG Capabilities**

Field	Description	Values	Example
ensure	creates or destroys the port-channel given as a resource ID	absent, present	ensure => present
lacp	The LACP mode of the LAG	passive   active   on	lacp => on
links	List of ports assigned to the LAG	List of link names	links => ['ethernet 1/6','ethernet 1/5']

#### 4.18.5.5 Layer 3 Interface Capabilities

**Table 41 - L3 Interface Capabilities**

Field	Description	Values	Example
ensure	Creates or destroys the interface VLAN specified in the resource ID.	present, absent	ensure => present
ipaddress	Sets IP address on the Layer 3 interface (requires netmask).	A valid IP address	ipaddress => '192.168.4.2'
netmask	Sets netmask for the IP address.	A valid netmask (of the form X.XX.XX.XX), which creates a valid combination with the given IP address	netmask => '255.255.255.0'
method	Configures the method of the L3 interface (currently supports only static method).	static	method => static

#### 4.18.5.6 OSPF Interface Capabilities

**Table 42 - OSPF Interface Capabilities**

Field	Description	Values	Example
ensure	Creates or destroys the OSPF interface of the associated interface of the VLAN specified in the resource ID	present, absent	ensure => present
area_id	The associated area ID	Integer representing an IP	area_id => '7200'
Type	The network type	broadcast, point_to_point	type => 'point_to_point'

#### 4.18.5.7 OSPF Area Capabilities

**Table 43 - OSPF Area Capabilities**

Field	Description	Values	Example
ensure	Creates or destroys the OSPF area specified in the resource ID	present, absent	ensure => present
router_id	The OSPF area associated router ID (currently supports only default router)	default	router_id => 'default'
ospf_area_mode	The OSPF area mode	normal, stub, nssa	ospf_area_mode => 'stub'
subnets	A list of associated subnets	List of subnets	["192.168.4.0/24", "192.168.5.0/24"]

#### 4.18.5.8 Router OSPF Capabilities

**Table 44 - Router OSPF Capabilities**

Field	Description	Values	Example
ensure	Enables/disables the router ID specified in the resource ID	present, absent	ensure => present

#### 4.18.5.9 Protocol LLDP, SNMP, IP Routing and Spanning Tree Capabilities

**Table 45 - Protocol Enable/Disable Capabilities**

Field	Description	Values	Example
ensure	Enables/disables the protocol specified in the resource ID	present, absent	ensure => present

#### 4.18.5.10 Fetched Image Capabilities

**Table 46 - 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

**Table 46 - Fetched Image Capabilities**

Field	Description	Values	Example
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

#### 4.18.5.11 Installed Image Capabilities

**Table 47 - 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

#### 4.18.6 Supported Resources for Each Type

**Table 48 - Fetched Image Capabilities**

Resource Type	Puppet Type Name	Supported Resource IDs	Example
Network device	netdev_device	\$hostname	netdev_device { \$hostname: }
Layer 1 interface	netdev_interface	'ethernet <#ID>', 'port-channel <#id>', 'ib <#ID>'	netdev_interface{'ethernet 1/3': ensure => absent}
Layer 2 interface	netdev_l2_interface	'ethernet <#ID>', 'port-channel <#id>'	netdev_l2_interface{'ethernet 1/3': ensure => absent}

**Table 48 - Fetched Image Capabilities**

Resource Type	Puppet Type Name	Supported Resource IDs	Example
VLAN	netdev_vlan	VLAN name string	netdev_vlan {'Vlan244': vlan_id => 244, ensure => present }
LAG	netdev_lag	'port-channel <#id>'	netdev_lag {'port-channel 101': ensure => present }
Layer 3 interface	netdev_l3_interface	'vlan <#ID>'	netdev_l3_interface { 'vlan 4': ipaddress => '192.168.4.2', netmask => '255.255.255.0'}
OSPF interface	netdev_ospf_interface	'vlan <#ID>'	netdev_ospf_interface { 'vlan 4': ensure => present, area_id => '10' }
OSPF area	netdev_ospf_area	Valid area ID (representing an IP)	netdev_ospf_area {'10': ensure => present, ospf_area_mode=>'stub'}
OSPF router	netdev_router_ospf	Currently only supports 'default'	netdev_router_ospf {'default': ensure => present }
Protocol	mlnx_protocol	ip_routing, lldp, snmp, spanning_tree	mlnx_protocol { 'ip_routing': ensure => present }
Fetched image	mlnx_fetched_img	The image file name	mlnx_fetched_image { 'image-PPC_M460EX-3.3.4300.img': ensure => present }
Installed image	mlnx_installed_img	The image version name	mlnx_installed_img { '3.3.4300': ensure => present }

## 4.18.7 Troubleshooting

This section presents common issues that may prevent the switch from connecting to the puppet server.

### 4.18.7.1 Switch and Server Clocks are not Synchronized

This can be fixed by using NTP to synchronize the clocks at the switch (using the CLI command `ntp`) and at the server (e.g. using `ntpdate`).

### 4.18.7.2 Outdated or Invalid SSL Certificates Either on the Switch or the Server

This can be fixed on the switch using the CLI command `puppet-agent clear-certificates` (requires `puppet-agent restart` to take effect).

On the server it can be fixed by running `puppet cert clean <switch_fqdn>` (FQDN is the Fully Qualified Domain Name which consists of a hostname and a domain suffix).

#### 4.18.7.3 Communications Issue

Make sure it is possible to ping the puppet server hostname from the switch (using the CLI command `ping`).

If the hostname is not reachable (e.g. no DNS server) it can be statically added to the switch local hosts lookup (using the CLI command `ip host`).

Make sure that port 8140 is open (using the command `tracepath {<hostname> | <ip>}/8140`).

## 4.18.8 Commands

### puppet-agent

**puppet-agent**

Enters puppet agent configuration mode.

**Syntax Description** N/A

**Default** None

**Configuration Mode** Config

**History** 3.3.4200

**Role** admin

**Example**  
`switch (config) # puppet-agent  
switch (config puppet-agent) #`

**Related Commands**

**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.

<b>Syntax Description</b>	hostname	Puppet server hostname. Free string may be entered.
<b>Default</b>	puppet	
<b>Configuration Mode</b>	Config Puppet	
<b>History</b>	3.3.4200	
<b>Role</b>	admin	
<b>Example</b>	<pre>switch (config puppet-agent) # master-hostname my-puppet-server-host- name switch (config puppet-agent) #</pre>	
<b>Related Commands</b>		
<b>Notes</b>		

## 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.

<b>Syntax Description</b>	time	Can be in seconds (“30” or “30s”), minutes (“30m”), hours (“6h”), days (“2d”), or years (“5y”).
<b>Default</b>	30m	
<b>Configuration Mode</b>	Config Puppet	
<b>History</b>	3.3.4302	
<b>Role</b>	admin	
<b>Example</b>	switch (config puppet-agent) # run-interval 40m switch (config puppet-agent) #	
<b>Related Commands</b>	show puppet-agent	
<b>Notes</b>		

## 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 output with run interval

**Role** admin

**Example**

```
switch (config puppet-agent) # show puppet-agent
Puppet agent is disabled
Puppet master hostname: puppet
Run interval: 40m
switch (config puppet-agent) #
```

**Related Commands**

**Notes**

## show puppet-agent log

**show puppet-agent log [[not] [matching | continuous] <string> | files [[not] matching] <string>]**

Displays the Puppet agent's log file.

<b>Syntax Description</b>	continuous files matching not string	Puppet agent log messages as they arrive. Displays archived Puppet agent log files. Displays Puppet agent log that match a given string. Displays Puppet agent log that do not meet a certain string. Free string.
<b>Default</b>	N/A	
<b>Configuration Mode</b>	Any Command Mode	
<b>History</b>	3.3.4200	
<b>Role</b>	admin	
<b>Example</b>	<pre>switch (config puppet-agent) # show puppet-agent log Mon Nov 04 11:52:42 +0000 2013 Puppet (notice): Starting Puppet client version 3.2.3 Mon Nov 04 11:52:44 +0000 2013 Puppet (warning): Unable to fetch my node definition, but the agent run will continue: Mon Nov 04 11:52:44 +0000 2013 Puppet (warning): Could not intern from pson: source '#&lt;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_12_interface[ethernet 1/6]/untagged_vlan (notice): untagged_vlan changed 'default' to 'Vlan103' Mon Nov 04 11:53:43 +0000 2013 /Netdev_12_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_12_interface[ethernet 1/5]/vlan_tagging (notice): vlan_tagging changed 'enable' to 'disable' Mon Nov 04 11:53:48 +0000 2013 /Netdev_12_interface[ethernet 1/5]/tagged_vlans (notice): tagged_vlans changed '[]' to '[Vlan100,Vlan101,Vlan102]' Mon Nov 04 11:53:51 +0000 2013 /Netdev_12_interface[ethernet 1/1]/tagged_vlans (notice): tagged_vlans changed '[]' to '[Vlan101,Vlan104]' Mon Nov 04 11:53:51 +0000 2013 /Netdev_12_interface[ethernet 1/1]/untagged_vlan (notice): untagged_vlan changed 'default' to 'Vlan100' Mon Nov 04 11:53:54 +0000 2013 /Netdev_12_interface[ethernet 1/3]/tagged_vlans (notice): tagged_vlans changed '[]' to '[Vlan101,Vlan104]' Mon Nov 04 11:53:54 +0000 2013 /Netdev_12_interface[ethernet 1/3]/untagged_vlan (notice): untagged_vlan changed 'default' to 'Vlan100' Mon Nov 04 11:53:58 +0000 2013 /Netdev_12_interface[ethernet 1/4]/vlan_tagging (notice): vlan_tagging changed 'enable' to 'disable' Mon Nov 04 11:53:58 +0000 2013 /Netdev_12_interface[ethernet 1/4]/tagged_vlans (notice): tagged_vlans changed '[]' to '[Vlan100,Vlan101,Vlan102]' Mon Nov 04 11:54:03 +0000 2013 /Netdev_12_interface[ethernet 1/2]/tagged_vlans (notice): tagged_vlans changed '[]' to '[Vlan101,Vlan104]' Mon Nov 04 11:54:03 +0000 2013 /Netdev_12_interface[ethernet 1/2]/untagged_vlan (notice): untagged_vlan changed 'default' to 'Vlan100' Mon Nov 04 11:54:06 +0000 2013 Puppet (notice): Finished catalog run in 47.90 seconds switch (config puppet-agent) #</pre>	

### Related Commands

### Notes

## 4.19 Control Plain Policing

Control Plain 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 policy 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-prohibited 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.

<b>Syntax Description</b>	N/A
<b>Default</b>	Disabled
<b>Configuration Mode</b>	Config
<b>History</b>	3.5.1000
<b>Role</b>	admin
<b>Example</b>	<pre>switch (config) # ip filter enable switch (config) #</pre>
<b>Related Commands</b>	N/A
<b>Notes</b>	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.

<b>Syntax Description</b>	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
<b>Default</b>	Accept for input and output chains	
<b>Configuration Mode</b>	Config	
<b>History</b>	3.5.1000	
<b>Role</b>	admin	
<b>Example</b>	<pre>switch (config) # ipv6 filter chain input policy accept switch (config) #</pre>	
<b>Related Commands</b>	N/A	
<b>Notes</b>		

## 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.

<b>Syntax Description</b>	chain_name	A chain to which to add or modify a filter: <ul style="list-style-type: none"> <li>• input – input chain or ingress interfaces</li> <li>• output – output chain or egress interfaces</li> </ul>
	rule	<ul style="list-style-type: none"> <li>• append tail – appends operation to the bottom of operation list</li> <li>• insert &lt;oper_num&gt; – inserts operation at specified position (existing operation at that position moves back in the list)</li> <li>• modify &lt;oper_num&gt; – modifies existing operation at specified position. Only the parameters specified in this invocation are altered; everything else is left untouched.</li> <li>• move &lt;oper_num1&gt; to &lt;oper_num2&gt; – moves one operation to another place in the operation list</li> <li>• set &lt;oper_num&gt; – sets operation at specified position (overwrites existing)</li> </ul>
	target	<ul style="list-style-type: none"> <li>• accept – allows the packets that match the rule into the management plane</li> <li>• drop – drops packets that match the rule</li> <li>• rate-limit – allows with rate limiting in packets per sec (PPS)</li> <li>• reject-with – drops the packet and replies with an ICMP error message</li> </ul>

---

param	<ul style="list-style-type: none"> <li>• comment &lt;text&gt; – specifies description string for this rule (60 chars max)</li> <li>• dest-addr &lt;ip&gt; – 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).</li> <li>• not-dest-addr &lt;ip&gt; – IP not matching a specific destination address range</li> <li>• dest-port &lt;port(s)&gt; – matching a specific destination port or port range</li> <li>• not-dest-port &lt;port(s)&gt; – port not matching a specific destination port or port range</li> <li>• dup-delete – deletes any preexisting duplicates of this rule</li> <li>• in-intf – interface matching a specific inbound interface</li> <li>• not-in-intf &lt;if_name&gt; – interface not matching a specific inbound interface</li> <li>• out-intf &lt;if_name&gt; – matches a specific outbound interface</li> <li>• not-out-intf &lt;if_name&gt; – interface not matching a specific outbound interface</li> </ul>
param4 (cont.)	<ul style="list-style-type: none"> <li>• protocol &lt;if_name&gt; – matches a specific protocol <ul style="list-style-type: none"> <li>• tcp</li> <li>• udp</li> <li>• icmp</li> <li>• all</li> </ul> </li> <li>• not-protocol &lt;protocol&gt; – does not match a specific protocol <ul style="list-style-type: none"> <li>• tcp</li> <li>• udp</li> <li>• icmp</li> <li>• all</li> </ul> </li> <li>• source-addr &lt;ip&gt; – matches a specific source address range</li> <li>• not-source-addr &lt;ip&gt; – does not match a specific source address range</li> <li>• source-port &lt;port(s)&gt; – matches a specific source port or port range</li> <li>• not-source-port &lt;port(s)&gt; – does not match a specific source port or port range</li> <li>• state – matches packets in a particular state. Possible values: <ul style="list-style-type: none"> <li>• established – packet associated with an established connection which has seen traffic in both directions</li> <li>• related – packet that starts a new connection but is related to an existing connection</li> <li>• new – packet that starts a new, unrelated connection</li> <li>• A combination can be entered separated by commas</li> </ul> </li> </ul>

---

<b>Default</b>	N/A
<b>Configuration Mode</b>	Config
<b>History</b>	3.5.1000
<b>Role</b>	admin
<b>Example</b>	<pre>switch (config) # ipv6 filter enable chain input rule append tail target drop state related protocol all dup-delete switch (config) #</pre>
<b>Related Commands</b>	N/A
<b>Notes</b>	<ul style="list-style-type: none"><li>The source and destination ports may each be either a single number, or a range specified as “&lt;low&gt;-&lt;high&gt;”. For example: “10-20” would specify ports 10 through 20 (inclusive).</li><li>The port parameter only works in conjunction with TCP and UDP.</li><li>Setting a “positive” rule removes any corresponding “not-” rules, and vice-versa</li><li>The “state” parameter is a classification of the packet relative to existing connections</li><li>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.</li></ul>

## 4.20 Resource Scale

MLNX-OS® allows dynamic allocation of internal resources so that different internal subsystems could use as much resources as are available until resource exhaustion is reached.

Internal subsystems (e.g. ACL, OF, IP router) may use internal resources according to configured allocation policy mode which could be one of the following:

- Loose – a configuration that supports flexible user experience while providing protection to assure some protection against flooding of ARP
- Strict – allows backward compatibility



Transition between modes saves configuration and reloads the system.

The default configuration on different types of systems is as follows:

- SwitchX®-2 PPC: Strict
- SwitchX®-2 x86: Loose in Ethernet profile
- Spectrum™: Loose

### 4.20.1 Ethernet Resources

#### 4.20.1.1 Strict Mode

Table 49 presents the number of resources available for each SwitchX® based node in strict mode.

**Table 49 - Number of Resources per Node in Strict Mode**

Resource	Max Resources
Number of ACL rules	1488
Number of MAC addresses	48K
Number of IPv4 neighbors	2048
Number of IPv4 UC routes	4094
Number of IPv4 MC routes	671
Number of IPv4 (ECMP) UC routes	2K

#### 4.20.1.2 Loose Mode – SwitchX®

Table 50 presents the number of resources available for each SwitchX® based node in loose mode.

**Table 50 - Number of Resources per Node in Strict Mode for SwitchX Based Systems**

Resource	Max Resources
Number of ACL rules	5120
Number of MAC addresses	48K
Number of IPv4 neighbors	8000
Number of IPv4 UC routes	10936
Number of IPv4 MC routes	2047
Number of IPv4 (ECMP) UC routes	5312

#### 4.20.1.3 Loose Mode – Spectrum™

Table 51 presents the number of resources available for each Spectrum™ based node in strict mode.

**Table 51 - Number of Resources per Node in Strict Mode for Spectrum Based Systems**

Resource	Max Resources
Number of ACL rules	5120
Number of MAC addresses	88K
Number of IPv4 neighbors	8000
Number of IPv4 UC routes	10936
Number of IPv4 MC routes	2047
Number of IPv4 (ECMP) UC routes	5312

## 4.20.2 Commands

### system resource table

```
system resource table {loose | strict}  
no system resource table
```

Configures system resource table.

The no form of the command restores the system to its default mode.

<b>Syntax Description</b>	loose	Sets system resource table mode as loose
	strict	Sets system resource table mode as strict
<b>Default</b>	SwitchX®-2 x86: Loose Spectrum™: Loose	
<b>Configuration Mode</b>	Config	
<b>History</b>	3.5.1000	
	3.6.3004	Added support for Proxy-ARP
<b>Role</b>	admin	
<b>Example</b>	switch (config) # system resource table strict	
<b>Related Commands</b>	N/A	
<b>Notes</b>	<ul style="list-style-type: none"><li>x86 based systems support strict and loose modes</li><li>Spectrum based systems only support loose mode</li><li>Transition between modes saves configuration and reloads the system (after user approval)</li></ul>	

## show system resource table

**show system resource table [<table-id>]**

Displays all system resource in-use value.

<b>Syntax Description</b>	table-id	Displays information for a specific in-use resource table
<b>Default</b>	N/A	
<b>Configuration Mode</b>	Any Command Mode	
<b>History</b>	3.5.1000	
	3.6.3004	Added support for Proxy-ARP
<b>Role</b>	admin	

### Example

```

switch (config) # show system resource table
-----
Table-Id          In-Use
-----
acl              0
ipv4-uc          1
ipv4-mc          0
ipv4-neigh       0
ipv6-uc          0
ipv6-mc          0
ipv6-neigh       0

System mode: loose
Total configured entries: 1

switch (config) # show system resource table acl
-----
Table-Id          In-Use
-----
acl              0      0
eth-ipv4-uc      7500   0
ib-ipv4-uc       3750   0
ib-ipv4-grh      1875   0
uc-route         160    0
ipv4-mc          0      0

Mode: loose
Total configured entries: 0

```

<b>Related Commands</b>	N/A
-------------------------	-----

<b>Notes</b>
--------------

## 4.21 Linux Dockers

MLNX-OS® adds the ability for users to run their own applications on a Linux docker's image embedded in the switch SW. The container is a pure application sandbox with resource isolation in terms of memory and compute from the system code/NOS. The container implementation complements MLNX-OS's VM support to provide a new set of capabilities:

- Access to network traffic – containers are implemented in MLNX-OS® in the same name space as the network devices. This allows the SW to send and receive packets from the switch's ports by opening a standard Linux socket over the network device, using an IP address that has been set to the device via the legacy management interface (e.g. JSON over HTTP).



The socket should have a unique port number to prevent ambiguity of applications between the container and the MLNX-OS®.

- Calling the SDK interfaces – Applications running in the docker container are able to implement its own set of tools such as telemetry features within the network devices. By calling the switch SDK APIs, it can read data that is not exposed in the MLNX-OS® user interface, or register to receive events that occur in the system (e.g. port up/down).



The container implementation does not limit the container developer from calling the SDK to set parameters yet. This is strongly discouraged as it may cause unexpected system behavior where the MLNX-OS® and the container application manage the same resources.

- Query the Linux tables provisioned by MLNX-OS® such as neighbor cache, routing tables, L3 interfaces attributes etc.

It is possible to configure multiple containers, however, they would compete for the same memory and compute resources preallocated by MLNX-OS® (varies for different systems). For the proper function of the overall system, it is strongly recommended that all resource configuration done from the container should use MLNX-OS® user interfaces such as JSON/SNMP utilizing the internal loopback interface.

#### 4.21.1 Commands

##### docker

**docker**  
**no docker**

Enables dockers then enters docker configuration context.  
The no form of the command disables dockers, removes configuration, and deletes all containers and docker images.

<b>Syntax Description</b>	N/A
<b>Default</b>	N/A
<b>Configuration Mode</b>	Config
<b>History</b>	3.6.2940
<b>Role</b>	admin
<b>Example</b>	<pre>switch (config) # docker switch (config docker) #</pre>
<b>Related Commands</b>	N/A
<b>Notes</b>	

## commit

**commit <container-name> <image-name> <image-version>**

Creates a new image from a running container.

<b>Syntax Description</b>	container-name	Name of the running container to commit
	image-name	Name of the new image to be created
	image-version	Version of the new image to be created
<b>Default</b>	N/A	
<b>Configuration Mode</b>	Config Docker	
<b>History</b>	3.6.2940	
<b>Role</b>	admin	
<b>Example</b>	switch (config docker) # commit mycontainer test latest	
<b>Related Commands</b>	N/A	
<b>Notes</b>		

## remove image

**remove image <image-name> <image-version>**

Removes an image from the Linux docker service.

<b>Syntax Description</b>	image-name image-version	Name of the new image to be deleted Version of the new image to be deleted
<b>Default</b>	N/A	
<b>Configuration Mode</b>	Config Docker	
<b>History</b>	3.6.3520 3.6.2940	
<b>Role</b>	admin	
<b>Example</b>	switch (config docker) # remove image test latest	
<b>Related Commands</b>	docker	
<b>Notes</b>		

## exec

**exec <container-name> <program-executable>**

Executes a program within a running container.

<b>Syntax Description</b>	container-name	Name of the running container to commit
	program-executable	Linux command
<b>Default</b>	N/A	
<b>Configuration Mode</b>	Config Docker	
<b>History</b>	3.6.3520 3.6.2940	
<b>Role</b>	admin	
<b>Example</b>	switch (config docker) # exec mycontainer "ls -la"	
<b>Related Commands</b>	docker	
<b>Notes</b>		

## load

**load <image-name>**

Loads an image from a TAR archive.

<b>Syntax Description</b>	image-name	Name of the TAR image to be loaded
<b>Default</b>	N/A	
<b>Configuration Mode</b>	Config Docker	
<b>History</b>	3.6.2940	
<b>Role</b>	admin	
<b>Example</b>	switch (config docker) # load test	
<b>Related Commands</b>	docker	
<b>Notes</b>		

## pull

**pull <image-name>[:<version>]**

Pulls a docker image from a docker repository.

<b>Syntax Description</b>	image-name Format: Name:Version If only “Name” is provided, “version” defaults to latest
<b>Default</b>	N/A
<b>Configuration Mode</b>	Config Docker
<b>History</b>	3.6.2940
<b>Role</b>	admin
<b>Example</b>	<pre>switch (config docker) # pull test Using default tag: latest latest: Pulling from library/test 45a2e645736c: Pull complete Digest: sha256:c577af3197aacedf79c5a204cd7f493c8e07ffbce7f88f7600bf19c688c38799 Status: Downloaded newer image for test:latest switch (config docker) #</pre>
<b>Related Commands</b>	docker
<b>Notes</b>	

## save

**save <image-name> <version>**

Saves an image to a TAR archive.

<b>Syntax Description</b>	image-name	Image name Format: Name Version If only “Name” is provided, “Version” defaults to latest
<b>Default</b>	N/A	
<b>Configuration Mode</b>	Config Docker	
<b>History</b>	3.6.2940	
<b>Role</b>	admin	
<b>Example</b>		switch (config docker) # save test Saving: test.img this could take a while... Compressing: test.img this could take a while... switch (config docker) #
<b>Related Commands</b>	docker	
<b>Notes</b>		

## shutdown

**shutdown**  
**no shutdown**

Stops all docker containers, and deletes all non-auto containers.  
The no form of the command enables the docker Linux service and runs all configured auto-start containers

<b>Syntax Description</b>	N/A
<b>Default</b>	N/A
<b>Configuration Mode</b>	Config Docker
<b>History</b>	3.6.2940
<b>Role</b>	admin
<b>Example</b>	switch (config docker) # no shutdown
<b>Related Commands</b>	docker
<b>Notes</b>	

## start

```
start <image-name> <image-version> <container-name> <starting-point>
no start <container-name>
```

Starts a new container from an image.

The no form of the command stops a running docker container.

<b>Syntax Description</b>	<table border="0"> <tr> <td>image-name</td><td>Name of the new image to be started</td></tr> <tr> <td>image-version</td><td>Version of the image to be started</td></tr> <tr> <td>container-name</td><td>Name of the running container to commit</td></tr> <tr> <td>starting-point</td><td> <ul style="list-style-type: none"> <li>• init – persistent, start the container after boot, when system initialization is done</li> <li>• data-path-ready – persistent, start the container after boot, when data-path is ready to be configured</li> <li>• now – start the container now, this is not persistent</li> </ul> </td></tr> </table>	image-name	Name of the new image to be started	image-version	Version of the image to be started	container-name	Name of the running container to commit	starting-point	<ul style="list-style-type: none"> <li>• init – persistent, start the container after boot, when system initialization is done</li> <li>• data-path-ready – persistent, start the container after boot, when data-path is ready to be configured</li> <li>• now – start the container now, this is not persistent</li> </ul>
image-name	Name of the new image to be started								
image-version	Version of the image to be started								
container-name	Name of the running container to commit								
starting-point	<ul style="list-style-type: none"> <li>• init – persistent, start the container after boot, when system initialization is done</li> <li>• data-path-ready – persistent, start the container after boot, when data-path is ready to be configured</li> <li>• now – start the container now, this is not persistent</li> </ul>								

**Default**	N/A															
**Configuration Mode**	Config Docker															
**History**					----------	----------------------		3.6.2940			3.6.3520			3.6.4110	Added example output	
**Role**	admin															
**Example**	``` switch (config docker) # start centos latest test now Starting docker container. Please wait (this can take a minute)... switch (config docker) #  switch (config docker) # no start test  switch (config docker) # start busybox latest mmm now privileged ? network           Add network privileges to the container           (--privilege flag) sdk from the           Add required mounts to use Mellanox SDK           container ```															
**Related Commands**	docker															
**Notes**	The no form of the command will also remove the container if it is not persistent.															

## image upload

**image upload <filename> <upload\_url>**

Uploads an image file to a remote host.

<b>Syntax Description</b>	filename upload_url	Name of file FTP, TFTP, SCP and SFTP are supported (e.g. scp://username[:password]@hostname/path/filename)
<b>Default</b>	N/A	
<b>Configuration Mode</b>	Config	
<b>History</b>	3.6.2940	
<b>Role</b>	admin	
<b>Example</b>	switch (config) # image upload centos.img.gz scp://username:password@192.168.10.125/var/www/html/<image_name>	
<b>Related Commands</b>	N/A	
<b>Notes</b>		

## file image upload

**file image upload <filename> <upload\_url>**

Uploads a file to a remote host.

<b>Syntax Description</b>	filename upload_url	Name of file FTP, TFTP, SCP and SFTP are supported (e.g. scp://username[:password]@hostname/path/filename)
<b>Default</b>	N/A	
<b>Configuration Mode</b>	Config	
<b>History</b>	3.6.2940	
<b>Role</b>	admin	
<b>Example</b>	switch (config) # file image upload centos.img.gz scp://username:password@192.168.10.125/var/www/html/<image_name>	
<b>Related Commands</b>	N/A	
<b>Notes</b>		

## docker label

[no] docker label <label name>

Creates a label which can be used as shared storage between containers.  
The no form of the command removes the label.

<b>Syntax Description</b>	N/A
<b>Default</b>	N/A
<b>Configuration Mode</b>	Config
<b>History</b>	3.6.4110
<b>Role</b>	admin
<b>Example</b>	<pre>switch (config) # docker label switch (config) #</pre>
<b>Related Commands</b>	N/A
<b>Notes</b>	

## docker copy-sdk

### docker copy-sdk

The command provides access to the switch SDK APIs, enabling applications running on dockers access to the switch hardware.

<b>Syntax Description</b>	N/A
<b>Default</b>	N/A
<b>Configuration Mode</b>	Config
<b>History</b>	3.6.4110
<b>Role</b>	admin
<b>Example</b>	<pre>switch (config) # docker copy-sdk switch (config) #</pre>
<b>Related Commands</b>	N/A
<b>Notes</b>	

## show docker images

### show docker images

Display docker images.

<b>Syntax Description</b>	N/A
<b>Default</b>	N/A
<b>Configuration Mode</b>	Any Command Mode
<b>History</b>	3.6.3520 3.6.2940
<b>Role</b>	admin
<b>Example</b>	<pre>switch (config) # show docker images ----- Image          Version   Created        Size ----- ubuntu         latest    Less than a secon 117MB d ago ubuntu-sdk     v1       41 seconds ago 215MB</pre>
<b>Related Commands</b>	N/A
<b>Notes</b>	

## show docker ps

**show docker ps**

Display docker containers.

<b>Syntax Description</b>	N/A
<b>Default</b>	N/A
<b>Configuration Mode</b>	Any Command Mode
<b>History</b>	3.6.3520 3.6.2940
<b>Role</b>	admin
<b>Example</b>	<pre>switch (config) # show docker ps ----- Container          Image:Version      Created           Status ----- my_ubuntu_app      ubuntu:latest     56 seconds ago   Up 50 seconds</pre>
<b>Related Commands</b>	N/A
<b>Notes</b>	

## show docker labels

### show docker labels

Displays docker labels.

<b>Syntax Description</b>	N/A
<b>Default</b>	N/A
<b>Configuration Mode</b>	Config
<b>History</b>	3.6.4110
<b>Role</b>	admin
<b>Example</b>	<pre>switch (config) # docker label label_name1 (config) # docker label label_name2 (config) # docker start busybox latest cont_name1 data-path-ready init now (config) # docker start busybox latest cont_name1 data-path-ready init now (config) # docker start busybox latest cont_name1 now label privileged (config) # docker start busybox latest cont_name1 now label dagan label_name1 label_name2 (config) # docker start busybox latest cont_name1 now label label_name1 Attempting to start docker container. Please wait (this can take a minute)... (config) # docker start busybox latest cont_name2 init label label_name1 (config) # show docker labels Storage label : label_name1     configured containers list : cont_name2     active containers list : cont_name1  Storage label : label_name2</pre>
<b>Related Commands</b>	N/A
<b>Notes</b>	

## 5 Ethernet Switching

### 5.1 Interface

Interface Ethernet have the following physical set of configurable parameters

- Admin state – enabling or disabling the interface
- Flow control – admin state per direction (send or receive)
- MTU (Maximum Transmission Unit) – 1500-9216 bytes
- Speed – 1/10/40/56/100GbE (depending interface type and system)
- Description – user defined string
- Module-type – the type of the module plugged in the interface

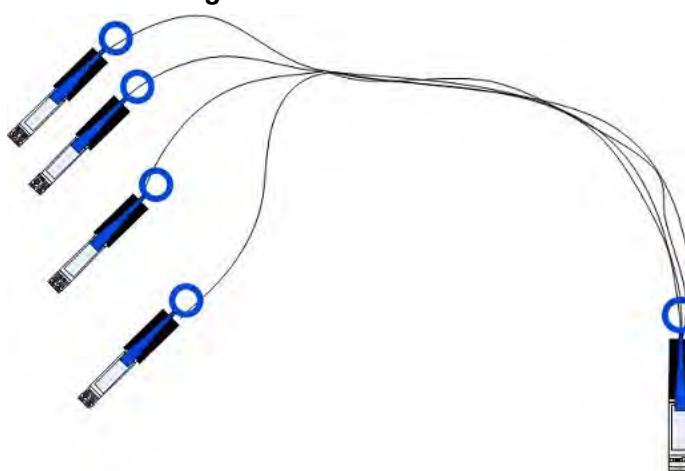


To use 100GbE QSFP interfaces as 25/10GbE (via QSA adapter), the speed must be manually set with the command “speed 25000” or “speed 10000” respectively under the interface configuration mode.

#### 5.1.1 Break-Out Cables

The break-out cable is a unique Mellanox capability, where a single physical quad-lane QSFP port is divided into 2 dual-lane ports or 4 single-lane ports. It maximizes the flexibility of the end user to use the Mellanox switch with a combination of dual-lane, single-lane and quad-lane interfaces according to the specific requirements of its network. Certain ports cannot be split at all, and there are ports which can be split into 2 ports only (for more information please refer to your Switch System Hardware User Manual). 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 or 1,2,3,4). Each sub-physical port is then handled as an individual port. For example, splitting port 10 into 4 lanes gives the following new ports: 1/10/1, 1/10/2, 1/10/3, 1/10/4.

**Figure 17: Break-Out Cable**



A split-4 operation results in blocking a quad-lane port in addition to the one being split. A set of hardware restrictions determine which of the ports can be split.

Specific ports can be split by using a QSFP 1X4 breakout cable to split one single-lane port into 4 lanes (4 SFP+ connectors). These 4 lanes then go, one lane to each of the 4 SFP+ connectors.



Splitting the interface deletes all configuration on that interface.

When splitting an interface's traffic into 4 data streams (four lanes) one of the other ports on the switch is disabled (unmapped).

To see the exact splitting options available per system, refer to each specific system's hardware user manual (Cabling chapter) located on the Mellanox website.

#### 5.1.1.1 Changing the Module Type to a Split Mode

➤ *To split an interface:*

**Step 1.** Shut down all the ports related to the interface. Run:

- in case of split-2, shut down the current interface only
- in case of split-4, shut down the current interface and the other interface according switch system's spec

```
switch (config) # interface ethernet 1/1
switch (config interface ethernet 1/1) # shutdown
switch (config interface ethernet 1/1) # exit
switch (config) # interface ethernet 1/4
switch (config interface ethernet 1/4) # shutdown
```

**Step 2.** Split the ports as desired. Run:

```
switch (config interface ethernet 1/4) # module-type qsfp-split-4
switch (config interface ethernet 1/4) #
```

**Step 3.** The following warning will be displayed:

```
the following interfaces will be unmapped: 1/420 1/19.
Choose Yes when prompted Type 'yes' to confirm split
```

The <ports> field in the warning refers to the affected ports from splitting port <inf> in the applied command.



Please beware that splitting a port into 4 prevents you from accessing the splittable port, and an additional one. For example, in the procedure above, ports 3 and 4 become unaccessible.

### 5.1.1.2 Unsplitting a Split Port

➤ *To unsplit a split port:*

**Step 1.** Shut down all of the split ports. Run:

```
switch (config interface ethernet 1/4/4) # shutdown
switch (config interface ethernet 1/4/4) # exit
switch (config) # interface ethernet 1/4/3
switch (config interface ethernet 1/4/3) # shutdown
switch (config interface ethernet 1/4/3) # exit
switch (config) # interface ethernet 1/4/2
switch (config interface ethernet 1/4/2) # shutdown
switch (config interface ethernet 1/4/2) # exit
switch (config) # interface ethernet 1/4/1
switch (config interface ethernet 1/4/1) # shutdown
```

**Step 2.** From the first member of the split (1/4/1), change the module-type back to QSFP. Run:

```
switch (config interface ethernet 1/4/1) # module-type qsfp
```



The module-type can be changed **only** from the first member of the split and **not** from the interface which has been split.

The following warning will be displayed:

The following interfaces will be unmapped: 1/4/1 1/4/2 1/4/3 1/4/4.

**Step 3.** Type “yes” when prompted “Type ‘yes’ to confirm unsplit.”

### 5.1.2 56GbE Link Speed

Mellanox offers proprietary speed of 56Gb/s per Ethernet interface.



The following OPNs support 56GbE:

- MSX6036F-xxxx
- MSX1036x-xxxS
- MSX1024x-xxxS
- MSX1012x-xxxx
- MSX6012F-xxxx
- MSX6018F-xxxx

The following OPNs do not support 56GbE:

- MSX6036T-xxxx
- MSX1036x-xxxR
- MSX6012T-xxxx
- MSX6018T-xxxx



56GbE speed is not supported on SwitchX® (A1) ASIC based switch systems.

➤ **To achieve 56GbE link speed:**

**Step 1.** Make sure your system is 56Gb/s capable (e.g. SX6036F, SX1024, and SX1036).

**Step 2.** Set the system profile to be eth-single-switch, and reset the system:

```
switch (config) # system profile eth-single-profile
```

**Step 3.** Set the speed for the desired interface to 56GbE as follows. Run:

```
switch (config) # interface ethernet 1/1
switch (config interface ethernet 1/1) # speed 56000
switch (config interface ethernet 1/1) #
```

**Step 4.** Verify the speed is 56GbE

```
switch (config) # show interfaces ethernet 1/1
Eth1/1
Admin state: Enabled
Operational state: Down
Description: N/A
Mac address: 00:02:c9:5d:e0:26
MTU: 1522 bytes
Flow-control: receive off send off
Actual speed: 56 Gbps
Switchport mode: access
Rx
0 frames
0 unicast frames
0 multicast frames
0 broadcast frames
0 octets
0 error frames
0 discard frames
Tx
0 frames
0 unicast frames
0 multicast frames
0 broadcast frames
0 octets
0 discard frames
switch (config) #
```

### 5.1.3 Transceiver Information

MLNX-OS® offers the option of viewing the transceiver information of a module or cable connected to a specific interface. The information is a set of read-only parameters burned onto the EEPROM of the transceiver by the manufacturer. The parameters include identifier (connector type), cable type, speed and additional inventory attributes.

- **To display transceiver information of a specific interface, run:**

```
switch (config) # show interfaces ethernet 1/10 transceiver
Port 1/10 state
    identifier          : QSFP+
    cable/module type   : Passive copper, unequalized
    ethernet speed and type: 56GigE
    vendor              : Mellanox
    cable length        : 1m
    part number         : MC2207130-001
    revision            : A3
    serial number       : MT1238VS04936
switch (config) #
```



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

### 5.1.4 High Power Transceivers

Mellanox switch systems offer high power transceiver (LR4) support in the following ports:

**Table 52 - LR4/ER4 Switch and Port Support**

Transceiver			Switch OPN	Supported Ports
Speed	Protocol	Power Consumption [W]		
40GbE	LR4/ER4	3.5	SN2100/SN2410/SN2700	All ports
			SX1036/SX1710	1, 3, 33, 35
			SX1012	All ports
			SX1024/SX1410	50, 52, 54, 56, 58, 60
100GbE	LR4	4.5	SN2100	1, 2, 15, 16
			SN2410	49, 50, 55, 56
			SN2700	1, 2, 31, 32

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 ethernet” is run.

### 5.1.5 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 of errors that can be corrected depends on the FEC algorithm and the amount of redundant data.

100GbE Mellanox-to-Mellanox Ethernet connections always enable standard Reed Solomon (RS) FEC on all cables.

If a Mellanox system is connected to a 3rd party system, then FEC is only activated if the 3rd party requests it also.

## 5.1.6 Commands

### interface ethernet

**interface ethernet <slot>/<port>|/<subport>]-[<slot>/<port>|/<subport>]]**

Enters the Ethernet interface or Ethernet interface range configuration mode.

<b>Syntax Description</b>	<slot>/<port>	Ethernet port number.
	subport	Ethernet subport number. to be used in case of split port.
<b>Default</b>	N/A	
<b>Configuration Mode</b>	Config	
<b>History</b>	3.1.0000	
	3.2.1100	Added range support
<b>Role</b>	admin	
<b>Example</b>	<pre>switch (config) # interface ethernet 1/1 switch (config interface ethernet 1/1) # exit switch (config) # interface ethernet 1/1-1/10 switch (config interface ethernet 1/1-1/10) #</pre>	
<b>Related Commands</b>	show interfaces ethernet	
<b>Note</b>		

## boot-delay

**boot-delay [<time>]**  
**no boot-delay**

Configures interface boot-delay timer.

The no form of the command returns boot-delay time to its default value.

<b>Syntax Description</b>	time	Boot delay time in seconds Range: 0-600
<b>Default</b>	0 seconds	
<b>Configuration Mode</b>	Config Interface Ethernet Config Interface Port Channel Config Interface MLAG Port Channel	
<b>History</b>	3.6.2002	
<b>Role</b>	admin	
<b>Example</b>	switch (config interface ethernet 1/1) # boot-delay 60	
<b>Related Commands</b>	show interfaces ethernet	
<b>Note</b>	This command delays the interface from boot time of the interface Configuration save and system reboot is required for the configuration to take effect.	

## flowcontrol

**flowcontrol {receive | send} {off | on} [force]**

Enables or disables IEEE 802.3x link-level flow control per direction for the specified interface.

<b>Syntax Description</b>	receive   send	receive - ingresses direction send - egresses direction
	off   on	on - enables IEEE 802.3x link-level flow control for the specified interface on receive or send. off - disables IEEE 802.3x link-level flow control for the specified interface on receive or send
	force	Forces command implementation.
<b>Default</b>	receive off, send off	
<b>Configuration Mode</b>	Config Interface Ethernet Config Interface Port Channel Config Interface MLAG Port Channel	
<b>History</b>	3.1.0000 3.3.4500                          Added MLAG port-channel configuration mode	
<b>Role</b>	admin	
<b>Example</b>	<pre>switch (config interface ethernet 1/1) # flowcontrol receive off switch (config interface ethernet 1/1) #</pre>	
<b>Related Commands</b>	show interfaces ethernet	
<b>Note</b>	N/A	

## module-type

**module-type <type> [force]**  
**no module-type <type> [force]**

Splits the interface to two or four separate interfaces, or merges them back to a single interface (QSFP).

The no form of the command resets the interface to its default configuration.

<b>Syntax Description</b>	type	qsfp - Port runs at 40000/56000Mbps qsfp-split-2 - Port is split and runs at 2X10000Mb/s qsfp-split-4 - Port is split and runs at 4X10000Mb/s
	force	Force the split operation without asking for user confirmation.
<b>Default</b>	QSFP	
<b>Configuration Mode</b>	Config Interface Ethernet	
<b>History</b>	3.1.1400	
	3.5.0000	Added note
	3.6.3640	Added note
	3.6.4006	Added note
<b>Role</b>	admin	
<b>Example</b>	<pre>switch (config interface ethernet 1/4) # module-type qsfp-split-4 The following interfaces will be unmapped: 1/4 1/1 Type 'yes' to confirm split: yes switch (config interface ethernet 1/4) #</pre>	
<b>Related Commands</b>		
<b>Note</b>	<ul style="list-style-type: none"> <li>• Port can't be splitted when storm-control is configured on port</li> <li>• Force command don't remove storm-control configuration. Error output:  <pre>% Storm control configuration must be removed from interface Eth1/2</pre> </li> <li>• After a split port is created or deleted, the forwarding mode for each split port is set according to the global configuration</li> <li>• The affected interfaces should be disabled prior to the operation</li> <li>• In order to unsplit the interface, use the command with "qsfp", the speed is set to 40Gb/s "module-type qsfp"</li> <li>• The following speeds are supported on the different Ethernet interface types: <ul style="list-style-type: none"> <li>• qsfp - 1G, 10G, 25G, 40G, 50G, 56G, 100G</li> <li>• qsfp-split-2 - 1G, 10G, 25G, 50G</li> <li>• qsfp-split-4 - 1G, 10G, 25G</li> </ul> </li> </ul>	

**mtu****mtu <frame-size>**

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

<b>Syntax Description</b>	frame-size	This value may be 1500-9216 bytes
<b>Default</b>	1500 bytes	
<b>Configuration Mode</b>	Config Interface Ethernet Config Interface Port Channel Config Interface MLAG Port Channel	
<b>History</b>	3.1.0000	
	3.3.4500	Added MLAG port-channel configuration mode
<b>Role</b>	admin	
<b>Example</b>	<pre>switch (config interface ethernet 1/1) # mtu 9216 switch (config interface ethernet 1/1) #</pre>	
<b>Related Commands</b>	show interfaces ethernet	
<b>Note</b>		

## shutdown

**shutdown**  
**no shutdown**

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

## description

**description <string>**  
**no description**

Sets an interface description.

The no form of the command returns the interface description to its default value.

<b>Syntax Description</b>	string	40 bytes
<b>Default</b>	""	
<b>Configuration Mode</b>	Config Interface Ethernet Config Interface Port Channel Config Interface MLAG Port Channel	
<b>History</b>	3.1.0000	
	3.3.4500	Added MLAG port-channel configuration mode
<b>Role</b>	admin	
<b>Example</b>	<pre>switch (config interface ethernet 1/1) # description my-interface switch (config interface ethernet 1/1) #</pre>	
<b>Related Commands</b>	show interfaces ethernet	
<b>Note</b>		

speed

**speed <port speed> [force]**  
**no speed**

Sets the speed of the interface.

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

## load-interval

**load-interval <time>**  
**no load-interval**

Sets the interface counter interval.

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

<b>Syntax Description</b>	time	In seconds.
<b>Default</b>	300 seconds.	
<b>Configuration Mode</b>	Config Interface Ethernet Config Interface Port Channel Config Interface MLAG Port Channel	
<b>History</b>	3.3.0000	
	3.3.4500	Added MLAG port-channel configuration mode
<b>Role</b>	admin	
<b>Example</b>	switch (config interface ethernet 1/1) # load-interval 30 switch (config interface ethernet 1/1) #	
<b>Related Commands</b>	show interfaces ethernet	
<b>Note</b>	This interval is used for the ingress rate and egress rate counters.	

## ip address dhcp

**ip address dhcp**  
**no ip address dhcp**

Enables DHCP on this Ethernet interface.

<b>Syntax Description</b>	N/A
<b>Default</b>	Disabled
<b>Configuration Mode</b>	Config Interface Ethernet set as router interface Config Interface Port Channel set as router interface
<b>History</b>	3.4.2008
<b>Role</b>	admin
<b>Example</b>	<pre>switch (config interface ethernet 1/1) # ip address dhcp switch (config interface ethernet 1/1) #</pre>
<b>Related Commands</b>	interface ethernet show interfaces ethernet
<b>Note</b>	

## fec-override

```
fec-override <fec-configuration> [force]
no fec-override <fec-configuration> [force]
```

Changes FEC configuration on a specific port or range of ports.  
The no form of the command resets this parameter to its default value.

<b>Syntax Description</b>	fec-configuration	<ul style="list-style-type: none"><li>auto – auto-FEC selection</li><li>no-fec – disables FEC</li><li>fec-on – enables FEC</li></ul>
	force	Forces configuration (does not require toggling interface to take effect)
<b>Default</b>	Auto-FEC selection	
<b>Configuration Mode</b>	Config Interface Ethernet	
<b>History</b>	3.5.0000	
	3.6.2002	Added force option
<b>Role</b>	admin	
<b>Example</b>	switch (config interface ethernet 1/2) # fec-override fec-on	
<b>Related Commands</b>	show interfaces ethernet	
<b>Notes</b>	<ul style="list-style-type: none"><li>This command is supported only on Spectrum™ based switch systems</li><li>Use this command with caution. There is no limitation in configuring non-standard FEC. It may cause the link to malfunction.</li></ul>	

## **clear counters**

## **clear counters**

Clears the interface counters.

## show interfaces status

### show interfaces status

Displays the configuration and status for the interface

<b>Syntax Description</b>	N/A				
<b>Default</b>	N/A				
<b>Configuration Mode</b>	Any Command Mode				
<b>History</b>	3.6.4006				
<b>Role</b>	admin				
<b>Example</b>	<pre>switch (config) # show interfaces status ----- Port      Oper State    Admin     Speed      Description ----- mgmt0    Down        Enabled   1000Mb/s (auto) - mgmt1    Down        Enabled   UNKNOWN    - Eth1/1    Down        Enabled   100 Gbps   - Eth1/2    Up          Enabled   100 Gbps   - Eth1/3    Up          Enabled   100 Gbps   - Eth1/4    Up          Enabled   100 Gbps   - Eth1/5    Up          Enabled   100 Gbps   - Eth1/6    Down        Enabled   100 Gbps   - Eth1/7    Down        Enabled   100 Gbps   - Eth1/8    Down        Enabled   100 Gbps   - Eth1/9    Down        Enabled   100 Gbps   - Eth1/10   Up          Enabled   100 Gbps   - Eth1/11   Up          Enabled   100 Gbps   - Eth1/12   Up          Enabled   100 Gbps   - Eth1/13   Up          Enabled   100 Gbps   - Eth1/14   Down        Enabled   100 Gbps   - Eth1/15   Up          Enabled   100 Gbps   - Eth1/16   Up          Enabled   100 Gbps   - Eth1/17   Down        Enabled   100 Gbps   - Eth1/18   Down        Enabled   100 Gbps   - ... </pre>				

### Related Commands

<b>Note</b>	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 running the command “show interfaces ethernet” is run. For more information, please refer to Section 5.1.4, “High Power Transceivers,” on page 608.
-------------	---

## show interfaces ethernet

**show interfaces ethernet <inf>**

Displays the configuration and status for the interface.

<b>Syntax Description</b>	inf	Interface number: <slot>/<port>.
<b>Default</b>	N/A	
<b>Configuration Mode</b>	Any Command Mode	
<b>History</b>	3.1.0000 3.6.1002 3.6.2002 3.6.3640 3.6.4110 3.6.5000	Added “error packets” counter to Tx, “Last change in operational status”, and “Isolation group” to output Added “boot delay” parameters to output Added support for “forwarding mode” Updated example output “Forwarding mode” Added telemetry to output
<b>Role</b>	admin	
<b>Example</b>	<pre>switch (config) # show interfaces ethernet 1/14  Eth1/14   Admin state: Enabled   Operational state: Up   Last change in operational status: 4w4d and 22:35:26 ago (1 oper change)   Boot delay time: 60 sec   Boot delay timer status: N/A   Description: N\A   Mac address: f4:52:14:5c:73:f8   MTU: 1500 bytes(Maximum packet size 1522 bytes)   Fec: auto   Flow-control: receive off send off   Actual speed: 100 Gbps   Width reduction mode: disabled   DHCP client: Disabled   IP Address: 8.9.14.9 /24   Broadcast address: 8.9.14.255   Arp timeout: 1500 seconds   VRF: default   MAC learning mode: Enabled   Isolation group: N\A   Forwarding mode: inherited cut-through   Telemetry sampling: Disabled TCs: N\A   Telemetry threshold: Enabled TCs: 3 (ucast), 1 (mcast)   Telemetry threshold level: 900   Last clearing of "show interface" counters: Never   60 seconds ingress rate: 168 bits/sec, 21 bytes/sec, 1 packets/sec   60 seconds egress rate: 160 bits/sec, 20 bytes/sec, 1 packets/sec</pre>	

```
Rx
 559480      packets
 4335      unicast packets
 550812      multicast packets
 4333      broadcast packets
 56941600    bytes
 0          error packets
 0          discard packets

Tx
 557579      packets
 4332      unicast packets
 548912      multicast packets
 4335      broadcast packets
 54615032    bytes
 0          error packets
 0          discard packets
##
Forwarding mode: inherited cut-through
##
```

---

### Related Commands

---

**Note**

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 running the command “show interfaces ethernet” is run. For more information, please refer to Section 5.1.4, “High Power Transceivers,” on page 608.

---

## show interfaces counters

**show interfaces <type> <id> counters [priority <prio>]**

Displays the extended counters for the interface.

<b>Syntax Description</b>	id	Interface number: <slot>/<port>										
	priority	Displays interface extended counters per priority. Range: 0-7 or “all”										
<b>Default</b>	N/A											
<b>Configuration Mode</b>	Any Command Mode											
<b>History</b>	<table><tr><td>3.1.0000</td><td></td></tr><tr><td>3.5.1000</td><td>Added notes</td></tr><tr><td>3.6.1002</td><td>Added “error packets” counter to Tx</td></tr><tr><td>3.6.4006</td><td>Added extended output for storm-control</td></tr><tr><td>3.6.5000</td><td>Added hoq discard packets counter</td></tr></table>		3.1.0000		3.5.1000	Added notes	3.6.1002	Added “error packets” counter to Tx	3.6.4006	Added extended output for storm-control	3.6.5000	Added hoq discard packets counter
3.1.0000												
3.5.1000	Added notes											
3.6.1002	Added “error packets” counter to Tx											
3.6.4006	Added extended output for storm-control											
3.6.5000	Added hoq discard packets counter											
<b>Role</b>	admin											

**Example**

```

switch (config) # show interfaces ethernet 1/1 counters

Rx
0          packets
0          unicast packets
0          multicast packets
0          broadcast packets
0          bytes
0          packets of 64 bytes
0          packets of 65-127 bytes
0          packets of 128-255 bytes
0          packets of 256-511 bytes
0          packets of 512-1023 bytes
0          packets of 1024-1518 bytes
0          packets Jumbo
0          error packets
0          discard packets
0          hog discard packets
0          fcs errors
0          undersize packets
0          oversize packets
0          pause packets
0          unknown control opcode
0          symbol errors
(appears only on L2 ethernet ports and port-channels supported interfaces)
..0          packets
..0          unicast packets
..0          multicast packets
..
0          error packets
0          discard packets
0          discard packets by Storm Control
0          fcs errors
0          undersize packets

Tx
0          packets
0          unicast packets
0          multicast packets
0          broadcast packets
0          bytes
0          error packets
0          discard packets
0          hog discard packets
0          pause packets
0          TX wait
0          TX wait useconds
0          queue depth TCO
0          queue depth TC1
0          queue depth TC2
0          queue depth TC3
0          queue depth TC4
0          queue depth TC5
0          queue depth TC6
0          queue depth TC7

switch (config) #

```

---

### Related Commands

**Note**

- Spectrum™ based systems display queue depth for TC0 - TC7
  - SwitchX® based systems display queue depth for TC0 - TC3 only
-

## show interfaces ethernet description

**show interfaces ethernet [<inf>] description**

Displays the admin status and protocol status for the specified interface.

<b>Syntax Description</b>	inf	Interface number: <slot>/<port>.												
<b>Default</b>	N/A													
<b>Configuration Mode</b>	Any Command Mode													
<b>History</b>	3.1.0000													
	3.4.1100	Updated Example												
<b>Role</b>	admin													
<b>Example</b>	<pre>switch (config) # show interfaces ethernet description</pre> <table><thead><tr><th>Interface</th><th>Admin state</th><th>Operational state</th></tr></thead><tbody><tr><td>Eth1/58</td><td>Enabled</td><td>Down</td></tr><tr><td>Eth1/59</td><td>Enabled</td><td>Up</td></tr><tr><td>Eth1/60</td><td>Enabled</td><td>Down (Suspend)</td></tr></tbody></table> <pre>switch (config) # show interfaces ethernet 1/60 description</pre> <pre>Eth1/60</pre> <pre>    Admin state: Enabled     Operational state: Down (Suspend) switch (config) #</pre>		Interface	Admin state	Operational state	Eth1/58	Enabled	Down	Eth1/59	Enabled	Up	Eth1/60	Enabled	Down (Suspend)
Interface	Admin state	Operational state												
Eth1/58	Enabled	Down												
Eth1/59	Enabled	Up												
Eth1/60	Enabled	Down (Suspend)												
<b>Related Commands</b>														
<b>Note</b>														

## show interfaces ethernet rates

**show interfaces ethernet [<inf>] rates [<transfer-rate-unit>]**

Displays the current transfer rate of the interface.

---

<b>Syntax Description</b>	transfer-rate-unit	<ul style="list-style-type: none"> <li>• KB – displays interface transfer rate in KB/s</li> <li>• MB – displays interface transfer rate in MB/s</li> <li>• GB – displays interface transfer rate in GB/s</li> <li>• If no parameter is entered transfer rate is displayed in readable unit (KB/MB/GB/BS) depending on the range</li> </ul>																														
<b>Default</b>	N/A																															
<b>Configuration Mode</b>	Any Command Mode																															
<b>History</b>	3.6.2002																															
<b>Role</b>	admin																															
<b>Example</b>	<pre>switch (config) # show interfaces ethernet rates KB</pre> <table> <thead> <tr> <th>Port</th> <th colspan="2">egress</th> <th colspan="2">ingress</th> </tr> <tr> <th></th> <th>avg rate (KB/s)</th> <th>pkts/sec</th> <th>avg rate (KB/s)</th> <th>pkts/sec</th> </tr> </thead> <tbody> <tr> <td>Eth1/1</td> <td>0</td> <td>0</td> <td>0.032</td> <td>1</td> </tr> <tr> <td>Eth1/2</td> <td>0</td> <td>0</td> <td>0.032</td> <td>1</td> </tr> <tr> <td>Eth1/3</td> <td>0</td> <td>0</td> <td>0</td> <td>0</td> </tr> <tr> <td>...</td> <td></td> <td></td> <td></td> <td></td> </tr> </tbody> </table> <pre>switch (config) #</pre>		Port	egress		ingress			avg rate (KB/s)	pkts/sec	avg rate (KB/s)	pkts/sec	Eth1/1	0	0	0.032	1	Eth1/2	0	0	0.032	1	Eth1/3	0	0	0	0	...				
Port	egress		ingress																													
	avg rate (KB/s)	pkts/sec	avg rate (KB/s)	pkts/sec																												
Eth1/1	0	0	0.032	1																												
Eth1/2	0	0	0.032	1																												
Eth1/3	0	0	0	0																												
...																																
<b>Related Commands</b>																																
<b>Note</b>																																

---

## show interfaces ethernet status

**show interfaces ethernet [<inf>] status**

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

<b>Syntax Description</b>	inf	Interface number: <slot>/<port>.																
<b>Default</b>	N/A																	
<b>Configuration Mode</b>	Any Command Mode																	
<b>History</b>	3.1.0000																	
	3.4.1100	Updated Example																
<b>Role</b>	admin																	
<b>Example</b>	<pre>switch (config) # show interfaces ethernet status</pre> <table><thead><tr><th>Port</th><th>Operational state</th><th>Speed</th><th>Negotiation</th></tr></thead><tbody><tr><td>Eth1/58</td><td>Down</td><td>40 Gbps</td><td>No-Negotiation</td></tr><tr><td>Eth1/59</td><td>Up</td><td>40 Gbps</td><td>No-Negotiation</td></tr><tr><td>Eth1/60</td><td>Down (Suspend)</td><td>40 Gbps</td><td>No-Negotiation</td></tr></tbody></table> <pre>switch (config) #</pre>		Port	Operational state	Speed	Negotiation	Eth1/58	Down	40 Gbps	No-Negotiation	Eth1/59	Up	40 Gbps	No-Negotiation	Eth1/60	Down (Suspend)	40 Gbps	No-Negotiation
Port	Operational state	Speed	Negotiation															
Eth1/58	Down	40 Gbps	No-Negotiation															
Eth1/59	Up	40 Gbps	No-Negotiation															
Eth1/60	Down (Suspend)	40 Gbps	No-Negotiation															
<b>Related Commands</b>																		
<b>Note</b>																		

## show interfaces ethernet transceiver

**show interfaces ethernet [<inf>] transceiver**

Displays the transceiver info.

<b>Syntax Description</b>	inf	interface number: <slot>/<port>
<b>Default</b>	N/A	
<b>Configuration Mode</b>	Any Command Mode	
<b>History</b>	3.1.0000	
<b>Role</b>	admin	
<b>Example</b>	<pre>switch (config) # show interfaces ethernet 1/1 transceiver Port 1/1 state       identifier          : QSFP+       cable/module type   : Optical cable/module       ethernet speed and type: 40GBASE - SR4       vendor              : Mellanox       cable_length        : 50 m       part number         : MC2210411-SR4       revision            : A1       serial number       : TT1151-00006 switch (config) #</pre>	

### Related Commands

- |             |  |
|-------------|--|
| <b>Note</b> | <ul style="list-style-type: none"><li>For a full list of the supported cables and transceivers, please refer to <a href="http://www.hpe.com/support/hpsc">http://www.hpe.com/support/hpsc</a></li><li>If a high power transceiver (e.g. LR4) is used, it will be indicated in the field “cable/module type”.</li></ul> |
|-------------|--|

## show interfaces ethernet transceiver counters

**show interfaces ethernet [<inf>] transceiver counters**

Displays PHY counters.

<b>Syntax Description</b>	inf	interface number: <slot>/<port>												
<b>Default</b>	N/A													
<b>Configuration Mode</b>	Any Command Mode													
<b>History</b>	3.6.1002													
<b>Role</b>	admin													
<b>Example</b>	<pre>switch (config) # show interfaces ethernet 1/1 transceiver counters</pre> <table><tr><td>Rx</td><td></td><td></td></tr><tr><td>phy received bits</td><td>17725862707200</td><td></td></tr><tr><td>phy symbol errors</td><td>0</td><td></td></tr><tr><td>phy corrected bits</td><td>0</td><td></td></tr></table>		Rx			phy received bits	17725862707200		phy symbol errors	0		phy corrected bits	0	
Rx														
phy received bits	17725862707200													
phy symbol errors	0													
phy corrected bits	0													
<b>Related Commands</b>														
<b>Note</b>	<ul style="list-style-type: none"><li>The counter “phy received bits” provides information on the total amount of traffic received and can be used to estimate the ratio of error traffic</li><li>The counter “phy symbol errors” provides information on the error traffic that was not corrected because the FEC algorithm could not do it or because FEC was not active on this interface</li><li>The counter “phy corrected bits” provides the number of corrected bits by the active FEC mode (RS/FC)</li><li>This command is only supported on Spectrum™ based switch systems</li></ul>													

## show interfaces ethernet transceiver counters details

**show interfaces ethernet [<inf>] transceiver counters**

Displays all PHY counters.

<b>Syntax Description</b>	inf	interface number: <slot>/<port>
<b>Default</b>	N/A	
<b>Configuration Mode</b>	Any Command Mode	
<b>History</b>	3.6.1002	
<b>Role</b>	admin	
<b>Example</b>	<pre>switch (config) # show interfaces ethernet 1/1 transceiver counters details  ----- Phy counters ----- Symbol errors 0 Sync headers errors 0 Edpl/bip errors lane0 0 Edpl/bip errors lane1 0 Edpl/bip errors lane2 0 Edpl/bip errors lane3 0 FC corrected blocks lane0 0 FC corrected blocks lane1 0 FC corrected blocks lane2 0 FC corrected blocks lane3 0 FC uncorrectable blocks lane0 0 FC uncorrectable blocks lane1 0 FC uncorrectable blocks lane2 0 FC uncorrectable blocks lane3 0 RS corrected blocks 0 RS uncorrectable blocks 0 RS no errors blocks 1130552748 RS single error blocks 0 RS corrected symbols total 0 RS corrected symbols lane0 0 RS corrected symbols lane1 0 RS corrected symbols lane2 0 RS corrected symbols lane3 0 Link down events 0 Successful recovery events 0 Time since last clear 176127</pre>	
<b>Related Commands</b>		
<b>Note</b>	The number of lanes displayed depends on interface splitter ratio (4-way-split – each split has only 1 lane; 2-way-split – each split has 2 lanes)	

## show interfaces ethernet transceiver diagnostics

**show interfaces ethernet [<inf>] transceiver diagnostics**

Displays cable channel monitoring and diagnostics info for this interface. Tx and Rx power are reported in mW and dBm units.

<b>Syntax Description</b>	inf	Interface number: <slot>/<port>
<b>Default</b>	N/A	
<b>Configuration Mode</b>	Any Command Mode	
<b>History</b>	3.6.2002	
	3.6.4006	Updated output to report Tx and Rx power in mW and dBm units.
<b>Role</b>	admin	

**Example**

```

switch (config) # show interfaces ethernet 1/35 transceiver diagnostics
Port 1/35 transceiver diagnostic data:
Temperature (-127C to +127C)
    Temperature : 32 C
    Hi Temp Alarm Thresh : 80 C
    Low Temp Alarm Thresh : -10 C
    Temperature Alarm : None

Voltage ( 0 to 6.5535 V)
    Voltage : 3.24250 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 : 0.98970 mW / -0.04496 dBm
    Ch2 Tx Power : 1.12020 mW / 0.49296 dBm
    Ch3 Tx Power : 1.13240 mW / 0.54000 dBm
    Ch4 Tx Power : 1.07200 mW / 0.30195 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 : 1.14760 mW / 0.59791 dBm
    Ch2 Rx Power : 0.99280 mW / -0.03138 dBm
    Ch3 Rx Power : 1.01120 mW / 0.04837 dBm
    Ch4 Rx Power : 1.09500 mW / 0.39414 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) : 15-05-2016

```

**Related Commands**
**Note**

This example is for a QSFP transceiver

## **show interfaces ethernet transceiver raw**

## **show interfaces ethernet [<inf>] transceiver raw**

Displays cable info for this interface.

### **Related Commands**

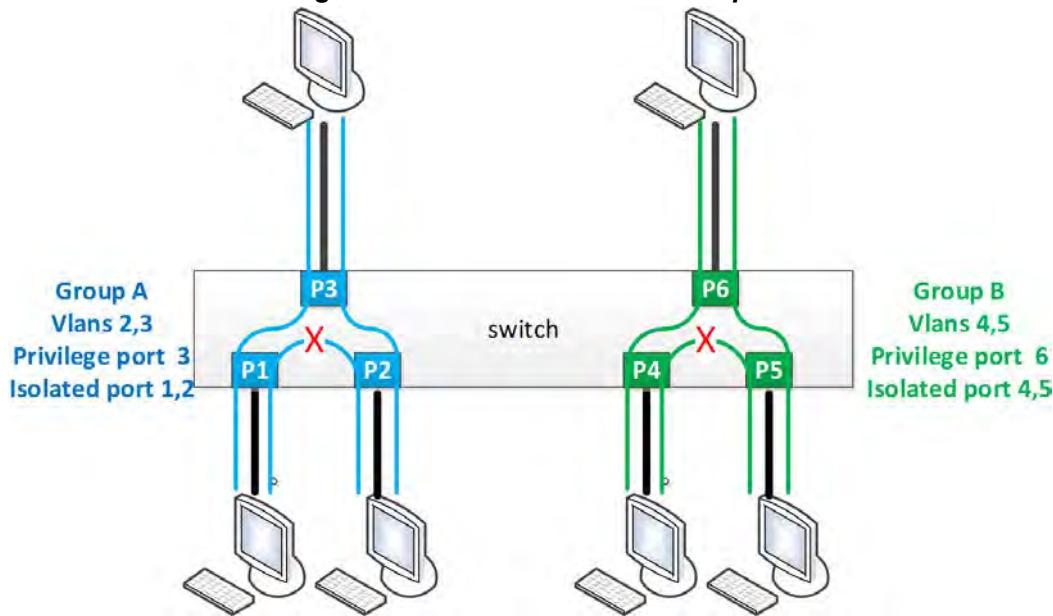
## Note

## 5.2 Interface Isolation

Interface isolation provides the ability to group interfaces in sets where traffic from each port is isolated from other interfaces in the group. The isolated interfaces in the group, however, are able to communicate with the interface marked as privileged.

### 5.2.1 Configuring Isolated Interfaces

*Figure 18: Interface Isolation Example*



➤ *To configure isolated interfaces:*

**Step 1.** Create the VLANs to be used. Run:

```
switch (config) # vlan 2-5
(config vlan 2-5) # exit
```

**Step 2.** Unlock isolation interface protocol. Run:

```
switch (config) # protocol isolation-group
```

**Step 3.** Create isolation Group A. Run:

```
switch (config) # isolation-group GroupA
```

**Step 4.** Assign VLANs 2 and 3 to isolation Group A. Run:

```
(config isolation-group GroupA) # vlan 2-3
(config isolation-group GroupA) # exit
```

**Step 5.** Create isolation Group B. Run:

```
switch (config) # isolation-group GroupB
```

**Step 6.** Assign VLANs 4 and 5 to isolation Group B. Run:

```
(config isolation-group GroupB) # vlan 4-5
(config isolation-group GroupB) # exit
```

**Step 7.** Set Ethernet interfaces 1-3 to access for VLAN 3. Run:

```
(config) # interface ethernet 1/1 switchport access vlan 3  
(config) # interface ethernet 1/2 switchport access vlan 3  
(config) # interface ethernet 1/3 switchport access vlan 3
```

**Step 8.** Isolate Ethernet interfaces 1 and 2 and set Ethernet interfaces 3 as privileged. Run:

```
(config) # interface ethernet 1/1-1/2 isolation-group GroupA mode isolated  
(config) # interface ethernet 1/3 isolation-group GroupA mode privileged
```

**Step 9.** Enable isolation Group A. Run:

```
(config) # isolation-group GroupA no shutdown
```

**Step 10.** Set Ethernet interfaces 4-6 to trunk. Run:

```
(config) # interface ethernet 1/4 switchport mode trunk  
(config) # interface ethernet 1/5 switchport mode trunk  
(config) # interface ethernet 1/6 switchport mode trunk
```

**Step 11.** Isolate Ethernet interfaces 4 and 5 and set Ethernet interfaces 6 as privileged. Run:

```
(config) # interface ethernet 1/4-1/5 isolation-group GroupA mode isolated  
(config) # interface ethernet 1/6 isolation-group GroupA mode privileged
```

**Step 12.** Enable isolation Group B. Run:

```
(config) # isolation-group GroupB no shutdown
```

**Step 13.** Verify configuration. Run:

```
(config) # show isolation-group  
Isolation group: GroupA  
State: Enabled  
VLANs: 2, 3  
Privileged port: Eth1/3  
Isolated ports: Eth1/1, Eth1/2  
  
Isolation group: GroupB  
State: Enabled  
VLANs: 4, 5  
Privileged port: Eth1/6  
Isolated ports: Eth1/4, Eth1/5
```

## 5.2.2 Commands

### protocol isolation-group

**protocol isolation-group**  
**no protocol isolation-group**

Enables interface isolation and unlocks further isolation-group commands.  
The no form of the command disables interface isolation and locks other isolation-group commands.

<b>Syntax Description</b>	N/A
<b>Default</b>	Disabled
<b>Configuration Mode</b>	Config
<b>History</b>	3.6.1002
<b>Role</b>	admin
<b>Example</b>	<pre>switch (config) # protocol isolation-group</pre>
<b>Related Commands</b>	
<b>Note</b>	<ul style="list-style-type: none"><li>• MLAG must be disabled before enabling interface isolation</li><li>• When disabled, all configuration is lost</li></ul>

## isolation-group

```
isolation-group <name>
no isolation-group <name>
```

Creates isolation group.

The no form of the command deletes isolation group.

<b>Syntax Description</b>	N/A
<b>Default</b>	N/A
<b>Configuration Mode</b>	Config
<b>History</b>	3.6.1002
<b>Role</b>	admin
<b>Example</b>	switch (config) # isolation-group mygroup
<b>Related Commands</b>	protocol isolation-group
<b>Note</b>	<ul style="list-style-type: none"><li>The no form of this command deletes the isolation group, removes its attached ports, and the VLANs from the group</li><li>Up to 64 isolation groups can be created</li></ul>

## shutdown

**shutdown**  
**no shutdown**

Enables isolation group.

The no form of the command disables isolation group.

<b>Syntax Description</b>	N/A
<b>Default</b>	Disabled
<b>Configuration Mode</b>	Config Isolation Group
<b>History</b>	3.6.1002
<b>Role</b>	admin
<b>Example</b>	<pre>switch (config isolation-group mygroup) # no shutdown</pre>
<b>Related Commands</b>	<code>protocol isolation-group</code> <code>isolation-group</code>
<b>Note</b>	Enabling isolation groups fails if there are VLANs with ports both inside and outside the group.

## vlan

```
vlan <vid>
no vlan <vid>
```

Adds a VLAN to isolation group.

The no form of the command removes a VLAN from an isolation group.

<b>Syntax Description</b>	N/A
<b>Default</b>	N/A
<b>Configuration Mode</b>	Config Isolation Group
<b>History</b>	3.6.1002
<b>Role</b>	admin
<b>Example</b>	<pre>switch (config isolation-group mygroup) # vlan 10</pre>
<b>Related Commands</b>	<pre>protocol isolation-group isolation-group</pre>
<b>Note</b>	<ul style="list-style-type: none"><li>Enabling isolation groups fails if there are VLANs with ports both inside and outside the group</li><li>The VLAN must be created before running this command</li><li>All interfaces in the VLAN must be attached to only this isolation group</li><li>The VLAN added cannot have a respective VLAN interface</li></ul>

## isolation-group mode

```
isolation-group <name> mode {isolated | privileged}
no isolation-group <name> mode {isolated | privileged}
```

Adds a VLAN to isolation group.

The no form of the command removes a VLAN from an isolation group.

<b>Syntax Description</b>	<table> <tr> <td>name</td><td>The isolation group name</td></tr> <tr> <td>isolated</td><td>Configures this interface as isolated</td></tr> <tr> <td>privileged</td><td>Configures this interface as privileged</td></tr> </table>	name	The isolation group name	isolated	Configures this interface as isolated	privileged	Configures this interface as privileged
name	The isolation group name						
isolated	Configures this interface as isolated						
privileged	Configures this interface as privileged						
<b>Default</b>	N/A						
<b>Configuration Mode</b>	Config Interface Ethernet Config Interface Port Channel						
<b>History</b>	3.6.1002						
<b>Role</b>	admin						
<b>Example</b>	<pre>switch (config interface ethernet 1/2) # isolation-group mygroup mode privileged</pre>						
<b>Related Commands</b>							
<b>Note</b>	<ul style="list-style-type: none"> <li>Enabling isolation groups fails if there are VLANs with ports both inside and outside the group</li> <li>The VLAN must be created before running this command</li> <li>All interfaces in the VLAN must be attached to only this isolation group</li> <li>The VLAN added cannot have a respective VLAN interface</li> </ul>						

## show isolation-group

**show isolation-group <name>**

Displays isolation group information.

<b>Syntax Description</b>	N/A
<b>Default</b>	N/A
<b>Configuration Mode</b>	Any Command Mode
<b>History</b>	3.6.1002
	3.6.5000 Updated Example
<b>Role</b>	admin
<b>Example</b>	<pre>switch (config) # show isolation-group mygroup Isolation group 1:     State:          Disabled     VLANs:         N/A     Privileged port: N/A     Isolated ports: N/A</pre>
<b>Related Commands</b>	
<b>Note</b>	

## 5.3 Link Aggregation Group (LAG)

Link Aggregation protocol describes a network operation in which several same speed links are combined into a single logical entity with the accumulated bandwidth of the originating ports. LAG groups exchange Lag Aggregation Control Protocol (LACP) packets in order to align the functionality between both endpoints of the LAG. To equally send traffic on all LAG links, the switch uses a hash function which can use a set of attributes as key to the hash function.

As many as 16 physical ports can be aggregated on a single LAG.

### 5.3.1 Configuring Static Link Aggregation Group (LAG)

➤ *To configure a static LAG:*

**Step 1.** Log in as admin.

**Step 2.** Enter config mode. Run:

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

**Step 3.** Create a port-channel entity. Run:

```
switch (config) # interface port-channel 1  
switch (config interface port-channel 1) #
```

**Step 4.** Change back to config mode.

```
switch (config interface port-channel 1) # exit  
switch (config) #
```

**Step 5.** Add a physical port to the port-channel. Run:

```
switch (config interface ethernet 1/4) # channel-group 1 mode on  
switch (config interface ethernet 1/4) #
```



If the physical port is operationally up, this port becomes an active member of the aggregation. Consequently, it becomes able to convey traffic.

### 5.3.2 Configuring Link Aggregation Control Protocol (LACP)

➤ *To configure LACP:*

**Step 1.** Log in as admin.

**Step 2.** Enter config mode. Run:

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

**Step 3.** Create a port-channel entity. Run:

```
switch (config) # interface port-channel 1  
switch (config interface port-channel 1) #
```

**Step 4.** Change back to config mode. Run:

```
switch (config interface port-channel 1) # exit  
switch (config) #
```

**Step 5.** Enable LACP in the switch. Run:

```
switch (config) # lACP  
switch (config) #
```

**Step 6.** Add a physical port to the port-channel. Run:

```
switch (config interface ethernet 1/4) # channel-group 1 mode active/passive  
switch (config interface ethernet 1/4) #
```

### 5.3.3 Commands

#### interface port-channel

```
interface port-channel <1-4096>[-<2-4096>]
no interface port-channel <1-4096>[-<2-4096>]
```

Creates a LAG and enters the LAG configuration mode. There is an option to create a range of LAG interfaces.

The no form of the command deletes the LAG, or range of LAGs.

<b>Syntax Description</b>	1-4096 / 2-4096	LAG number
<b>Default</b>	N/A	
<b>Configuration Mode</b>	Config	
<b>History</b>	3.1.1400	
	3.2.1100	Added range support
	3.4.0000	Added note
	3.6.3640	Added note
<b>Role</b>	admin	
<b>Example</b>	<pre>switch (config)# interface port-channel 1 switch (config interface port-channel 1) # exit switch (config)# interface port-channel 1-10 switch (config interface port-channel 1-10) #</pre>	
<b>Related Commands</b>		
<b>Note</b>	<ul style="list-style-type: none"> <li>If a LAG is also an IPL, attempting to delete it without first deleting the IPL is rejected by the management.</li> <li>LAG have forwarding mode in accordance with the global configuration</li> </ul>	

## lacp

**lacp**  
**no lacp**

Enables LACP in the switch.

The no form of the command disables LACP in the switch.

---

**Syntax Description** N/A

---

**Default** LACP is disabled.

**Configuration Mode** Config

**History** 3.1.1400

**Role** admin

**Example**  
switch (config)# lacp  
switch (config)#

---

**Related Commands**

---

**Note**

---

## lacp system-priority

**lacp system-priority <1-65535>**  
**no lacp system-priority**

Configures the LACP system priority.  
The no form of the command sets the LACP system-priority to default.

<b>Syntax Description</b>	1-65535	LACP system-priority.		
<b>Default</b>	32768			
<b>Configuration Mode</b>	Config			
<b>History</b>	3.1.1400			
<b>Role</b>	admin			
<b>Example</b>	<pre>switch (config)# lacp system-priority 1 switch (config)# show lacp interfaces port-channel Port-channel Module Admin Status is enabled Port-channel System Identifier is 00:02:c9:5c:61:70 LACP System Priority: 3 switch (config)#+</pre>			
<b>Related Commands</b>				
<b>Note</b>				

## lacp (interface)

```
lacp {rate fast | port-priority <1-65535>}
no lacp {rate fast | port-priority}
```

Configures the LACP interface parameters.

The no form of the command sets the LACP interface configuration to default.

<b>Syntax Description</b>	rate fast	Sets LACP PDUs on the port to be in fast (1 second) or slow rate. (30 seconds).												
	1-65535	LACP port-priority.												
<b>Default</b>	rate - slow (30 seconds) port-priority 32768													
<b>Configuration Mode</b>	Config													
<b>History</b>	3.1.1400													
<b>Role</b>	admin													
<b>Example</b>	<pre>switch (config interface ethernet 1/7)# lacp rate fast switch (config interface ethernet 1/7)# show lACP interfaces ethernet 1/7 Port : 1/7 ----- Port State = Down Channel Group : 1 Pseudo port-channel = Po1 LACP port-priority = 32768 LACP Rate = Slow LACP Activity : Passive LACP Timeout : Short  Aggregation State : Aggregation, Defaulted,</pre> <table border="1"> <thead> <tr> <th>Port</th> <th>LACP State</th> <th>Port Admin Priority</th> <th>Oper Key</th> <th>Port Number</th> <th>Port State</th> </tr> </thead> <tbody> <tr> <td>1/7</td> <td>Down</td> <td>128</td> <td>1</td> <td>1</td> <td>0x7</td> </tr> </tbody> </table> <pre>switch (config)# </pre>		Port	LACP State	Port Admin Priority	Oper Key	Port Number	Port State	1/7	Down	128	1	1	0x7
Port	LACP State	Port Admin Priority	Oper Key	Port Number	Port State									
1/7	Down	128	1	1	0x7									

### Related Commands

<b>Note</b>	Configuring LACP rate (fast or slow) will configure the peer port to send (fast or slow), it does not make any affect on the local port LACP rate.
-------------	--

## port-channel load-balance ethernet

```
port-channel load-balance ethernet <method>
no port-channel load-balance ethernet <method>
```

Configures the port-channel load balancing distribution function method.  
The no form of the command sets the distribution function method to default.

<b>Syntax Description</b>	method	Possible load balance methods: <ul style="list-style-type: none"><li>• destination-ip</li><li>• destination-mac</li><li>• destination-port</li><li>• source-destination-ip</li><li>• source-destination-mac</li><li>• source-destination-port</li><li>• source-ip</li><li>• source-mac</li><li>• source-port</li></ul>
<b>Default</b>	source-destination-mac	
<b>Configuration Mode</b>	Config	
<b>History</b>	3.1.1400	
<b>Role</b>	admin	
<b>Example</b>	switch (config)# port-channel load-balance ethernet destination-ip source-port source-mac	
<b>Related Commands</b>		
<b>Note</b>	Several load balance methods can be configured (refer to the example)	

## channel-group

**channel-group <1-4096> [mode {on | active | passive}]  
no channel-group**

Assigns and configures a physical interface to a port channel.

The no form of the command removes a physical interface from the port-channel.

<b>Syntax Description</b>	1-4096	The port channel number.
	mode on	Static assignment the port to LAG. LACP will not be enabled on this port.
	mode active/passive	Dynamic assignment of the port to LAG. LACP will be enabled in either passive or active mode.
<b>Default</b>	N/A	
<b>Configuration Mode</b>	Config Interface Ethernet	
<b>History</b>	3.1.1400 3.4.0008                  Added a note 3.6.3640                  Added a note 3.6.4006                  Added a note	
<b>Role</b>	admin	
<b>Example</b>	<pre>switch (config interface ethernet 1/7)# channel-group 1 mode active</pre>	
<b>Related Commands</b>	<a href="#">show interfaces port-channel summary</a> <a href="#">show interfaces port-channel compatibility-parameters</a> <a href="#">show lacp interfaces ethernet</a>	
<b>Note</b>	<ul style="list-style-type: none"> <li>Setting the mode to active/passive is possible only in LACP is enabled.</li> <li>The first port in the LAG decide if the LAG will be static (“on”) or LACP (“active”, “passive”).</li> <li>All the ports in the LAG must have the same configuration, determines by the first port added to the LAG. The port with a different configuration will be rejected, for the list of dependencies refer to ‘show interfaces port-channel compatibility-parameters’</li> <li>A physical port may only be part of one channel-group</li> <li>Added support to check if the forwarding mode of the interface is the same as the forwarding mode of LAG. Error output:  <code>% Channel-group and Ethernet port have different port forwarding mode configuration</code> </li> <li>Port can't be added to port-channel when storm-control is configured on port. Error output:  <code>% Interface * has storm control configuration and can't be added to LAG</code> </li> </ul>	

## lacp-individual enable

**lacp-individual enable [force]**  
**no lacp-individual enable [force]**

Configures the LAG to act with LACP-individual capabilities.  
The no form of the command disables the LACP-individual capability.

<b>Syntax Description</b>	force	Toggles the interface after enabling LACP-individual.
<b>Default</b>	N/A	
<b>Configuration Mode</b>	Config Interface Port Channel	
<b>History</b>	3.4.1100	
<b>Role</b>	admin	
<b>Example</b>	switch (config interface port-channel 10)# lacp-individual enable force	
<b>Related Commands</b>		
<b>Note</b>	If a switch is connected via LAG to a host without LACP capability, running this command on that LAG allows a member port (with the lowest numerical priority value), acting as an individual, to communicate with the host.	

## ip address dhcp

**ip address dhcp**  
**no ip address dhcp**

Enables DHCP on this LAG interface.

<b>Syntax Description</b>	N/A
<b>Default</b>	Disabled
<b>Configuration Mode</b>	Config Interface Port Channel set as router interface
<b>History</b>	3.4.2008
<b>Role</b>	admin
<b>Example</b>	<pre>switch (config interface port channel 10) # ip address dhcp switch (config interface port channel 10) #</pre>
<b>Related Commands</b>	<a href="#">interface port-channel</a> <a href="#">show interface port-channel</a>
<b>Note</b>	

## show lacp counters

### show lacp counters

Displays the LACP PDUs counters.

**Syntax Description** N/A

**Default** N/A

**Configuration Mode** Any Command Mode

**History** 3.1.1400

**Role** admin

**Example**

```
switch (config)# show lacp counters
LACPDU          Marker          Marker Response      LACPDU
Port           Sent Recv       Sent Recv           Sent Recv  Illegal   Unknown
-----          -----
Port-channel: 1
-----
1/7            0    0           0    0           0    0    0
```

switch (config) # switch (config)#

**Related Commands**

**Note**

## show lacp interfaces ethernet

**show lacp interface ethernet <inf>**

Displays the LACP interface configuration and status.

<b>Syntax Description</b>	inf	Interface number, for example “1/1”.														
<b>Default</b>	N/A															
<b>Configuration Mode</b>	Any Command Mode															
<b>History</b>	3.1.1400															
<b>Role</b>	admin															
<b>Example</b>	<pre>switch (config) # show lacp interfaces ethernet 1/4 Port : 1/4 ----- Port State = Down Channel Group : 1 Pseudo port-channel = Po1 LACP port-priority = 128 LACP Rate = Slow LACP Activity : Passive LACP Timeout : Short  Aggregation State : Aggregation, Defaulted,</pre> <table border="1"> <thead> <tr> <th>Port</th> <th>State</th> <th>LACP Priority</th> <th>Port Admin Key</th> <th>Oper Key</th> <th>Port Number</th> <th>Port State</th> </tr> </thead> <tbody> <tr> <td>1/4</td> <td>Down</td> <td>128</td> <td>1</td> <td>1</td> <td>0x4</td> <td>0x0</td> </tr> </tbody> </table>		Port	State	LACP Priority	Port Admin Key	Oper Key	Port Number	Port State	1/4	Down	128	1	1	0x4	0x0
Port	State	LACP Priority	Port Admin Key	Oper Key	Port Number	Port State										
1/4	Down	128	1	1	0x4	0x0										

### Related Commands

### Note

## show lacp interfaces neighbor

### show lacp interfaces neighbor

Displays the LACP interface neighbor status.

<b>Syntax Description</b>	N/A	
<b>Default</b>	N/A	
<b>Configuration Mode</b>	Any Command Mode	
<b>History</b>	3.1.1400	
	3.4.0000	Updated output
<b>Role</b>	admin	

---

**Example**

```
switch (config) # show lacp interfaces neighbor
Flags:
A - Device is in Active mode
P - Device is in Passive mode

Channel group 1 neighbors

Port 1/4
-----
Partner System ID      : 00:00:00:00:00:00
Flags                  : A
LACP Partner Port Priority : 0
LACP Partner Oper Key   : 0
LACP Partner Port State : 0x0

Port State Flags Decode
-----
Activity : Active
Aggregation State : Aggregation, Sync, Collecting, Distributing

MLAG channel group 25 neighbors

Port 1/49
-----
Partner System ID      : 00:02:c9:fa:c4:c0
Flags                  : A
LACP Partner Port Priority : 255
LACP Partner Oper Key   : 33
LACP Partner Port State : 0xbc

Port State Flags Decode
-----
Activity : Active
Aggregation State : Aggregation, Sync, Collecting, Distributing

MLAG channel group 28 neighbors

Port 1/51
-----
Partner System ID      : f4:52:14:10:d8:f1
Flags                  : A
LACP Partner Port Priority : 255
LACP Partner Oper Key   : 33
LACP Partner Port State : 0xbc

Port State Flags Decode
-----
Activity : Active
Aggregation State : Aggregation, Sync, Collecting, Distributing

switch (config) #
```

---

**Related Commands**

---

**Note**

## show lacp

### show lacp

Displays the LACP global parameters.

<b>Syntax Description</b>	N/A
<b>Default</b>	N/A
<b>Configuration Mode</b>	Any Command Mode
<b>History</b>	3.4.0000
<b>Role</b>	admin
<b>Example</b>	<pre>switch (config) # show lacp Port-channel Module Admin Status is enabled switch (config) #</pre>
<b>Related Commands</b>	
<b>Note</b>	

## show lacp interfaces system-identifier

**show lacp interfaces {mlag-port-channel | port-channel} <instance> system-identifier**

Displays the system identifier of LACP.

<b>Syntax Description</b>	instance	LAG or MLAG instance.
<b>Default</b>	N/A	
<b>Configuration Mode</b>	Any Command Mode	
<b>History</b>	3.4.0000	
<b>Role</b>	admin	
<b>Example</b>	<pre>switch (config)# show lacp interfaces port-channel 2 system-identifier Priority: 12345 MAC: 00:02:C9:AC:2A:60 switch (config)#+</pre>	
<b>Related Commands</b>		
<b>Note</b>		

## show interfaces port-channel

**show interfaces port-channel <port-channel>**

Displays LAG configuration properties.

<b>Syntax Description</b>	port-channel	LAG interface whose properties to display
<b>Default</b>	N/A	
<b>Configuration Mode</b>	Any Command Mode	
<b>History</b>	3.3.4000	
	3.4.1100	Updated Example
	3.6.1002	Added “error packets” counter to Tx
	3.6.5000	Added telemetry to output
<b>Role</b>	admin	

**Example**

```
switch (config) # show interfaces port-channel 2

Po2
Admin state: Enabled
Operational state: Up
Description: N\A
Mac address: 00:00:00:00:00:00
MTU: 9216 bytes (Maximum packet size 9238 bytes)
lacp-individual mode: Enabled
Flow-control: receive off send off
Actual speed: 2 X 40 Gbps
Width reduction mode: disabled
Switchport mode: trunk
MAC learning mode: Enabled
Last clearing of "show interface" counters : Never
Telemetry sampling: Disabled TCs: N\A
Telemetry threshold:Enabled TCs: 3 (ucast), 1 (mcast)
Telemetry threshold level: 900
60 seconds ingress rate: 2440 bits/sec, 305 bytes/sec, 5 packets/sec
60 seconds egress rate: 2440 bits/sec, 305 bytes/sec, 5 packets/sec
```

Rx	
24060	packets
23447	unicast packets
598	multicast packets
15	broadcast packets
1796876	bytes
0	error packets
0	discard packets
Tx	
23961	packets
23454	unicast packets
496	multicast packets
11	broadcast packets
1805778	bytes
0	error packets
4	discard packets

---

**Related Commands**

---

**Note**

---

## show interfaces port-channel counters

**show interfaces port-channel <port-channel> counters**

Displays the extended counters for the interface.

<b>Syntax Description</b>	port-channel	LAG interface whose properties to display
<b>Default</b>	N/A	
<b>Configuration Mode</b>	Any Command Mode	
<b>History</b>	3.6.1002	
<b>Role</b>	admin	
<b>Example</b>	<pre>switch (config) # show interfaces port-channel 3 counters  Rx   0          packets   0          unicast packets   0          multicast packets   0          broadcast packets   0          bytes   0          packets of 64 bytes   0          packets of 65-127 bytes   0          packets of 128-255 bytes   0          packets of 256-511 bytes   0          packets of 512-1023 bytes   0          packets of 1024-1518 bytes   0          packets Jumbo   0          error packets   0          discard packets   0          fcs errors   0          undersize packets   0          oversize packets   0          pause packets   0          unknown control opcode   0          symbol errors  Tx   1000000  packets   0          unicast packets   1000000  multicast packets   0          broadcast packets   1505000000 bytes   1000000  error packets   0          discard packets   0          pause packets  switch (config) #</pre>	

---

### Related Commands

---

### Note

## show interfaces port-channel compatibility-parameters

**show interfaces port-channel compatibility-parameters**

Displays port-channel parameters.

<b>Syntax Description</b>	N/A
<b>Default</b>	N/A
<b>Configuration Mode</b>	Any Command Mode
<b>History</b>	3.3.4000 3.6.3640      Added “forwarding mode” as compatibility parameter to output.
<b>Role</b>	admin
<b>Example</b>	<pre>switch (config) # show interfaces port-channel compatibility-parameters * Port-mode * Speed * MTU * Flow Control * Access VLAN * Allowed VLAN list * Flowcontrol &amp; PFC * Channel-group mode * CoS parameters * MAC learning disable * Forwarding mode  Static configuration on the port should be removed: * ACL port binding * Static mrouter * sflow * OpenFlow * port mirroring local analyzer port * Static mac address switch (config) #</pre>
<b>Related Commands</b>	
<b>Note</b>	

## show interfaces port-channel load-balance

**show interfaces port-channel load-balance**

Displays the type of load-balancing in use for port-channels.

<b>Syntax Description</b>	N/A	N/A
<b>Default</b>	N/A	
<b>Configuration Mode</b>	Any Command Mode	
<b>History</b>	3.3.4000	
<b>Role</b>	admin	
<b>Example</b>	<pre>switch (config) # show interfaces port-channel load-balance source-destination-mac switch (config) #</pre>	
<b>Related Commands</b>		
<b>Note</b>		

## show interfaces port-channel summary

### show interfaces port-channel summary

Displays a summary for the port-channel interfaces.

<b>Syntax Description</b>	N/A	
<b>Default</b>	N/A	
<b>Configuration Mode</b>	Any Command Mode	
<b>History</b>	3.1.1400	
	3.4.1100	Updated Example
<b>Role</b>	admin	
<b>Example</b>	<pre>switch (config) # show interfaces port-channel summary Flags: D - Down, U - Up, P - Up in port-channel (members)       S - Suspend in port-channel (members), I - Individual  ----- Group Port-      Type      Member Ports Channel ----- 1 Po2(U)        LACP      Eth1/58(D) Eth1/59(I) Eth1/60(S) 2 Po5(D)        LACP      Eth1/1(S)  Eth1/33(I) 3 Po10(U)       LACP      Eth1/49(P) Eth1/50(P) Eth1/51(S) Eth1/52(S) switch (config) #</pre>	
<b>Related Commands</b>		
<b>Note</b>		

## 5.4 Link Layer Discovery Protocol (LLDP)

The Link Layer Discovery Protocol (LLDP) is a vendor-neutral Link Layer protocol in the Internet Protocol Suite used by network devices for advertising their identity, capabilities, and neighbors on a IEEE 802 LAN. The protocol is formally defined in IEEE 802.1AB.

### 5.4.1 Configuring LLDP

➤ *To configure the LLDP on the switch:*

**Step 1.** Log in as admin.

**Step 2.** Enter config mode. Run:

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

**Step 3.** Enable LLDP globally on the switch. Run:

```
switch (config) # lldp
switch (config) #
```

**Step 4.** Enable LLDP per interface. Run:

```
switch (config interface ethernet 1/1) # lldp receive
switch (config interface ethernet 1/1) # lldp transmit
```

**Step 5.** Display LLDP local information. Run:

```
switch (config) # show lldp local

LLDP is Enabled

Local global configuration
Chassis sub type: macAddress (4)
Chassis id: 00:11:22:33:44:55
System Name: "switch-111111"
System Description: my-system-description
Supported capabilities: B
Supported capabilities enabled: B
```

**Step 6.** Display LLDP remote information. Run:

```
switch (config)# show lldp interfaces ethernet 1/1 remote

Ethernet 1/1
Remote Index: 1
Remote chassis id: 00:11:22:33:44:55 ; chassis id subtype: mac
Remote port-id: ethenret 1/2; port id subtype: local
Remote port description: ethernet 1/2
Remote system name: remote-system
Remote system description: remote-system-description
Remote system capabilities supported: B ; B
```

## 5.4.2 DCBX

Data Center Bridging (DCB) is an enabler for running the Ethernet network with lossless connectivity using priority-based flow control and enhanced transmission selection. DCBX (exchange) complements the DCB implementation by offering a dynamic protocol that communicates DCB attributes between peering endpoint.

MLNX-OS supports two versions of DCBX TLVs running on top of LLDP:

- DCBX IEEE
- DCBX CEE

By default DCBX IEEE is enabled when LLDP is enabled (LLDP, however, is not enabled by default).

For more information, please refer to the Mellanox Community at:

<https://community.mellanox.com/docs/DOC-2485>.

## 5.4.3 Commands

### lldp

**lldp**  
**no lldp**

Enables LLDP globally.  
The no form of the command disables the LLDP.

<b>Syntax Description</b>	N/A
<b>Default</b>	Disabled
<b>Configuration Mode</b>	Config
<b>History</b>	3.2.0300
<b>Role</b>	admin
<b>Example</b>	<pre>switch (config)# lldp switch (config)#{/pre&gt;</pre>
<b>Related Commands</b>	show lldp local
<b>Note</b>	

## lldp reinit

**lldp reinit <seconds>**  
**no lldp reinit**

Sets the delay in seconds from enabling the LLDP on the port until re-initialization will be attempted.

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

<b>Syntax Description</b>	seconds	1-10
<b>Default</b>	2	
<b>Configuration Mode</b>	Config	
<b>History</b>	3.2.0300	
<b>Role</b>	admin	
<b>Example</b>	switch (config)# lldp reinit 10 switch (config)#	
<b>Related Commands</b>	show lldp timers	
<b>Note</b>		

## lldp timer

**lldp timer <seconds>**  
**no lldp timer**

Sets the LLDP interval at which LLDP frames are transmitted. (lldpMessageTxInterval)

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

<b>Syntax Description</b>	seconds	5-32768
<b>Default</b>	30	
<b>Configuration Mode</b>	Config	
<b>History</b>	3.2.0300	
<b>Role</b>	admin	
<b>Example</b>	switch (config)# lldp timer 10 switch (config)#	
<b>Related Commands</b>	show lldp timers	
<b>Note</b>		

## lldp tx-delay

**lldp tx-delay <seconds>**  
**no lldp tx-delay**

Indicates the delay in seconds between successive LLDP frame transmissions  
The no form of the command sets the parameter to default.

Syntax Description	seconds	1-8192
<b>Default</b>	2	
<b>Configuration Mode</b>	Config	
<b>History</b>	3.2.0300	
<b>Role</b>	admin	
<b>Example</b>	switch (config)# lldp tx-delay 10 switch (config)#	
<b>Related Commands</b>	show lldp timers	
<b>Note</b>	The recommended value for the tx-delay is set by the following formula: $1 \leq \text{lldp tx-delay} \leq (0.25 * \text{lldp timer})$	

## lldp tx-hold-multiplier

```
lldp tx-hold-multiplier <seconds>
no lldp tx-hold-multiplier
```

The time-to-live value expressed as a multiple of the lldpMessageTxInterval object.  
The no form of the command sets the parameter to default.

Syntax Description	seconds	1-8192
<b>Default</b>	2	
<b>Configuration Mode</b>	Config	
<b>History</b>	3.2.0300	
<b>Role</b>	admin	
<b>Example</b>	switch (config)# lldp tx-hold-multiplier 10 switch (config)#	
<b>Related Commands</b>	show lldp timers	
<b>Note</b>	The actual time-to-live value used in LLDP frames, can be expressed by the following formula: TTL = min(65535, (lldpMessageTxInterval * lldpMessageTxHoldMultiplier)) For example, if the value of lldpMessageTxInterval is '30', and the value of lldpMessageTxHoldMultiplier is '4', then the value '120' is encoded in the TTL field in the LLDP header.	

## lldp (interface)

**lldp {receive | transmit}**  
**no lldp {receive | transmit}**

Enables LLDP receive or transmit capabilities.

The no form of the command disables LLDP receive or transmit capabilities.

Syntax Description	med-tlv-select	Enables LLDP media TLVs
	receive	Enables LLDP receive on this port
	tlv-select	Enables LLDP TLVs
	transmit	Enables LLDP transmit on this port
<b>Default</b>	Enabled for receive and trasmit.	
<b>Configuration Mode</b>	Config Interface Ethernet	
<b>History</b>	3.2.0300	
<b>Role</b>	admin	
<b>Example</b>	<pre>switch (config interface ethernet 1/1)# lldp receive switch (config interface ethernet 1/1)#{</pre>	
<b>Related Commands</b>	show lldp interface	
<b>Note</b>	The LLDP is disabled by default (globally)	

## lldp tlv-select

**lldp tlv-select {[dcbx] [dcbx-cee] [port-description] [sys-name] [sys-description] [sys-capabilities] [management-address] [none] all}**

Sets the LLDP basic TLVs to be transmitted on this port.

<b>Syntax Description</b>	dcbx	Enables LLDP-DCBX TLVs
	dcbx-cee	Enables LLDP-DCBX CEE TLVs
	port-description	LLDP port description TLV
	sys-name	LLDP system name TLV
	sys-description	LLDP system description TLV
	sys-capabilities	LLDP system capabilities TLV
	management-address	LLDP management address TLV
	all	all above TLVs
	none	None of the above TLVs
<b>Default</b>	all	
<b>Configuration Mode</b>	Config Interface Ethernet	
<b>History</b>	3.2.0300	
	3.3.0000	Added “none” parameter
	3.3.4302	Added “dcbx” parameter
	3.3.4402	Added “dcbx-cee” parameter
<b>Role</b>	admin	
<b>Example</b>	<pre>switch (config interface ethernet 1/1)# lldp tlv-select port-description sys-name switch (config interface ethernet 1/1)# </pre>	
<b>Related Commands</b>	show lldp interface	
<b>Note</b>		

## lldp med-tlv-select

**lldp med-tlv-select {all | media-capability | network-policy | none}**

Configures LLDP media TLV attributes.

<b>Syntax Description</b>	all media-capabilities network-policy none	Enables all LLDP media TLVs Enables Media Capabilities TLV Enables Network-Policy TLV Disables all LLDP media TLVs
<b>Default</b>	Disabled	
<b>Configuration Mode</b>	Config Interface Ethernet	
<b>History</b>	3.6.1002	
<b>Role</b>	admin	
<b>Example</b>	<pre>switch (config interface ethernet 1/1)# lldp med-tlv-select all switch (config interface ethernet 1/1)#{</pre>	
<b>Related Commands</b>	show lldp interface	
<b>Note</b>		

## dcb application-priority

**dcb application-priority <selector> <protocol> <priority>**

Adds an application to the application priority table.

<b>Syntax Description</b>	selector	Protocol type: ethertype
	protocol	Protocol field in hexadecimal notation (e.g. ‘0x8906’ for FCoE, ‘0x8914’ for FIP).
	priority	Range: 0-7.
<b>Default</b>	No applications are available. The table is empty.	
<b>Configuration Mode</b>	Config	
<b>History</b>	3.3.4200 3.4.0008	
<b>Role</b>	admin	
<b>Example</b>	<pre>switch (config-if)# dcb application-priority ethertype 0x8906 switch (config-if)#{/pre}</pre>	
<b>Related Commands</b>	show lldp interface	
<b>Note</b>		

## clear lldp counters

**clear lldp counters [interface ethernet <Device | Port>]**

Clears LLDP counters for all ports or for a specific port.

<b>Syntax Description</b>	N/A
<b>Default</b>	N/A
<b>Configuration Mode</b>	Global
<b>History</b>	3.6.4006
<b>Role</b>	admin
<b>Example</b>	<pre>switch (config) # clear lldp counters switch (config) # clear lldp counters interface ethernet 1/1</pre>
<b>Related Commands</b>	N/A
<b>Note</b>	

## show lldp local

### show lldp local

Displays LLDP local information.

**Syntax Description** N/A

**Default** N/A

**Configuration Mode** Any Command Mode

**History** 3.2.0300

**Role** admin

**Example**

```
switch (config)# show lldp local
LLDP is Enabled
Local global configuration

Chassis sub type: macAddress (4)
Chassis id: 0002C9030046AF00
System Name: my-switch
System Description: SX1036
Supported capabilities: B,R
Supported capabilities enabled: B

switch (config)#+
```

**Related Commands**

**Note**

## show lldp interfaces

**show lldp interfaces [ethernet <inf> [med-cap | remote]]**

Displays LLDP remote interface table information.

<b>Syntax Description</b>	inf	Local interface number (e.g. 1/1)
	med-cap	Displays local port media capabilities information
	remote	Displays LLDP Ethernet remote configuration & status
<b>Default</b>	N/A	
<b>Configuration Mode</b>	Any Command Mode	
<b>History</b>	3.2.0300 3.3.4200                          Updated Example 3.6.1002                           Updated Example	
<b>Role</b>	admin	
<b>Example</b>	<pre>switch (config)# show lldp interfaces TLV flags: PD: port-description, SN: sys-name, SD: sys-description, SC: sys-capabilities, MA: management-address ETS-C: ETS-Configuration, ETS-R: ETS-Recommendation, AP: Application Priority, PFC: Priority Flow Control CEE: Converged Enhanced Ethernet DCBX version MED-CAP: Media Capabilities MED-NWP: MED-Network Policy  Interface Receive   Transmit   TLVs ----- Eth1/1  Enabled    Enabled    PD, SD Eth1/2  Enabled    Enabled    PD, SN, SD, SC, MA, PFC, AP, ETS-C, ETS-R Eth1/3  Disabled   Disabled   PD, SN, SD, SC, MA, PFC, AP, ETS-C, ETS-R, MED-NWP Eth1/4  Enabled    Enabled    PD, SN, SD, SC, MA, PFC, AP, ETS-C, ETS-R,                            MED-CAP, MED-NWP Eth1/5  Enabled    Enabled    PD, SN, SD, SC, MA, PFC, AP, ETS-C, ETS-R Eth1/6  Enabled    Enabled    PD, SN, SD, SC, MA, PFC, AP, ETS-C, ETS-R Eth1/7  Enabled    Enabled    PD, SN, SD, SC, MA, PFC, AP, ETS-C, ETS-R</pre>	

### Related Commands

### Note

## show lldp remote

### show lldp remote

Displays LLDP remote information (remote device id, remote port id, remote system name).

<b>Syntax Description</b>	N/A			
<b>Default</b>	N/A			
<b>Configuration Mode</b>	Any Command Mode			
<b>History</b>	3.6.3004			
<b>Role</b>	admin			
<b>Example</b>	<pre>switch (config)# show lldp remote ----- Local Interface      Device ID          Port ID        System Name ----- Eth1/4               e4:1d:2d:a5:f3:35   e4:1d:2d:a5:f3:35   Not Advertised Eth1/10              e4:1d:2d:44:65:00   Eth1/10        arc-switch108 Eth1/11              e4:1d:2d:44:65:00   Eth1/11        arc-switch108 Eth1/12              e4:1d:2d:44:65:00   Eth1/12        arc-switch108 Eth1/13              e4:1d:2d:44:65:00   Eth1/13        arc-switch108 Eth1/14              e4:1d:2d:44:65:00   Eth1/14        arc-switch108 Eth1/15              e4:1d:2d:44:65:00   Eth1/15        arc-switch108 Eth1/16              e4:1d:2d:44:65:00   Eth1/16        arc-switch108 Eth1/17              e4:1d:2d:44:65:00   Eth1/17        arc-switch108 Eth1/18              e4:1d:2d:44:65:00   Eth1/18        arc-switch108 Eth1/19              e4:1d:2d:44:65:00   Eth1/19        arc-switch108 Eth1/20              e4:1d:2d:44:65:00   Eth1/20        arc-switch108 Eth1/21              e4:1d:2d:44:65:00   Eth1/21        arc-switch108 Eth1/22              e4:1d:2d:44:65:00   Eth1/22        arc-switch108 Eth1/23              e4:1d:2d:44:65:00   Eth1/23        arc-switch108 Eth1/24              e4:1d:2d:44:65:00   Eth1/24        arc-switch108 Eth1/25              e4:1d:2d:44:65:00   Eth1/25        arc-switch108 Eth1/26              e4:1d:2d:44:65:00   Eth1/26        arc-switch108 Eth1/31              e4:1d:2d:44:65:00   Eth1/31        arc-switch108 Eth1/32              e4:1d:2d:44:65:00   Eth1/32        arc-switch108</pre>			

### Related Commands

#### Note

## show lldp statistics [interface ethernet <inf>]

show lldp statistics [interface ethernet <inf>]

Displays LLDP interface statistics.

**Syntax Description** N/A

**Default** N/A

**Configuration Mode** Any Command Mode

**History** 3.2.0300

**Role** admin

**Example**

```
switch (config)# show lldp statistics interface ethernet 1/1
Interface Frames In In TLVs TLVs Ageout Out
Discarded Errors Total Discarded Unrecognize Frames
-----
Eth 1/1 0 0 10 0 0 0 0 0
```

**Related Commands**

**Note**

## show lldp statistics global

### show lldp statistics global

Displays LLDP global statistics.

**Syntax Description** N/A

**Default** N/A

**Configuration Mode** Any Command Mode

**History** 3.2.0300

**Role** admin

**Example**

```
switch (config)# show lldp timers
Remote Table Last Change Time : 10300
Remote Table Inserts : 5
Remote Table Deletes : 0
Remote Table Drops : 0
Remote Table Ageouts : 0
switch (config)#+
```

**Related Commands**

**Note**

## show lldp timers

### show lldp timers

Displays LLDP timers configuration

**Syntax Description** N/A

**Default** N/A

**Configuration Mode** Any Command Mode

**History** 3.2.0300

**Role** admin

**Example**

```
switch (config)# show lldp timers
msg-tx-interval:30
tx-delay:2
tx-hold:4
tx-reinit-delay:2
switch (config)#+
```

**Related Commands**

**Note**

## show dcb application-priority

### show dcb application-priority

Displays application priority admin table.

<b>Syntax Description</b>	N/A
<b>Default</b>	N/A
<b>Configuration Mode</b>	Any Command Mode
<b>History</b>	3.3.4200
<b>Role</b>	admin
<b>Example</b>	<pre>switch (config)# show dcb application-priority Application priority configuration   Selector      Protocol  Priority   -----+-----+-----+   Ethertype    0x8906    3   Ethertype    0x8914    3 switch (config)# </pre>
<b>Related Commands</b>	
<b>Note</b>	

## 5.5 VLANs

A Virtual Local Area Network (VLAN) is an L2 segment of the network which defines a broadcast domain and is identified by a tag added to all Ethernet frames running within the domain. This tag is called a VLAN ID (VID) and can take a value of 1-4094.

Each port can have a switch mode of either:

- Access – access port is a port connected to a host. It can accept only untagged frames, and assigns them a default configured VLAN (Port VLAN ID). On egress, traffic sent from the access port is untagged.
- Access-dcb – this mode is Mellanox specific that receives ingress untagged traffic but sends egress priority tag (VLAN ID = 0)
- Hybrid – hybrid port is a port connected to either switches or hosts. It can receive both tagged and untagged frames and assigns untagged frames a default configured VLAN (Port VLAN ID). It receives tagged frames with VLANs of which the port is a member (these VLANs' names are allowed). On egress, traffic of allowed VLANs sent from the Hybrid port is sent tagged, while traffic sent with PVID is untagged.
- Trunk – trunk port is a port connecting 2 switches. It accepts only tagged frames with VLANs of which the port is a member. On egress, traffic sent from the Trunk port is tagged. By default, a Trunk port is, automatically, a member on all current VLANs.

### 5.5.1 Configuring Access Mode and Assigning Port VLAN ID (PVID)

➤ *To configure Access mode and assign PVID to interfaces:*

**Step 1.** Log in as admin.

**Step 2.** Enter config mode. Run:

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

**Step 3.** Create a VLAN. Run:

```
switch (config) # vlan 6
switch (config vlan 6) #
```

**Step 4.** Change back to config mode. Run:

```
switch (config vlan 6) # exit
switch (config) #
```

**Step 5.** Enter the interface context. Run:

```
switch (config) # interface ethernet 1/22
switch (config interface ethernet 1/22) #
```

**Step 6.** From within the interface context, configure the interface mode to Access. Run:

```
switch (config interface ethernet 1/22) # switchport mode access
```

**Step 7.** From within the interface context, configure the Access VLAN membership. Run:

```
switch (config interface ethernet 1/22) # switchport access vlan 6
```

**Step 8.** Change back to config mode. Run:

```
switch (config interface ethernet 1/22) # exit  
switch (config) #
```

### 5.5.2 Configuring Hybrid Mode and Assigning Port VLAN ID (PVID)

➤ *To configure Hybrid mode and assign PVID to interfaces:*

**Step 1.** Log in as admin.

**Step 2.** Enter config mode. Run:

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

**Step 3.** Create a VLAN. Run:

```
switch (config) # vlan 6  
switch (config vlan 6) #
```

**Step 4.** Change back to config mode. Run:

```
switch (config vlan 6) # exit  
switch (config) #
```

**Step 5.** Enter the interface context. Run:

```
switch (config) # interface ethernet 1/22  
switch (config interface ethernet 1/22) #
```

**Step 6.** From within the interface context, configure the interface mode to Access. Run:

```
switch (config interface ethernet 1/22) # switchport mode hybrid  
switch (config interface ethernet 1/22) #
```

**Step 7.** From within the interface context, configure the Access VLAN membership. Run:

```
switch (config interface ethernet 1/22) # switchport access vlan 6  
switch (config interface ethernet 1/22) #
```

**Step 8.** Change to config mode again. Run:

```
switch (config interface ethernet 1/22) # exit  
switch (config) #
```

### 5.5.3 Configuring Trunk Mode VLAN Membership

➤ *To configure Trunk mode VLAN membership:*

**Step 1.** Log in as admin.

**Step 2.** Enter config mode. Run:

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

**Step 3.** Create a VLAN. Run:

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

**Step 4.** Change back to config mode. Run:

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

**Step 5.** Enter the interface context. Run:

```
switch [standalone: master] (config) # interface ethernet 1/35  
switch [standalone: master] (config interface ethernet 1/35) #
```

**Step 6.** From within the interface context, configure the interface mode to Trunk. Run:

```
switch [standalone: master] (config interface ethernet 1/35) # switchport mode trunk  
switch [standalone: master] (config interface ethernet 1/35) #
```

#### 5.5.4 Configuring Hybrid Mode VLAN Membership

➤ *To configure Hybrid mode VLAN membership:*

**Step 1.** Log in as admin.

**Step 2.** Enter config mode. Run:

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

**Step 3.** Create a VLAN. Run:

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

**Step 4.** Change back to config mode. Run:

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

**Step 5.** Enter the interface context. Run:

```
switch (config) # interface ethernet 1/35  
switch (config interface ethernet 1/35) #
```

**Step 6.** From within the interface context, configure the interface mode to Hybrid. Run:

```
switch (config interface ethernet 1/35) # switchport mode hybrid  
switch (config interface ethernet 1/35) #
```

**Step 7.** From within the interface context, configure the allowed VLAN membership. Run:

```
switch (config interface ethernet 1/35) # switchport hybrid allowed-vlan add 10  
switch (config interface ethernet 1/35) #
```

**Step 8.** Change to config mode again. Run:

```
switch (config interface ethernet 1/35) # exit  
switch (config) #
```

## 5.5.5 Commands

### vlan

```
vlan {<vlan-id> | <vlan-range>}
no vlan {<vlan-id> | <vlan-range>}
```

Creates a VLAN or range of VLANs, and enters a VLAN context.  
The no form of the command deletes the VLAN or VLAN range.

<b>Syntax Description</b>	vlan-id vlan-range	1-4094. Any range of VLANs.
<b>Default</b>	VLAN 1 is enabled by default.	
<b>Configuration Mode</b>	Config	
<b>History</b>	3.1.1400	
<b>Role</b>	admin	
<b>Example</b>	<pre>switch (config) # vlan 10 switch (config vlan 10) # show vlan  VLAN      Name                  Ports ----      ----- 1         default              Eth1/2, Eth1/3, Eth1/4/1, Eth1/4/2 ... 10  switch (config vlan 10) #</pre>	
<b>Related Commands</b>	show vlan switchport mode switchport [trunk   hybrid] allowed-vlan	
<b>Note</b>	Interfaces are not added automatically to VLAN unless configured with trunk or hybrid mode with “all” option turned on.	

## name

**name <vlan-name>**  
**no name**

Adds VLAN name.

The no form of the command deletes the VLAN name.

<b>Syntax Description</b>	vlan-name	40-character long string.
<b>Default</b>	No name available.	
<b>Configuration Mode</b>	Config VLAN	
<b>History</b>	3.1.1400	
<b>Role</b>	admin	
<b>Example</b>	<pre>switch (config) # vlan 10 switch (config vlan 10) # name my-vlan-name switch (config vlan 10) # show vlan        VLAN      Name            Ports       ----      -----          -----         1        default        Eth1/2, Eth1/3, Eth1/4/1, Eth1/4/2, Eth1/         5,  Eth1/6, Eth1/7, Eth1/8, Eth1/9, Eth1/10,  Eth1/11, Eth1/12, Eth1/13, Eth1/14, Eth1/         15,  Eth1/16, Eth1/17, Eth1/18, Eth1/19, Eth1/         20,  Eth1/21, Eth1/22, Eth1/23, Eth1/24, Eth1/         25,  Eth1/26, Eth1/27, Eth1/28, Eth1/29, Eth1/         30,  Eth1/31, Eth1/32, Eth1/33, Eth1/34, Eth1/         35,  Eth1/36, Po34, Po4096         10       my-vlan-name</pre>	
<b>Related Commands</b>	<a href="#">show vlan</a> <a href="#">switchport mode</a> <a href="#">switchport [trunk   hybrid] allowed-vlan</a>	
<b>Note</b>	Name can not be added to a range of VLANs.	

## show vlan

**show vlan [id <vlan-id>]**

Displays the VLAN table.

<b>Syntax Description</b>	vlan-id	1-4094.									
<b>Default</b>	N/A										
<b>Configuration Mode</b>	Any Command Mode										
<b>History</b>	3.1.1400										
<b>Role</b>	admin										
<b>Example</b>	<pre>switch (config vlan 10) # show vlan</pre> <table><thead><tr><th>VLAN</th><th>Name</th><th>Ports</th></tr></thead><tbody><tr><td>1</td><td>default</td><td>Eth1/2, Eth1/3, Eth1/4/1, Eth1/4/2 ...</td></tr><tr><td>10</td><td>my-vlan-name</td><td></td></tr></tbody></table>		VLAN	Name	Ports	1	default	Eth1/2, Eth1/3, Eth1/4/1, Eth1/4/2 ...	10	my-vlan-name	
VLAN	Name	Ports									
1	default	Eth1/2, Eth1/3, Eth1/4/1, Eth1/4/2 ...									
10	my-vlan-name										
<b>Related Commands</b>	<pre>show vlan switchport mode switchport [trunk   hybrid] allowed-vlan vlan</pre>										
<b>Note</b>											

## switchport mode

**switchport mode {access | dot1q-tunnel | trunk | hybrid | access-dcb}**  
**no switchport mode**

Sets the switch port mode.

The no form of the command sets the switch port mode to access.

<b>Syntax Description</b>	access	Untagged port. 802.1q tagged traffic are filtered. Egress traffic is untagged.
	dot1q-tunnel	Allows both tagged and untagged ingress Ethernet packets. Egress packets are tagged with a second VLAN (802.1Q) header.
	trunk	802.1q tagged port, untagged traffic is filtered.
	hybrid	Both 802.1q tagged and untagged traffic is allowed on the port.
	access-dcb	Untagged port, egress traffic is priority tagged.
<b>Default</b>	access	
<b>Configuration Mode</b>	Config Interface Ethernet Config Interface Port Channel Config Interface MLAG Port Channel	
<b>History</b>	3.1.1400  3.3.4500  3.4.3000	Added MLAG port-channel configuration mode  Added dot1q-tunnel parameter
<b>Role</b>	admin	
<b>Example</b>	<pre>switch (config) # interface ethernet 1/7 switch (config interface ethernet 1/7) # switchport mode access switch (config interface ethernet 1/7) # show interfaces switchport Interface   Mode   Access vlan   Allowed vlans ----- ----- ----- ----- Eth1/2   access      1 Eth1/3   access      1 Eth1/4/1  access      1 Eth1/4/2  access      1 Eth1/5   access      1 Eth1/6   access      1 ... Po34    access      1 Po4096  access      1 switch (config interface ethernet 1/7) #</pre>	

---

**Related Commands**

show vlan  
show interfaces switchport  
switchport access vlan  
switchport [trunk | hybrid] allowed-vlan  
switchport dot1q-tunnel qos-mode  
vlan

---

**Note**

---

## switchport dot1q-tunnel qos-mode

**switchport dot1q-tunnel qos-mode {pipe | uniform}**  
**no switchport dot1q-tunnel qos-mode**

Assigns QoS to the service provider's traffic.

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

<b>Syntax Description</b>	pipe	Gives the service provider's traffic QoS 0
	uniform	Gives the service provider's traffic the same QoS as the customer's traffic
<b>Default</b>	pipe	
<b>Configuration Mode</b>	Config Interface Ethernet Config Interface Port Channel Config Interface MLAG Port Channel	
<b>History</b>	3.4.3000	
<b>Role</b>	admin	
<b>Example</b>	<pre>switch (config interface ethernet 1/1) # switchport dot1q-tunnel qos- mode uniform switch (config interface ethernet 1/1) #</pre>	
<b>Related Commands</b>	show vlan show interfaces switchport switchport access vlan switchport [trunk   hybrid] allowed-vlan vlan	
<b>Note</b>		

## switchport access

**switchport access vlan <vlan-id>**  
**no switchport access vlan**

Sets the port access VLAN.

The no form of the command sets the port access VLAN to 1.

<b>Syntax Description</b>	vlan-id	1-4094.
<b>Default</b>	1	
<b>Configuration Mode</b>	Config Interface Ethernet Config Interface Port Channel Config Interface MLAG Port Channel	
<b>History</b>	3.1.1400  3.2.0500  3.3.4500	Format change (removed hybrid and access-dcb options). Previous command format was: “switchport {hybrid   access-dcb   access} vlan <vlan-id>”  Added MLAG port-channel configuration mode
<b>Role</b>	admin	
<b>Example</b>	<pre>switch (config) # interface ethernet 1/7 switch (config interface ethernet 1/7) # switchport access vlan 10 switch (config interface ethernet 1/7) # show interfaces switchport Interface   Mode   Access vlan   Allowed vlans ----- ----- ----- ----- Eth1/2   access      1 Eth1/3   access      1 Eth1/4/1  access      1 Eth1/4/2  access      1 Eth1/5   access      1 Eth1/6   access      1 Eth1/7   access     10 ... Po4096  access      1 switch (config interface ethernet 1/7) #</pre>	
<b>Related Commands</b>	show vlan show interfaces switchport switchport mode switchport [trunk   hybrid] allowed-vlan vlan	
<b>Note</b>	This command is not applicable for interfaces with port mode trunk. only one option (“access”, “access-dcb” or “hybrid”) is applicable to configure on the port, depends on the switchport mode of the port.	

## **switchport {hybrid, trunk} allowed-vlan**

```
switchport {hybrid, trunk} allowed-vlan {<vlan> | add <vlan> | remove <vlan>
all | except <vlan> | none}
```

Sets the port allowed VLANs.

<b>Syntax Description</b>	vlan	VLAN ID (1-4094) or VLAN range.
	add	Adds VLAN or range of VLANs.
	remove	Removes VLANs or range of VLANs.
	all	Adds all VLANs in available in the VLAN table. New VLANs added to the VLAN table are added automatically.
	except	Adds all VLANs expect this VLAN or VLAN range.
	none	Removes all VLANs.
<b>Default</b>	N/A	
<b>Configuration Mode</b>	Config Interface Ethernet Config Interface Port Channel Config Interface MLAG Port Channel	
<b>History</b>	3.1.1400	
<b>Role</b>	admin	
<b>Example</b>	<pre>switch (config) # interface ethernet 1/7 switch (config interface ethernet 1/7) # switchport hybrid allowed-vlan all switch (config interface ethernet 1/7) #show interfaces switchport Interface   Mode   Access vlan   Allowed vlans ----- ----- ----- ----- Eth1/2    access      1 Eth1/3    access      1 Eth1/4/1   access      1 Eth1/4/2   access      1 Eth1/5    access      1 Eth1/6    access      1 Eth1/7    hybrid      1          1, 10 ... Po34     access      1 Po4096   access      1 switch (config interface ethernet 1/7) #</pre>	

---

**Related Commands**

show vlan  
show interfaces switchport  
switchport access vlan  
switchport mode  
vlan

---

**Note**

This command is not applicable for interfaces with port mode access or access-dcb.

---

## switchport voice

**switchport voice vlan <vlan-id>**  
**no switchport voice vlan**

Configures voice VLAN for the interface.  
The no form of the command disables voice VLAN.

<b>Syntax Description</b>	vlan-id 1-4094.
<b>Default</b>	Disabled
<b>Configuration Mode</b>	Config Interface Ethernet Config Interface Port Channel Config Interface MLAG Port Channel
<b>History</b>	3.6.1002
<b>Role</b>	admin
<b>Example</b>	<pre>switch (config) # interface ethernet 1/7 switch (config interface ethernet 1/7) # switchport voice vlan 10 switch (config interface ethernet 1/7) # show interfaces switchport Interface   Mode   Access vlan   Allowed vlans ----- ----- ----- ----- Eth1/2    access      1 Eth1/3    access      1 Eth1/4/1   access     1 Eth1/4/2   access     1 Eth1/5    access      1 Eth1/6    access      1 Eth1/7    access     10 ... Po4096   access      1 switch (config interface ethernet 1/7) #</pre>
<b>Related Commands</b>	lldp med-tlv-select show vlan show interfaces switchport switchport mode switchport [trunk   hybrid] allowed-vlan vlan
<b>Note</b>	

## show interface switchport

### show interface switchport

Displays all interface switch port configurations.

<b>Syntax Description</b>	N/A
<b>Default</b>	N/A
<b>Configuration Mode</b>	Any Command Mode
<b>History</b>	3.1.1400
<b>Role</b>	admin
<b>Example</b>	<pre>switch (config) #show interfaces switchport Interface   Mode   Access vlan   Allowed vlans ----- ----- ----- ----- Eth1/2    access      1 Eth1/3    access      1 Eth1/4/1   access      1 Eth1/4/2   access      1 Eth1/5    access      1 Eth1/6    access      1 Eth1/7    hybrid      1          1, 10 ... Po34      access      1 Po4096   access      1 switch (config)# </pre>
<b>Related Commands</b>	<pre>show vlan switchport access vlan switchport mode vlan</pre>
<b>Note</b>	

## 5.6 Spanning Tree

The operation of Rapid Spanning Tree Protocol (RSTP) provides for rapid recovery of connectivity following the failure of a bridge/bridge port or a LAN. The RSTP component avoids this delay by calculating an alternate root port, and immediately switching over to the alternate port if the root port becomes unavailable. Thus, using RSTP, the switch immediately brings the alternate port to forwarding state, without the delays caused by the listening and learning states. The RSTP component conforms to IEEE standard 802.1D 2004.

RSTP enhancements is a set of functions added to increase the volume of RSTP in Mellanox switches. It adds a set of capabilities related to the behavior of ports in different segments of the network. For example: the required behavior of a port connected to a non-switch entity, such as host, is to converge quickly, while the required behavior of a port connected to a switch entity is to converge based on the RSTP parameters.

Additionally, it adds security issues on a port and switch basis, allowing the operator to determine the state and role of a port or the entire switch should an abnormal event occur. For example: If a port is configured to be root-guard, the operator will not allow it to become a root-port under any circumstances, regardless of any BPDU that will have been received on the port.

### 5.6.1 Port Priority and Cost

When two ports on a switch are part of a loop, the STP port priority and port path cost configuration determine which port on the switch is put in the forwarding state and which port is put in the blocking state.

To configure port priority use the following command:

```
switch (config interface etherent <inf>)# spanning-tree port-priority <0-240>
```

To configure port path cost use the following command:

```
switch (config interface etherent <inf>)# spanning-tree cost <1-200000000>
```

### 5.6.2 Port Type

Port type has the following configuration options:

- **edge** – is not assumed to be converged by the RSTP learning/forwarding mechanism. It converges to forwarding quickly.



It is recommended to configure the port type for all ports connected to hosts as edge ports.

- **normal** – is assumed to be connected to a switch, thus it tries to be converged by the RSTP learning/forwarding. However, if it does not receive any BPDUs, it is operationally moved to be edge.
- **network** – is assumed to be connected to a switch. If it does not receive any BPDUs, it is moved to discarding state.

Each of these configuration options is mutually exclusive.

Port type is configured using the command spanning-tree port type. It may be applied globally on the switch (Config) level, which configures all switch interfaces. Another option is to configure ports individually by entering the interface's configuration mode.

- Global configuration:

```
switch (config)# spanning-tree port type {edge , normal , network} default
```

- Interface configuration:

```
switch (config interface etherent <inf>)# spanning-tree port type {edge , normal, net-  
work}
```

### 5.6.3 BPDU Filter

Using BPDU filter prevents the CPU from sending/receiving BPDUs on specific ports.

BPDU filtering is configured per interface. When configured, the port does not send any BPDUs and drops all BPDUs that it receives. To configure BPDU filter, use the following command:

```
switch (config interface etherent <inf>)# spanning-tree bpdufilter {enable , disable}
```



Configuring BPDU filtering on a port connected to a switch can cause bridging loops because the port filters any BPDU it receives and goes to forwarding state.

### 5.6.4 BPDU Guard

BPDU guard is a security feature which, when enabled, shuts down the port in case it receives BPDU packets. This feature becomes useful when connecting to an unauthorized switch.

To configure BPDU guard use the following command:

```
switch (config interface etherent <inf>)# spanning-tree port type <type> bpduguard
```

### 5.6.5 Loop Guard

Loop guard is a feature that prevents loops in the network.

When a blocking port in a redundant topology transitions to the forwarding state (accidentally), an STP loop occurs. This happens when BPDUs are no longer received by one of the ports in a physically redundant topology.

Loop guard is useful in switched networks where devices are connected point-to-point. A designated bridge cannot disappear unless it sends an inferior BPDU or brings the link down on a point-to-point connection.



The loop guard configuration is only allowed on “network” port type.

If loop guard is enabled and the port does not receive BPDUs, the port is put into an inconsistent state (blocking) until the port starts to receive BPDUs again. A port in the inconsistent state does

not transmit BPDUs. If BPDUs are received again, loop guard alters its inconsistent state condition. STP converges to a stable topology without the failed link or bridge after loop guard isolates the failure.

Disabling loop guard moves all loop-inconsistent ports to listening state.

To configure loop guard use the following command:

```
switch (config interface etherent <inf>)# spanning-tree guard loop
```

### 5.6.6 Root Guard

Configuring root guard on a port prevents that port from becoming a root port. A port put in root-inconsistent (blocked) state if an STP convergence is triggered by a BPDU that makes that port a root port. The port is unblocked after the port stops sending BPDUs.

To configure loop guard use the following command:

```
switch (config interface etherent <inf>)# spanning-tree guard root
```

### 5.6.7 MSTP

Spanning Tree Protocol (STP) is a mandatory protocol to run on L2 Ethernet networks to eliminate network loops and the resulting broadcast storm caused by these loops. Multiple STP (MSTP) enables the virtualization of the L2 domain into several VLANs, each governed by a separate instance of a spanning tree which results in a network with higher utilization of physical links while still keeping the loop free topology on a logical level.

Up to 64 MSTP instances can be configured on a switch.

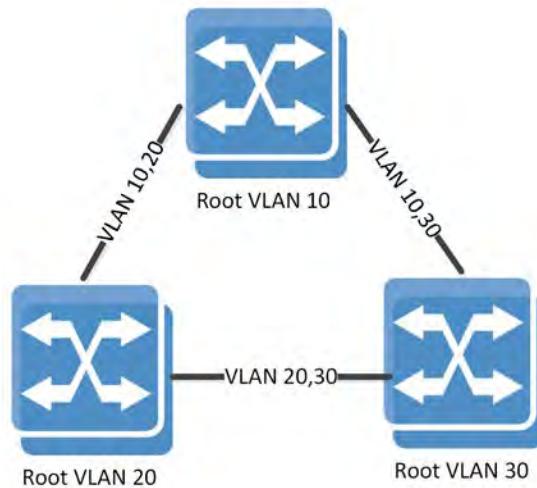
For MSTP network design over Mellanox L2 VMS, please refer to [Mellanox Virtual Modular Switch Reference Guide](#).

### 5.6.8 RPVST

Rapid Per-VLAN Spanning Tree (RPVST) flavor of the STP provides finer-grained traffic by paving a spanning-tree instance per each configured VLAN. Like MSTP, it allows a better utilization of the network links comparing to RSTP.

Figure 19 exhibits a typical RPVST network configuration to get a better utilization on the inter-switch trunk ports.

**Figure 19: RPVST Network Config**



#### 5.6.8.1 RPVST and VLAN Limitations

When the STP of the switch is set to RPVST, spanning tree is set on each of the configured VLANs in the system by default. To enable the spanning tree mode, the command “spanning-tree” must be run.

Each VLAN runs an STP state machine and an RPVST instance. There is a global limitation on the number of active state machines that can operate in MLNX-OS. Enforcement of this limitation is done through the maximum number of VLANs allowed in the system.

For x86 switch systems the limitation is 128 VLANs. For PPC systems, the more ports the switch system has the less VLANs it can support.

**Table 53 - Supported VLANs by RPVST per Switch System**

Switch System Model	Number of Supported VLANs
x86 systems	128
SX1012	17
SX1016	13
SX1024	13
SX1035	13
SX1036	13

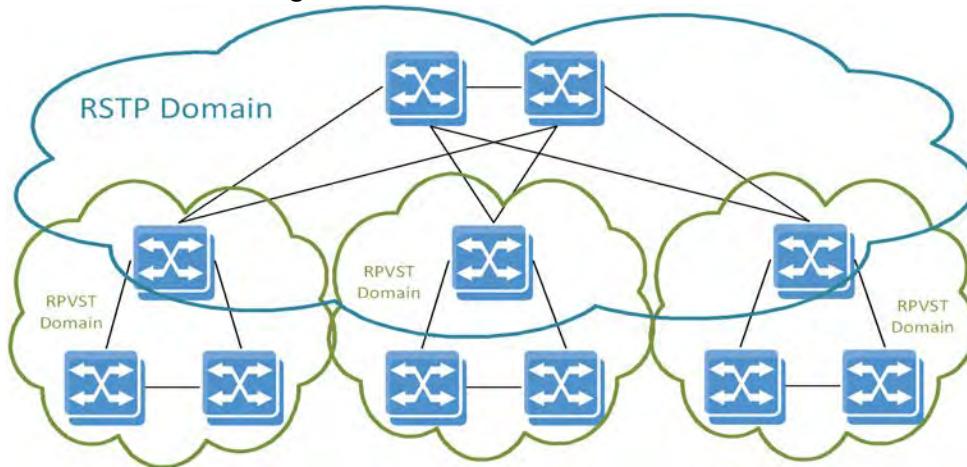
The state machine takes attributes like forward time, hello time, max age and priority, etc.



When configuring priority on a VLAN in RPVST, the operational priority given to the VLAN is a summation of what the user configured and the value of the VLAN itself. For example running “spanning-tree vlan 10 priority 32768” yields a priority of 32778 for VLAN 10.

### 5.6.8.2 RPVST and RSTP Interoperability

**Figure 20: RPVST and RSTP Cluster**



RPVST domains can be interconnected by a standard 802.1Q domain that runs RSTP protocol. While the RSTP domain builds a single common instance spanning tree, the RPVST domains at the edge continue to build a tree per VLAN while exchanging tagged RPVST multicast BPDUs.

(This exchange may happen on untagged RPVST BPDUs as well.) The switch devices that are in the boundary between the RPVST and the RSTP domains should be configured as RPVST mode.

When set to RPVST mode, the switch continues to run the common instance spanning tree (CIST) state machine on VLAN 1 by exchanging IEEE BPDUs with the legacy RSTP switches.

To successfully connect RSTP and RPVST domains, the system administrator must align the native VLAN configuration across all network switches, or in other words, the internal identification of untagged packets to VLAN.

## 5.6.9 Commands

### spanning-tree

**spanning-tree**  
**no spanning-tree**

Globally enables the spanning tree feature.  
The no form disables the spanning tree feature.

<b>Syntax Description</b>	N/A
<b>Default</b>	Spanning tree is enabled.
<b>Configuration Mode</b>	Config
<b>History</b>	3.1.0000
<b>Role</b>	admin
<b>Example</b>	<pre>switch (config) # no spanning-tree switch (config) #</pre>
<b>Related Commands</b>	show spanning-tree
<b>Note</b>	

## spanning-tree mode

**spanning-tree mode {rst | mst | rpvst}**  
**no spanning-tree mode**

Changes the spanning tree mode.

The no form of the command sets the parameter to its default value.

<b>Syntax Description</b>	mst rst rpvst	Multiple spanning tree. Rapid spanning tree. Rapid per-VLAN spanning tree.
<b>Default</b>	rst	
<b>Configuration Mode</b>	Config	
<b>History</b>	3.3.4150	
<b>Role</b>	admin	
<b>Example</b>	switch (config)# spanning-tree mode mst	
<b>Related Commands</b>		
<b>Note</b>	<ul style="list-style-type: none"><li>On x86 switch systems, the number of VLANs supported by RPVST are 128</li></ul>	

## spanning-tree (timers)

```
spanning-tree [forward-time <time in secs> | hello-time <time in secs> | max-age <time in secs>]
no spanning-tree [forward-time | hello-time | max-age | priority]
```

Sets the spanning tree timers.

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

<b>Syntax Description</b>	forward-time	Controls how fast a port changes its spanning tree state from Blocking state to Forwarding state. Parameter range: 4-30 seconds.
	hello-time	Determines how often the switch broadcasts its hello message to other switches when it is the root of the spanning tree. Parameter range: 1-2 seconds.
	max-age	Sets the maximum age allowed for the Spanning Tree Protocol information learnt from the network on any port before it is discarded. Parameter range: 6-40 seconds.
<b>Default</b>	forward-time: 15 seconds hello-time: 2 seconds max-age: 20 seconds	
<b>Configuration Mode</b>	Config	
<b>History</b>	3.1.0000	
<b>Role</b>	admin	
<b>Example</b>	switch (config) # spanning-tree forward-time switch (config) #	
<b>Related Commands</b>	show spanning-tree	
<b>Note</b>	The following formula applies on the spanning tree timers: $2 * (\text{ForwardTime} - 1) \geq \text{MaxAgeTime} \geq 2 * (\text{Hello Time} + 1)$	

## spanning-tree port type (default global)

```
spanning-tree port type {edge [bpdufilter | bpduguard] | network [bpduguard] | normal [bpduguard]} default  
no spanning-tree port type default
```

Configures all switch interfaces as edge/network/normal ports. These ports can be connected to any type of device.

The no form of the command disables the spanning tree operation.

<b>Syntax Description</b>	edge	Assumes all ports are connected to hosts/servers.
	bpdufilter	Configures to enable the spanning tree BPDU filter.
	bpduguard	Configures to enable the spanning tree BPDU guard.
	network	Assumes all ports are connected to switches and bridges.
	normal	The port type (edge or network) determines according to the spanning tree operational mode.
<b>Default</b>	Normal	
<b>Configuration Mode</b>	Config	
<b>History</b>	3.1.0000	
	3.4.0008	Updated command syntax
<b>Role</b>	admin	
<b>Example</b>	<pre>switch (config) # spanning-tree port type edge default switch (config) #</pre>	
<b>Related Commands</b>	show spanning-tree	
<b>Note</b>		

## spanning-tree priority

**spanning-tree priority <bridge-priority>**  
**no spanning-tree priority**

Sets the spanning tree bridge priority.  
The no form of the command sets the bridge priority to default.

<b>Syntax Description</b>	bridge-priority	Sets the bridge priority for the spanning tree. Its value must be in steps of 4096, starting from 0. Only the following values are applicable: 0, 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152, 53248, 57344, 61440.
<b>Default</b>	32786	
<b>Configuration Mode</b>	Config	
<b>History</b>	3.1.0000	
<b>Role</b>	admin	
<b>Example</b>	switch (config) # spanning-tree priority 4096 switch (config) #	
<b>Related Commands</b>	show spanning-tree	
<b>Note</b>		

## spanning-tree port-priority

**spanning-tree port-priority <priority>**  
**no spanning-tree port-priority**

Configures the spanning-tree interface priority.  
The no form of the command returns configuration to its default.

<b>Syntax Description</b>	priority	Spanning tree interface priority. The possible values are: 0, 16, 32, 48, 64, 80, 96, 112, 128, 144, 160, 176, 192, 208, 224, 240.
<b>Default</b>	128	
<b>Configuration Mode</b>	Config Interface Ethernet Config Interface Port Channel Config Interface MLAG Port Channel	
<b>History</b>	3.1.0000	
	3.3.4500	Added MLAG port-channel configuration mode
<b>Role</b>	admin	
<b>Example</b>	<pre>switch (config) # interface ethernet 1/1 switch (config interface ethernet 1/1) # spanning-tree port-priority 16 switch (config interface ethernet 1/1) #</pre>	
<b>Related Commands</b>	show spanning-tree	
<b>Note</b>		

## spanning-tree cost

**spanning-tree cost <port cost>**  
**no spanning-tree cost**

Configures the interface cost of the spanning tree.  
The no form of the command returns configuration to its default.

<b>Syntax Description</b>	port cost	Sets the spanning tree cost of an interface. Value range is 0-200000000.
<b>Default</b>	The default cost is derived from the speed. 1Gbps 20000 10Gbps 2000 40Gbps 500 56Gbps 357	
<b>Configuration Mode</b>	Config Interface Ethernet Config Interface Port Channel Config Interface MLAG Port Channel	
<b>History</b>	3.1.0000	
	3.3.4500	Added MLAG port-channel configuration mode
<b>Role</b>	admin	
<b>Example</b>	<pre>switch (config) # interface ethernet 1/1 switch (config interface ethernet 1/1) # spanning-tree cost 1000 switch (config interface ethernet 1/1) #</pre>	
<b>Related Commands</b>	show spanning-tree	
<b>Note</b>	<ul style="list-style-type: none"> <li>LAG default cost is calculated by dividing the port speed by the number of active links in UP state. For example: if there were 4 links in the LAG out of which only two are in UP state, assuming the port speed is 10Gbps, the LAG cost will be <math>2000/2 = 1000</math>.</li> <li>When configuring the cost for a LAG, the cost will be fixed to this configuration, no matter what the number of active links (UIP state) in the LAG is</li> <li>Unstable network may cause the LAG cost to change dynamically assuming the cost parameter is not configured for anything else other than default</li> </ul>	

## spanning-tree port type

**spanning-tree port type <port type>**  
**no spanning-tree port type**

Configures spanning-tree port type

The no form of the command returns configuration to default.

<b>Syntax Description</b>	default	According to global configuration
	edge	Assumes all ports are connected to hosts/servers.
	normal	The port type (edge or network) determines according to the spanning tree operational mode.
	network	Assumes all ports are connected to switches and bridges.
	bpdufilter	Configures to enable the spanning tree BPDU filter.
	bpduguard	Configures to enable the spanning tree BPDU guard.
<b>Default</b>	Globally defined by the command “spanning-tree port type <port-type> default”	
<b>Configuration Mode</b>	Config Interface Ethernet Config Interface Port Channel Config Interface MLAG Port Channel	
<b>History</b>	3.1.0000	
	3.3.4500	Added MLAG port-channel configuration mode
<b>Role</b>	admin	
<b>Example</b>	<pre>switch (config) # interface ethernet 1/1 switch (config interface ethernet 1/1) # spanning-tree port type edge switch (config interface ethernet 1/1) #</pre>	
<b>Related Commands</b>	show spanning-tree	
<b>Note</b>		

## spanning-tree guard

**spanning-tree guard {loop | root}**  
**no spanning-tree guard {loop | root}**

Configures spanning-tree guard.

The no form of the command returns configuration to default.

<b>Syntax Description</b>	loop	Enables loop-guard on the interface. If the loop-guard is enabled, upon a situation where the interface fails to receive BPDUs the switch will not egress data traffic on this interface.
	root	Enables root-guard on the interface. If root-guard is enabled on the interface, the interface will never be selected as root port.
<b>Default</b>	loop-guard and loop-guard are disabled.	
<b>Configuration Mode</b>	Config Interface Ethernet Config Interface Port Channel Config Interface MLAG Port Channel	
<b>History</b>	3.1.0000	
	3.3.4500	Added MLAG port-channel configuration mode
<b>Role</b>	admin	
<b>Example</b>	<pre>switch (config) # interface ethernet 1/1 switch (config interface ethernet 1/1) # spanning-tree guard root switch (config interface ethernet 1/1) #</pre>	
<b>Related Commands</b>	show spanning-tree	
<b>Note</b>		

## spanning-tree bpdufilter

```
spanning-tree bpdufilter {disable | enable}  
no spanning-tree bpdufilter
```

Configures spanning-tree BPDU filter on the interface. The interface will ignore any BPDU that it receives and will not send PDBUs. The STP state on the port will move to the forwarding state.

The no form of the command returns the configuration to default.

<b>Syntax Description</b>	disable enable	Disables the BPDU filter on this port. Enables the BPDU filter on this port.
<b>Default</b>	BPDU filter is disabled.	
<b>Configuration Mode</b>	Config Interface Ethernet Config Interface Port Channel Config Interface MLAG Port Channel	
<b>History</b>	3.1.0000	
<b>Role</b>	admin	
<b>Example</b>	<pre>switch (config) # interface ethernet 1/1 switch (config interface ethernet 1/1) # spanning-tree bpdufilter enable</pre>	
<b>Related Commands</b>	show spanning-tree	
<b>Note</b>	This command can be used when the switch is connected to hosts.	

## clear spanning-tree counters

### clear spanning-tree counters

Clears the spanning-tree counters.

<b>Syntax Description</b>	N/A
<b>Default</b>	N/A
<b>Configuration Mode</b>	Config
<b>History</b>	3.1.0000
<b>Role</b>	admin
<b>Example</b>	<pre>switch (config) # clear panning-tree counters switch (config) #</pre>
<b>Related Commands</b>	show spanning tree
<b>Note</b>	

## spanning-tree mst max-hops

```
spanning-tree mst max-hops <max-hops>
no spanning-tree mst max-hops
```

Specifies the max hop value inserts into BPDUs that sent out as the root bridge.  
The no form of the command sets the parameter to its default value.

<b>Syntax Description</b>	max-hops	Max hop value. The range is 6-40.
<b>Default</b>	20	
<b>Configuration Mode</b>	Config	
<b>History</b>	3.3.4150	
<b>Role</b>	admin	
<b>Example</b>	switch (config)# spanning-tree mst max-hops 20 switch (config)#	
<b>Related Commands</b>		
<b>Note</b>	<ul style="list-style-type: none"><li>The max hop setting determines the number of bridges in an MST region that a BPDU can traverse before it is discarded</li><li>This command is available when global STP mode is set to MST</li></ul>	

## spanning-tree mst priority

```
spanning-tree mst <mst-instance> priority <priority>
no spanning-tree mst <mst-instance> priority
```

Configures the specified instance's priority number.

The no form of the command sets the parameter to its default value.

Syntax Description	mst-instance	MST instance. Range is 1-64.
	priority	MST instance port priority. Possible values are: 0, 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152, 53248, 57344, 61440
Default	32768	
Configuration Mode	Config	
History	3.3.4150	
Role	admin	
Example	<pre>switch (config)# spanning-tree mst 1 priority 32768 switch (config)#</pre>	
Related Commands		
Note	<ul style="list-style-type: none"><li>• The bridge priority is the four most significant digits of the bridge ID, which is used by spanning tree algorithms to select the root bridge and choose among redundant links. Bridge ID numbers range from 0-65535 (16 bits); bridges with smaller bridge IDs are elected over other bridges.</li><li>• This command is available when global STP mode is set to MST</li></ul>	

## spanning-tree mst vlan

```
spanning-tree mst <mst-instance> vlan <vlan-range>
no spanning-tree mst <mst-instance> vlan <vlan-range>
```

Maps a VLAN or a range of VLANs into an MSTP instance.

The no form of the command unmaps a VLAN or a range of VLANs from MSTP instances.

<b>Syntax Description</b>	mst-instance vlan <vlan-range>	MST instance. Range is 1-64. A single VLAN or a range of VLANs. The format is <vlan> or <from-vlan>-<to-vlan>.
<b>Default</b>	N/A	
<b>Configuration Mode</b>	Config	
<b>History</b>	3.3.4150	
<b>Role</b>	admin	
<b>Example</b>	<pre>switch (config)# spanning-tree mst 1 vlan 10-20 switch (config)#</pre>	
<b>Related Commands</b>		
<b>Note</b>	This command is available when global STP mode is set to MST	

## spanning-tree mst revision

```
spanning-tree mst revision <number>
no spanning-tree mst revision
```

Configures the MSTP revision number.

The no form of the command sets the parameter to its default value.

<b>Syntax Description</b>	number	The MST revision number. Range is 0-65535.
<b>Default</b>	0	
<b>Configuration Mode</b>	Config	
<b>History</b>	3.3.4150	
<b>Role</b>	admin	
<b>Example</b>	<pre>switch (config)# spanning-tree mst revision 1 switch (config)#</pre>	
<b>Related Commands</b>		
<b>Note</b>	<ul style="list-style-type: none"><li>• The revision number is one of three parameters, along with the MST name and VLAN-to-instance map, that identify the switch's MST region</li><li>• This command is available when global STP mode is set to MST</li></ul>	

## spanning-tree mst name

```
spanning-tree mst name <name>
no spanning-tree mst name
```

Configures the MSTP name.

The no form of the command sets the parameter to its default value.

<b>Syntax Description</b>	name	MST name: Up to 32 characters.
<b>Default</b>	N/A	
<b>Configuration Mode</b>	Config	
<b>History</b>	3.3.4150	
<b>Role</b>	admin	
<b>Example</b>	<pre>switch (config)# spanning-tree mst name my-mst switch (config)#</pre>	
<b>Related Commands</b>		
<b>Note</b>	<ul style="list-style-type: none"><li>The name is one of three parameters, along with the MST revision number and VLAN-to-instance map, that identifies the switch's MST region</li><li>This command is available when global STP mode is set to MST</li></ul>	

## spanning-tree mst root

**spanning-tree mst <mst-instance> root <role>**  
**no spanning-tree mst <mst-instance> root**

Changes the bridge priority for the specified MST instance to the following values:

- Primary – 8192
- Secondary – 16384

The no form of the command sets the parameter to its default value.

<b>Syntax Description</b>	mst-instance role	MSTP instance. Possible range is 1-64. Values: “primary” or “secondary”.
<b>Default</b>	primary	
<b>Configuration Mode</b>	Config	
<b>History</b>	3.3.4150	
<b>Role</b>	admin	
<b>Example</b>	switch (config)# spanning-tree mst name my-mst switch (config)#	
<b>Related Commands</b>		
<b>Note</b>	<ul style="list-style-type: none"> <li>• The root command is a way to automate a system configuration while ‘playing’ with the priority field. The priority field granularity may be too explicit for some users in case you wish to have 2 levels of priority (primary and secondary). So by default all the switches get the same priority and while using the root option you can get the role of master and backup by setting the priority field to a predefined value.</li> <li>• This command is available when global STP mode is set to MST.</li> </ul>	

## spanning-tree mst port-priority

```
spanning-tree mst {mst-instance} port-priority <priority>
no spanning-tree mode
```

Changes the spanning tree mode.

The no form of the command sets the parameter to its default value.

Syntax Description	mst-instance	MST instance. Range is 1-64.
	priority	MST instance port priority. Valid values are: 0, 16, 32, 48, 64, 80, 96, 112, 128, 144, 160, 176, 192, 208, 224 and 240.
Default	rst	
Configuration Mode	Config Interface Ethernet Config Interface Port Channel	
History	3.3.4150	
Role	admin	
Example		<pre>switch (config interface ethernet 1/1)# spanning-tree mst 1 port- priority 32768 switch (config interface port-channel 1)# spanning-tree mst 1 port- priority 32768</pre>
<b>Related Commands</b>		
Note	This command is available when global STP mode is set to MST.	

## spanning-tree mst cost

**spanning-tree mst {mst-instance} cost <cost-value>**  
**no spanning-tree mode**

Configures the cost per MSTP instance.

The `no` form of the command sets the parameter to its default value.

<b>Syntax Description</b>	mst-instance	MST instance. Range is 1-64.
	cost-value	MST instance port cost. Range is 0-200000000.
<b>Default</b>	20000 for 1Gb/s, 2000 for 10Gb/s, 500 for 40Gb/s, 357 for 56Gb/s, 200 for 100Gb/s	
<b>Configuration Mode</b>	Config Interface Port Channel	
<b>History</b>	3.3.4150	
<b>Role</b>	admin	
<b>Example</b>	<pre>switch (config interface ethernet 1/1)# spanning-tree mst 1 cost 4000 switch (config interface port-channel 1)# spanning-tree mst 1 cost 4000 switch (config)#+</pre>	
<b>Related Commands</b>		
<b>Note</b>	This command is available when global STP mode is set to MST.	

## spanning-tree vlan forward-time

```
spanning-tree vlan <vid> forward-time <secs>
no spanning-tree vlan <vid> forward-time
```

Configures how fast an interface changes its spanning tree state from Blocking to Forwarding.

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

<b>Syntax Description</b>	secs	Parameter range: 4-30 seconds.
<b>Default</b>	15 seconds	
<b>Configuration Mode</b>	Config	
<b>History</b>	3.4.1100	
<b>Role</b>	admin	
<b>Example</b>	switch (config) # spanning-tree vlan 10 forward-time 15	
<b>Related Commands</b>	show spanning-tree	
<b>Note</b>	<ul style="list-style-type: none"><li>The following formula applies on the spanning tree timers: <math>2 * (\text{ForwardTime} - 1) \geq \text{MaxAgeTime} \geq 2 * (\text{Hello Time} + 1)</math></li><li>This command is available when global STP mode is set to RPVST</li></ul>	

## spanning-tree vlan hello-time

```
spanning-tree vlan <vid> hello-time <secs>
no spanning-tree vlan <vid> hello-time
```

Configures how often the switch broadcasts its hello message to other switches when it is the root of the spanning tree.

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

<b>Syntax Description</b>	secs	Parameter range: 1-2 seconds.
<b>Default</b>	2 seconds	
<b>Configuration Mode</b>	Config	
<b>History</b>	3.4.1100	
<b>Role</b>	admin	
<b>Example</b>	switch (config) # spanning-tree vlan 10 hello-time 2	
<b>Related Commands</b>	show spanning-tree	
<b>Note</b>	<ul style="list-style-type: none"><li>The following formula applies on the spanning tree timers: <math>2*(ForwardTime - 1) \geq MaxAgeTime \geq 2*(Hello Time + 1)</math></li><li>This command is available when global STP mode is set to RPVST</li></ul>	

## spanning-tree vlan max-age

```
spanning-tree vlan <vid> max-age <secs>
no spanning-tree vlan <vid> max-age
```

Sets the maximum age allowed for the Spanning Tree Protocol information learned from the network on any port before it is discarded.

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

<b>Syntax Description</b>	secs	Parameter range: 6-40 seconds.
<b>Default</b>	20 seconds	
<b>Configuration Mode</b>	Config	
<b>History</b>	3.4.1100	
<b>Role</b>	admin	
<b>Example</b>	switch (config) # spanning-tree vlan 10 max-age 20	
<b>Related Commands</b>	show spanning-tree	
<b>Note</b>	<ul style="list-style-type: none"><li>The following formula applies on the spanning tree timers: <math>2 * (\text{ForwardTime} - 1) \geq \text{MaxAgeTime} \geq 2 * (\text{Hello Time} + 1)</math></li><li>This command is available when global STP mode is set to RPVST</li></ul>	

## spanning-tree vlan priority

```
spanning-tree vlan <vid> priority <priority>
no spanning-tree vlan <vid> priority
```

Configures RPVST instance port priority.

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

<b>Syntax Description</b>	priority	Possible values are: 0, 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152, 53248, 57344, 61440.
<b>Default</b>	32768	
<b>Configuration Mode</b>	Config	
<b>History</b>	3.4.1100	
<b>Role</b>	admin	
<b>Example</b>	switch (config) # spanning-tree vlan 10 priority 32768	
<b>Related Commands</b>	show spanning-tree	
<b>Note</b>	<ul style="list-style-type: none"><li>The following formula applies on the spanning tree timers: <math>2 * (\text{ForwardTime} - 1) \geq \text{MaxAgeTime} \geq 2 * (\text{Hello Time} + 1)</math></li><li>This command is available when global STP mode is set to RPVST</li></ul>	

## show spanning-tree

### show spanning-tree

Displays spanning tree information.

<b>Syntax Description</b>	N/A
<b>Default</b>	N/A
<b>Configuration Mode</b>	Any Command Mode
<b>History</b>	3.1.0000 3.4.1100 Updated Example with R and G flags
<b>Role</b>	admin
<b>Example</b>	<pre>switch (config) # show spanning-tree  Switch ethernet-default  Spanning tree protocol is enabled rst  Spanning tree force version:2  Root ID     Priority 32768     Address 00:02:c9:7a:e9:40     Cost 1000     Port Eth1/32     Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec  Bridge ID     Priority 32768     Address 00:02:c9:96:c6:d0     Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec  L - Loop Inconsistent R - Root Inconsistent G - BPDU Guard Inconsistent  Interface      Role        Sts          Cost      Prio     Type ----          ----        ----          ----      ----     ---- Eth1/9         Designated  Forwarding   500       128      normal Eth1/22        Designated  Discarding(R) 500       128      normal Eth1/32        Root        Forwarding   500       128      normal Eth1/39        Disabled   Discarding(G) 2000      128      normal  switch (config) #</pre>
<b>Related Commands</b>	clear spanning-tree counters spanning-tree
<b>Note</b>	

## show spanning-tree detail

### show spanning-tree detail

Displays detailed spanning-tree configuration and statistics.

<b>Syntax Description</b>	N/A
<b>Default</b>	N/A
<b>Configuration Mode</b>	Any Command Mode
<b>History</b>	3.1.0000
	3.6.4110 Updated example output
	3.6.5000 Updated example output
<b>Role</b>	admin
<b>Example</b>	<pre>switch (config) # show spanning-tree detail  Switch ethernet-default Spanning tree protocol is enabled Bridge is executing the rst compatible Spanning Tree Protocol  Bridge Identifier priority: 32768 Bridge Identifier address: e4:1d:2d:3d:5e:c0 Configured hello time: 2, max age 20, forward delay 15 Current root: priority 32768, address e4:1d:2d:3d:5e:c0 Number of topology changes: 1, last change occurred 00:00:02 ago Last TCN received from: N/A Timers: hold 6 hello 2, max age 20, forward delay 15 Default port type: normal Default bpdu filter: disabled Default bpdu guard: disabled</pre>
<b>Related Commands</b>	<a href="#">clear spanning-tree counters</a> <a href="#">spanning-tree</a>
<b>Note</b>	

## show spanning-tree interface

```
show spanning-tree interface {ethernet <slot>/<port> | port-channel
<port-channel> | mlag-port-channel <mlag-port-channel>}
```

Display running state for specific interfaces.

<b>Syntax Description</b>	ethernet port-channel mlag-port-channel	Ethernet interface. LAG instance. MLAG instance.
<b>Default</b>	N/A	
<b>Configuration Mode</b>	Any Command Mode	
<b>History</b>	3.3.4150	
<b>Role</b>	admin	
<b>Example</b>	<pre>switch (config) # show spanning-tree interface ethernet 1/2 Eth1/2 is Disabled Discarding     Port path cost 500, Port priority 128, Port Identifier 128.5     Designated root has priority 0, address unknown     Designated bridge has priority 0, address unknown     Designated port id 0.0, designated path cost 0     Number of transitions to forwarding state: 0     Port type: normal     PortFast is: off     Bpdu filter: disabled     Bpdu guard: disabled     Loop guard: disabled     Root guard: disabled     Link type: point-to-point     BPDU: sent: 0    received: 0 switch (config) #</pre>	
<b>Related Commands</b>	<a href="#">clear spanning-tree counters</a> <a href="#">spanning-tree</a>	
<b>Note</b>		

## show spanning-tree mst

```
show spanning-tree mst [details | <instance> interface {ethernet <slot>/<port> | port-channel <port-channel> | mlag-port-channel <mlag-port-channel>}]
```

Displays basic multi-spanning-tree information.

<b>Syntax Description</b>	details	Displays detailed multi-spanning-tree configuration and statistics.
	ethernet	Ethernet interface.
	port-channel	LAG instance.
	mlag-port-channel	MLAG instance.
<b>Default</b>	N/A	
<b>Configuration Mode</b>	Any Command Mode	
<b>History</b>	3.3.4150	
<b>Role</b>	admin	
<b>Example</b>	<pre>switch (config) # show spanning-tree mst  MST0 vlans mapped: 1-1023,1025-2047,2049-3071,3073-4094 Interface      Role        Sts          Cost      Prio     Type ----          ----        ----          ----      ----     ---- Eth1/9         Designated  Forwarding   500      128.9    point-to-point Eth1/10        Designated  Forwarding   500      128.10   point-to-point Eth1/11        Back Up     Discarding   500      128.22   point-to-point switch (config) #</pre>	
<b>Related Commands</b>	<a href="#">clear spanning-tree counters</a> <a href="#">spanning-tree</a>	
<b>Note</b>		

## show spanning-tree root

### show spanning-tree root

Displays root multi-spanning-tree information.

**Syntax Description** N/A

**Default** N/A

**Configuration Mode** Any Command Mode

**History** 3.3.4150

**Role** admin

**Example**

```
switch (config) # show spanning-tree root
Instance  Priority  MAC addr      Root Cost  Hello Time Max Age  FWD Dly  Root Port
-----  -----  -----
MST0      32768    00:02:c9:71:ed:40  500       2          20           15        Eth1/20
MST1      32768    00:02:c9:71:f0:c0  0          2          20           15        -
MST2      0         00:02:c9:71:f0:c0  0          2          20           15        -
MST3      32768    00:02:c9:71:f0:c0  0          2          20           15        -
switch (config) #
```

**Related Commands**

clear spanning-tree counters  
spanning-tree

**Note**

## show spanning-tree vlan

**show spanning-tree vlan <vid> [detail | interface {ethernet <slot>/<port> | port-channel <port-channel> | mlag-port-channel <mlag-port-channel>}]**

Displays spanning tree information.

<b>Syntax Description</b>	vid	VLAN ID. Range is also supported Format: <vid1>[-<vid2>]
	detail	Displays detailed RPVST configuration and statistics
	ethernet	Ethernet interface
	port-channel	LAG instance
	mlag-port-channel	MLAG instance
<b>Default</b>	N/A	
<b>Configuration Mode</b>	Any Command Mode	
<b>History</b>	3.4.1100	
	3.6.5000	Updated example output
<b>Role</b>	admin	
<b>Example</b>	<pre>switch (config) # show spanning-tree detail  Switch ethernet-default Spanning tree protocol is enabled Bridge is executing the rpvst compatible Spanning Tree Protocol  Vlan 1:     Bridge Identifier priority: 32769     Bridge Identifier address: e4:1d:2d:3d:5e:c0     Configured hello time: 2, max age 20, forward delay 15     Current root: priority 32769, address e4:1d:2d:3d:5e:c0     Number of topology changes: 0, last change occurred 00:00:00 ago     Last TCN received from: N/A     Timers: hold 6 hello 2, max age 20, forward delay 15     Default port type: normal     Default bpdu filter: disabled     Default bpdu guard: disabled switch (config) #</pre>	
<b>Related Commands</b>	<a href="#">clear spanning-tree counters</a> <a href="#">spanning-tree</a>	
<b>Note</b>		

## show spanning-tree vlan topo-change-history

**show spanning-tree vlan <vid> topo-change-history**

Displays spanning-tree topology change notification history per vlan.

<b>Syntax Description</b>	vid	VLAN ID. Range is also supported. Format: <vid1>[-<vid2>]															
<b>Default</b>	N/A																
<b>Configuration Mode</b>	Any Command Mode																
<b>History</b>	3.6.4110																
<b>Role</b>	admin																
<b>Example</b>	<pre>switch (config) # show spanning-tree vlan 50 topo-change-history</pre> Vlan 50 ----- <table><thead><tr><th>Interface</th><th>Date</th><th>Time</th></tr></thead><tbody><tr><td>Eth1/49</td><td>07/18/17</td><td>04:39:58</td></tr><tr><td>Eth1/49</td><td>07/18/17</td><td>04:39:55</td></tr><tr><td>Eth1/49</td><td>07/18/17</td><td>04:38:11</td></tr><tr><td>Eth1/49</td><td>07/18/17</td><td>04:38:09</td></tr></tbody></table>		Interface	Date	Time	Eth1/49	07/18/17	04:39:58	Eth1/49	07/18/17	04:39:55	Eth1/49	07/18/17	04:38:11	Eth1/49	07/18/17	04:38:09
Interface	Date	Time															
Eth1/49	07/18/17	04:39:58															
Eth1/49	07/18/17	04:39:55															
Eth1/49	07/18/17	04:38:11															
Eth1/49	07/18/17	04:38:09															
<b>Related Commands</b>	<a href="#">spanning-tree</a>																
<b>Note</b>																	

## show spanning-tree mst topo-change-history

**Show spanning-tree mst <mst-instance> topo-change-history**

Displays spanning-tree topology change notification history per instance.

<b>Syntax Description</b>	mst-instance	MST instance. Range is 1-64.	
<b>Default</b>	N/A		
<b>Configuration Mode</b>	Any Command Mode		
<b>History</b>	3.6.4110		
<b>Role</b>	admin		
<b>Example</b>	<pre>switch (config) # show spanning-tree mst 5 topo-change-history</pre>		
	<pre>Instance 5</pre>		
	<pre>-----</pre>		
	Interface	Date	Time
	<pre>-----</pre>		
	Eth1/49	07/18/17	04:43:51
	Eth1/49	07/18/17	04:43:33
<b>Related Commands</b>	<a href="#">spanning-tree</a>		
<b>Note</b>			

## show spanning-tree topo-change-history

### show spanning-tree topo-change-history

Displays spanning-tree topology change notification history.

<b>Syntax Description</b>	mst-instance	MST instance. Range is 1-64.																														
<b>Default</b>	N/A																															
<b>Configuration Mode</b>	Any Command Mode																															
<b>History</b>	3.6.4110																															
<b>Role</b>	admin																															
<b>Example</b>	<pre>switch (config) # show spanning-tree topo-change-history</pre> ----- <table><thead><tr><th>Interface</th><th>Date</th><th>Time</th></tr></thead><tbody><tr><td>Eth1/49</td><td>07/27/17</td><td>09:39:38</td></tr><tr><td>Eth1/35</td><td>07/27/17</td><td>09:35:42</td></tr><tr><td>Eth1/35</td><td>07/27/17</td><td>09:35:40</td></tr><tr><td>Eth1/35</td><td>07/27/17</td><td>09:35:08</td></tr><tr><td>Eth1/35</td><td>07/27/17</td><td>09:35:06</td></tr><tr><td>Eth1/35</td><td>07/27/17</td><td>09:32:05</td></tr><tr><td>Eth1/35</td><td>07/27/17</td><td>09:32:03</td></tr><tr><td>Eth1/35</td><td>07/27/17</td><td>09:31:42</td></tr><tr><td>Eth1/35</td><td>07/27/17</td><td>09:31:40</td></tr></tbody></table>		Interface	Date	Time	Eth1/49	07/27/17	09:39:38	Eth1/35	07/27/17	09:35:42	Eth1/35	07/27/17	09:35:40	Eth1/35	07/27/17	09:35:08	Eth1/35	07/27/17	09:35:06	Eth1/35	07/27/17	09:32:05	Eth1/35	07/27/17	09:32:03	Eth1/35	07/27/17	09:31:42	Eth1/35	07/27/17	09:31:40
Interface	Date	Time																														
Eth1/49	07/27/17	09:39:38																														
Eth1/35	07/27/17	09:35:42																														
Eth1/35	07/27/17	09:35:40																														
Eth1/35	07/27/17	09:35:08																														
Eth1/35	07/27/17	09:35:06																														
Eth1/35	07/27/17	09:32:05																														
Eth1/35	07/27/17	09:32:03																														
Eth1/35	07/27/17	09:31:42																														
Eth1/35	07/27/17	09:31:40																														
<b>Related Commands</b>	<a href="#">spanning-tree</a>																															
<b>Note</b>																																

## 5.7 MAC Address Table

### 5.7.1 Configuring Unicast Static MAC Address

You can configure static MAC addresses for unicast traffic. This feature improves security and reduces unknown unicast flooding.

➤ *To configure Unicast Static MAC address:*

**Step 1.** Log in as admin.

**Step 2.** Enter config mode. Run:

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

**Step 3.** Run the command “mac-address-table static unicast <destination mac address> vlan <vlan identifier(1-4094)> interface ethernet <slot>/<port>”.

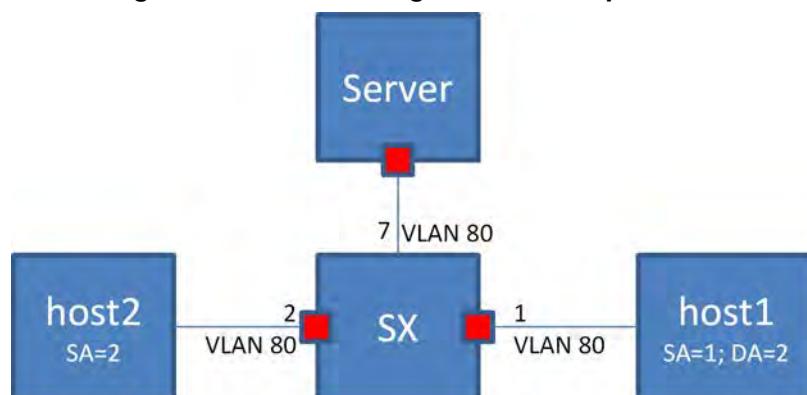
```
switch (config) # mac-address-table static 00:11:22:33:44:55 vlan 1 interface ethernet
1/1
```

### 5.7.2 MAC Learning Considerations

MAC learning may be disabled using the command `mac-learning disable` which is beneficial in the following situations:

- To prevent denial-of-service attacks
- To manage the available MAC address table space by controlling which interfaces can learn MAC addresses
- To duplicate to a dedicated server (port7) all the packets that one host (host1; port1) sends to another (host2; port2), like in port mirroring. To accomplish this, MAC learning is disabled on port2. In this case the FDB does not obtain the MAC address of host2. Also, to prevent broadcast to every port, it is possible to configure a VLAN (VLAN 80) which ports 1, 2 and 7 are member of.

**Figure 21: MAC Learning Disable Example Case**



## 5.7.3 Commands

### mac-address-table aging-time

```
mac-address-table aging-time <age>
no mac-address-table aging-time
```

Sets the maximum age of a dynamically learnt entry in the MAC address table.  
The no form of the command resets the aging time of the MAC address table to its default.

<b>Syntax Description</b>	age	10-1000000 seconds.
<b>Default</b>	300	
<b>Configuration Mode</b>	Config	
<b>History</b>	3.1.0600	
<b>Role</b>	admin	
<b>Example</b>	<pre>switch (config) # mac-address-table aging-time 50 switch (config) # show mac-address-table aging-time</pre>	
	Mac Address Aging Time: 50	
	<pre>switch (config) #</pre>	
<b>Related Commands</b>	show mac-address-table show mac-address-table aging time	
<b>Note</b>		

## mac-address-table static

```
mac-address-table static <mac address> vlan <vlan> interface <if-type> <if-number>
no mac-address-table static <mac address> vlan <vlan> interface <if-type> <if-number>
```

Configures a static MAC address in the forwarding database.

The no form of the command deletes a configured static MAC address from the forwarding database.

<b>Syntax Description</b>	mac address vlan if-type if-number	Destination MAC address. VLAN ID or VLAN range. Ethernet or port-channel interface type. The interface number (i.e. 1/1, 3).
<b>Default</b>	No static MAC addresses available in default.	
<b>Configuration Mode</b>	Config	
<b>History</b>	3.1.0600	
<b>Role</b>	admin	
<b>Example</b>	<pre>switch (config) # mac-address-table static aa:aa:aa:aa:aa:aa vlan 1 interface ethernet 1/7 switch (config) # show mac-address-table  Switch ethernet-default  Vlan      Mac Address          Type      Interface ----      -----              ----      ----- 1        aa:aa:aa:aa:aa:aa    static     Eth1/7 Number of unicast:      1 Number of multicast:    0 switch (config) #</pre>	
<b>Related Commands</b>	<a href="#">show mac-address-table</a> <a href="#">mac-address-table aging time</a>	
<b>Note</b>	The no form of the command will not clear a dynamic MAC address. Dynamic MAC addresses are cleared using the “clear mac-address-table dynamic” command.	

## mac-learning disable

**mac-learning disable**  
**no mac-learning disable**

Disables MAC-address learning.  
The no form of the command enables MAC-address learning.

<b>Syntax Description</b>	N/A
<b>Default</b>	Enabled
<b>Configuration Mode</b>	Config Interface Ethernet Config Interface Port Channel
<b>History</b>	3.1.0600
<b>Role</b>	admin
<b>Example</b>	<pre>switch (config interface ethernet 1/1) # mac-learning disable</pre>
<b>Related Commands</b>	
<b>Note</b>	<ul style="list-style-type: none"><li>When adding a port to a LAG, the port needs to be aligned with the LAG's configuration</li><li>When removing a port from a LAG, the port remains in whichever configuration the LAG is in</li><li>Disabling MAC learning is not supported on a local analyzer port.</li><li>Disabling MAC learning is not supported on an IPL LAG.</li></ul>

## clear mac-address-table dynamic

**clear mac-address-table dynamic**

Clear the dynamic entries in the MAC address table.

<b>Syntax Description</b>	N/A
<b>Default</b>	N/A
<b>Configuration Mode</b>	Config
<b>History</b>	3.1.0600
<b>Role</b>	admin
<b>Example</b>	<pre>switch (config) # clear mac-address-table dynamic switch (config) #</pre>
<b>Related Commands</b>	mac-address-table aging-time mac-address-table static show mac-address-table
<b>Note</b>	This command does not clear the MAC addresses learned on the mgmt0 port. Static entries are deleted using the “no mac-address-table static” command.

## show mac-address-table

**show mac-address-table [address <mac-address> | interface ethernet <if-number> | vlan [<vlan> | range <range>] | unicast | multicast]**

Displays the static and dynamic unicast and multicast MAC addresses for the switch.  
Various of filter options available.

<b>Syntax Description</b>	mac-address if-number vlan range unicast multicast	Filter the table to a specific MAC address. Filter the table to a specific interface. Filter the table to a specific VLAN number (1-4094). Filter the table to a range of VLANs. Filter the table to a unicast addresses only. Filter the table to a multicast addresses only.
<b>Default</b>	N/A	
<b>Configuration Mode</b>	Any Command Mode	
<b>History</b>	3.1.0600 3.3.4500	Updated Example
<b>Role</b>	admin	
<b>Example</b>	<pre>switch (config) # show mac-address-table  Switch ethernet-default        Vlan      Mac Address          Type      Interface       ---      -----          ----      -----       1        00:00:00:00:00:01    Static    Po5       1        00:00:3D:5C:FE:16    Dynamic   Eth1/1       1        00:00:3D:5D:FE:1B    Dynamic   Eth1/2 Number of unicast:      2 Number of multicast:    0 switch (config) #</pre>	
<b>Related Commands</b>	mac-address-table static clear mac-address-table	
<b>Note</b>		

## show mac-address-table aging-time

### show mac-address-table aging-time

Displays the MAC address table aging time.

<b>Syntax Description</b>	N/A
<b>Default</b>	N/A
<b>Configuration Mode</b>	Any Command Mode
<b>History</b>	3.1.0600
<b>Role</b>	admin
<b>Example</b>	<pre>switch (config) # mac-address-table aging-time 300 switch (config) # show mac-address-table aging-time  Mac Address Aging Time: 300  switch (config) #</pre>
<b>Related Commands</b>	mac-address-table aging-time mac-address-table static clear mac-address-table
<b>Note</b>	MAC addresses learned on the mgmt0 is not shown by this command.

## show mac-address-table interface

**show mac-address-table interface [port-channel | mlag-port-channel <if>]**

Displays the MAC address table of a port channel or an MLAG port channel.

<b>Syntax Description</b>	N/A
<b>Default</b>	N/A
<b>Configuration Mode</b>	Any Command Mode
<b>History</b>	3.6.4006
<b>Role</b>	admin
<b>Example</b>	<pre>switch (config) # show mac-address-table ----- Vlan Mac Address Type Port ----- 1 E4:1D:2D:37:11:22 Static Eth1/1 1 E4:1D:2D:37:3E:11 Static Po5  Number of unicast: 2 Number of multicast: 0  switch (config) # show mac-address-table interface port-channel 5 ----- Vlan Mac Address Type Port ----- 1 E4:1D:2D:37:3E:11 Static Po5  Number of unicast: 1 Number of multicast: 0</pre>
<b>Related Commands</b>	<a href="#">mac-address-table static</a> <a href="#">clear mac-address-table</a>
<b>Note</b>	

## show mac-address-table summary

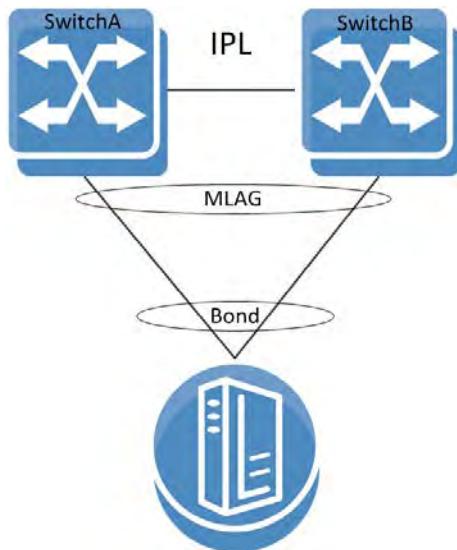
### show mac-address-table summary

Displays total number of unicast/multicast MAC address entries.

<b>Syntax Description</b>	N/A
<b>Default</b>	N/A
<b>Configuration Mode</b>	Any Command Mode
<b>History</b>	3.6.2002
<b>Role</b>	admin
<b>Example</b>	<pre>switch (config) # show mac-address-table summary Number of unicast:    4 Number of multicast:  0</pre>
<b>Related Commands</b>	<a href="#">mac-address-table static</a> <a href="#">clear mac-address-table</a>
<b>Note</b>	

## 5.8 MLAG

**Figure 22: Basic MLAG Setup**



All nodes in an MLAG must be of the same CPU type (i.e., x86).



Each switch configuration is independent and it is user responsibility to make sure to configure both switches similarly pertaining MLAG (e.g. MLAG port-channel VLAN membership, static MAC, ACL, etc.).

A link aggregation group (LAG) is used for extending the bandwidth from a single link to multiple links and provide redundancy in case of link failure. Extending the implementation of the LAG to more than a single device provides yet another level of redundancy that extends from the link level to the node level. This extrapolation of the LAG from single to multiple switches is referred to as multi-chassis link aggregation (MLAG).



MLAG is currently supported for 2 switches only.



The VIP address must be on the same management IP subnet.

A peered device (host or switch) connecting to switches running an MLAG runs a standard LAG and is unaware of the fact that the LAG connects to two separate switches.



MLAG links currently mandate disabling xSTP control protocol. However, interfaces not part of an MLAG can run any protocol independently.

The MLAG switches share an inter-peer link (IPL) between them for carrying control messages in a steady state or data packages in failure scenarios. Thus, the bandwidth of the IPL should be defined accordingly. The IPL itself can be a LAG and may be constructed of either 10GbE or 40GbE links. In such a case, PFC must be configured on this IPL. [Figure 23, “Basic MLAG Topology,” on page 749](#) illustrates this. The IPL serves the following purposes:

- MLAG protocol control – keepalive messages, MAC sync, MLAG port sync, etc.
- MLAG port failure – serves redundancy in case of a fallen link on one of the MLAG switches
- Layer-3 failure – serves redundancy in case of a failed connection between the MLAG switches and the rest of the L3 network should there be one



The IPL VLAN interface must be used only for MLAG protocol and must not be used by any other interfaces (e.g. port-channel, Ethernet).

The MLAG protocol is made up of the following components to be expanded later:

- Keepalive
- Unicast and multicast sync
- MLAG port sync

When positioned at the top of rack (ToR) and connecting with a Layer-3 uplink, the MLAG pair acts as the L3 border for the hosts connected to it. To allow default gateway redundancy, both MLAG switches should be addressed by the host via the same default gateway address.

MLAG uses an IP address (VIP) that is always directed to the MLAG-VIP master node.

When running MLAG with L3, VRRP or MAGP must be deployed. For more information, refer to [Section 6.8, “VRRP,” on page 1370](#) or [Section 6.9, “MAGP,” on page 1385](#) respectively.



When MLAG is connected through a Layer-2 based uplink, there is no need to apply default gateway redundancy towards hosts since this function is implemented on the L2/L3 border points of the network.

The two peer switches need to carry the exact same configuration of the MLAG attributes for guaranteeing proper functionality of the MLAG.



Ensuring that both switches are configured identically is the responsibility of the user and is not monitored by the MLNX-OS® software.



When working with MLAG the maximum number of MAC addresses

- on SwitchX®-2 based systems, is limited to 47,970. Without it, the number of MAC addresses would be 55,872.
- on Spectrum™ based systems, is limited to 88K. Without it, there is no limitation.



When transitioning from standalone into a group or vice versa, a few seconds are required for the node state to stabilize. During that time, group features such as Gateway HA, SM HA, and MLAG commands should not be executed. To run group features, wait for the CLI prompt to turn into [standalone:master], [<group>:master] or [<group>:standby] instead of [standalone:\*unknown\*] or [<group>:\*unknown\*].



In a scenario where there is no IP communication between the MGMT ports of the MLAG switches (for example when one MGMT port is disconnected), the following CLI prompt is displayed:

<hostname>[<mlag cluster name>:unknown]#

This does not reflect the MLAG state, but only the state of the cluster.

### 5.8.1 MLAG Keepalive and Failover

Master election in MLAG is based on the IPs of the nodes taking part of the MLAG. The master elected is that which has the highest IPL VLAN interface local IP address.



MLAG master/slave roles take effect in fault scenarios such as split-brain, peer faults, and during software upgrades.

The MLAG pair of switches periodically exchanges a keepalive message on a user configurable interval. If the keepalive message fails to arrive for three consecutive intervals the switches break into two standalone switches. In such case the remaining active switch begins to act as a stand-alone switch and assumes that its previously peering MLAG switch has failed.

To avoid a scenario where failure on the IPL causes both MLAG peers to assume that their peer has failed, a safety mechanism based on UDP packets running via the management plane is maintained and alerts both peers of IPL failure. In such a case of IPL failure, the slave shuts down its interfaces to avoid a split brain scenario and the master becomes a standalone switch.

### 5.8.2 Unicast and Multicast Sync

Unicast and multicast sync is a mechanism which syncs the unicast and multicast FDBs of the MLAG peers. It prevents unicast asymmetric traffic from loading the network with flood traffic and multicast traffic from being processed.

### 5.8.3 MLAG Port Sync

Under normal circumstances, traffic from the IPL cannot pass through the MLAG ports (the IPL is isolated from the MLAG ports). If one of the MLAG links break, the other MLAG switch opens that isolation and allows traffic from its peer through the IPL to flow via the MLAG port which accesses the destination of the fallen link.

### 5.8.4 MLAG Virtual System-MAC

A pair of MLAG switches uses a single virtual system MAC for L2 protocols (such as LACP) operating on the MLAG ports.

The virtual system MAC is automatically computed based on the MLAG VIP name, but can be manually set using the command “`system-mac`”.

MLAG relies on systems to have the same virtual system MAC. Therefore, if a system MAC mismatch is detected, the slave shuts down its interfaces.

### 5.8.5 Upgrading MLAG Pair

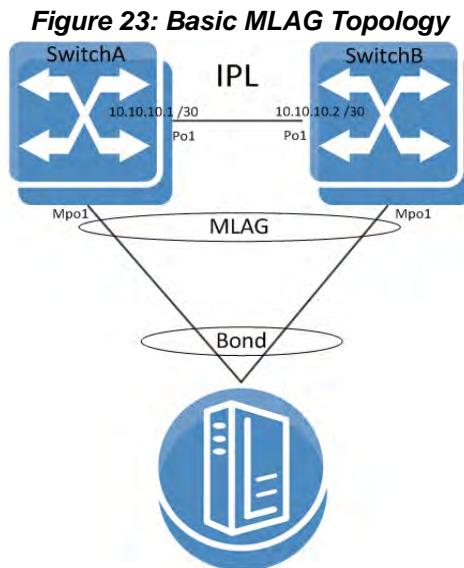
Switches in the same MLAG group must have the same MLNX-OS version.

When peers identify having different versions, they enter an upgrading state in which the slave peer waits for a specific period of time (according to the command “`upgrade-timeout`” on page 765) before closing its ports.

For more information on MLAG upgrade, please see Section 4.4.2, “Upgrading MLNX-OS HA Groups,” on page 230.

### 5.8.6 Configuring MLAG

This section provides a basic example of how to configure two switches and a server in an MLAG setup.



For more advanced configuration options, please refer to the following Mellanox Community post: <https://community.mellanox.com/docs/DOC-2262>.

➤ **To configure L2 MLAG:**

Prerequisites:

- Step 1.** Enable IP routing. Run:

```
switch (config)# ip routing
```

- Step 2.** (Recommended) Enable LACP in the switch. Run:

```
switch (config)# lacp
```

- Step 3.** Enable QoS on the switch to avoid congestion on the IPL port. Run:

```
switch (config)# dcb priority-flow-control enable force
```

- Step 4.** Enable the MLAG protocol commands. Run:

```
switch (config)# protocol mlag
```

Configuring the IPL:

- Step 1.** Create a VLAN for the inter-peer link (IPL) to run on. Run:

```
switch (config)# vlan 4000
switch (config vlan 4000)#

```

- Step 2.** Create a LAG. Run:

```
switch (config)# interface port-channel 1
switch (config interface port-channel 1)#

```

- Step 3.** Map a physical port to the LAG in active mode (LACP). Run:

```
switch (config)# interface ethernet 1/1 channel-group 1 mode active
```

- Step 4.** Set this LAG as an IPL. Run:

```
switch (config interface port-channel 1)# ipl 1
```

- Step 5.** Enable QoS on this specific interface. Run:

```
switch (config interface port-channel 1)# dcb priority-flow-control mode on force
```

- Step 6.** Create a VLAN interface. Run:

```
switch (config)# interface vlan 4000
switch (config interface vlan 4000)#

```

- Step 7.** Set an IP address and netmask for the VLAN interface.

Configure IP address for the IPL link on both switches:

**Note:** The IPL IP address should not be part of the management network, it could be any IP address and subnet that is not in use in the network. This address is not advertised outside the switch.

On SwitchA, run:

```
switch (config interface vlan 4000)# ip address 1.1.1.1 /30
```

On SwitchB, run:

```
switch (config interface vlan 4000)# ip address 1.1.1.2 /30
```

- Step 8.** Map the VLAN interface to be used on the IPL and set the peer IP address (the IP address of the IPL port on the second switch) of the IPL peer port. IPL peer ports must be configured on the same netmask.

On SwitchA, run:

```
switch (config interface vlan 4000)# ipl 1 peer-address 1.1.1.2
```

On SwitchB, run:

```
switch (config interface vlan 4000)# ipl 1 peer-address 1.1.1.1
```

- Step 9.** Configure a virtual IP (VIP) for the MLAG. MLAG VIP (Virtual IP) is important for retrieving peer information.

**Note:** The IP address should be within the subnet of the management interface (mgmt0). Do not use mgmt1. The management network is used for keep-alive messages between the switches. The MLAG domain must be unique name for each MLAG domain. In case you have more than one pair of MLAG switches on the same network, each domain (consist of two switches) should be configured with different name.

On SwitchA, run:

```
switch (config)# mlag-vip my-vip ip 10.234.23.254 /24
```

On SwitchB, run:

```
switch (config)# mlag-vip my-vip
```

- Step 10.** (Optional) Configure a virtual system MAC for the MLAG. Run:

```
switch (config)# mlag system-mac 00:00:5E:00:01:5D
```

#### Creating an MLAG interface:

- Step 1.** Create an MLAG interface for the host. Run:

```
switch (config)# interface mlag-port-channel 1
switch (config interface mlag-port-channel 1)#

```

- Step 2.** Disable STP. Run:

```
switch (config interface mlag-port-channel 1)# spanning-tree port type edge
switch (config interface mlag-port-channel 1)# spanning-tree bpduguard enable
```

- Step 3.** Bind an Ethernet port to the MLAG group. Run:

```
switch (config interface ethernet 1/2)# mlag-channel-group 1 mode on
```

- Step 4.** Create and enable the MLAG interface. Run:

```
switch (config interface mlag-port-channel 1)# no shutdown
```



STP must be disabled (no spanning-tree) on the MLAG switches when there is at least 1 MLAG port-channel connected to a switch and not to a host.

## Enabling MLAG:

### **Step 1.** Enable MLAG. Run:

```
switch [my-vip: master] (config mlag)# no shutdown
```



When running MLAG with L3, VRRP or MAGP must be deployed. For more information, refer to [Section 6.8, “VRRP,” on page 1370](#) or [Section 6.9, “MAGP,” on page 1385](#) respectively.

### ➤ *To verify MLAG configuration:*

#### **Step 1.** Examine MLAG configuration and status. Run:

```
SX2 [mellanox: master] (config)# show mlag
Admin status: Enabled
Operational status: Up
Reload-delay: 1 sec
Keepalive-interval: 30 sec
Upgrade-timeout: 60 min
System-mac: 00:00:5E:00:01:5D

MLAG Ports Configuration Summary:
Configured: 1
Disabled: 0
Enabled: 1

MLAG Ports Status Summary:
Inactive: 0
Active-partial: 0
Active-full: 1

MLAG IPLs Summary:
ID  Group          Vlan      Operational  Local          Peer
    Port-Channel   Interface  State        IP address    IP address
-----
1   Po1           1          Up          10.10.10.1  10.10.10.2

Peers state Summary:
System-id          State  Hostname
-----
F4:52:14:2D:9B:88 Up    <SX2>
F4:52:14:2D:9B:08 Up    SX1
switch [mellanox: master] (config)#

```

**Step 2.** Examine the MLAG summary table. Run:

```
switch [my-vip: master] (config)# show interfaces mlag-port-channel summary
MLAG Port-Channel Flags: D-Down, U-Up
P-Partial UP, S - suspended by MLAG
Port Flags: D - Down, P - Up in port-channel (members)
S - Suspend in port-channel (members), I - Individual
Group
Port-Channel      Type      Local Ports          Peer Ports
(D/P/S/I)          (D/P/S/I)
-----
1 Mpo2(U)        Static    Eth1/2(P)           Eth1/2(P)

switch (config)#

```

**Step 3.** Examine the MLAG statistics. Run:

```
switch [my-vip: master] (config)# show mlag statistics
IPL 1:
Rx Heartbeat : 516
Tx Heartbeat : 516
Rx IGMP tunnel : 0
Tx IGMP tunnel : 0
RX mlag-notification: 0
TX mlag-notification: 0
Rx port-notification : 0
Tx port-notification : 0
Rx FDB sync : 0
Tx FDB sync : 0
RX LACP manager: 1
TX LACP manager: 0
switch (config)#

```

[Enabling L3 Forwarding with User VRF](#)

If you want to use a VRF for IP routing and forwarding on an MLAG topology, it is recommended to configure an additional VLAN interface with the same user VRF context as the non-MLAG L3 interface that has to route through the same physical ports as the IPL. This would allow forwarding L3 traffic through this VLAN interface on the same ports as the IPL.

## 5.8.7 Commands

### protocol mlag

**protocol mlag**  
**no protocol mlag**

Enables MLAG functionality and unhides the MLAG commands.  
The no form of the command hides the MLAG commands and deletes its database.

---

#### Syntax Description

---

**Default** no protocol mlag

**Configuration Mode** Config

**History** 3.3.4500

**Role** admin

**Example**

```
switch (config) # protocol mlag
switch (config) #
```

---

#### Related Commands

---

- Note**
- Running the no form of this command hides MLAG commands.
  - MLAG may be enabled without IP routing, but without IP routing an IPL vLAN interface cannot be configured and thus MLAG does not function.
  - MLAG may be enabled without IGMP snooping, but if IGMP snooping is disabled, multicast FDBs do not sync.
-

## mlag

### mlag

Enters MLAG configuration mode.

<b>Syntax Description</b>	N/A
<b>Default</b>	N/A
<b>Configuration Mode</b>	Config
<b>History</b>	3.3.4500
<b>Role</b>	admin
<b>Example</b>	<pre>switch (config) # mlag switch (config mlag) #</pre>
<b>Related Commands</b>	
<b>Note</b>	

## shutdown

**shutdown**  
**no shutdown**

Disables MLAG.  
The no form of the command enables MLAG.

<b>Syntax Description</b>	N/A
<b>Default</b>	Disabled
<b>Configuration Mode</b>	Config MLAG
<b>History</b>	3.3.4500
<b>Role</b>	admin
<b>Example</b>	<pre>switch (config mlag) # no shutdown switch (config mlag) #</pre>
<b>Related Commands</b>	
<b>Note</b>	This parameter must be similar in all MLAG peers.

## interface mlag-port-channel

```
interface mlag-port-channel <if-number>
no interface mlag-port-channel <if-number>
```

Creates an MLAG interface.

The no form of the command deletes the MLAG interface.

Syntax Description	if-number	Integer. Interface number range: 1-1000.
<b>Default</b>	N/A	
<b>Configuration Mode</b>	Config	
<b>History</b>	3.3.4500	
<b>Role</b>	admin	
<b>Example</b>	<pre>switch (config) # interface mlag-port-channel 1 switch (config interface mlag-port-channel 1) #</pre>	
<b>Related Commands</b>		
<b>Note</b>	<ul style="list-style-type: none"><li>• The maximum number of interfaces is 64.</li><li>• The default Admin state is disabled.</li><li>• Range configuration is possible on this interface.</li><li>• This interface number must be the same in all the MLAG switches.</li></ul>	

**ipl**

**ipl <ipl-id>**  
**no ipl <ipl-id>**

Sets this LAG as an IPL port.

The no form of the command resets this LAG as regular LAG.

<b>Syntax Description</b>	ipl-id	IPL ID. Only “1” IPL port is supported.
<b>Default</b>	no ipl	
<b>Configuration Mode</b>	Config Interface Port Channel	
<b>History</b>	3.3.4500	
<b>Role</b>	admin	
<b>Example</b>	switch (config interface port-channel 1)# ipl 1	
<b>Related Commands</b>		
<b>Note</b>	<ul style="list-style-type: none"><li>If a LAG is set as IPL, only the commands “[no] shutdown”, “no ipl” and “no interface port-channel” become applicable.</li><li>A LAG interface set as IPL must have default LAG configuration, otherwise the set is rejected. Force option can be used.</li></ul>	

## ipl peer-address

```
ipl <ipl-id> peer-address <IP-Address>
no ipl <ipl-id>
```

Maps a VLAN interface to be used for an IPL LAG and sets the peer IP address of the IPL peer port.

The no form of the command deletes a peer IPL LAG and unbinds this VLAN interface from the IPL function.

<b>Syntax Description</b>	ipl-id IP-Address	IPL ID. Only “1” IPL port is supported. IPv4 address.
<b>Default</b>	N/A	
<b>Configuration Mode</b>	Config Interface VLAN	
<b>History</b>	3.3.4500	
<b>Role</b>	admin	
<b>Example</b>		<pre>switch (config interface vlan 1)# ipl 1 peer-address 10.10.10.10 switch (config interface vlan 1)#{/pre}</pre>
<b>Related Commands</b>		
<b>Note</b>		<ul style="list-style-type: none"><li>• The subnet mask is the same subnet mask of the VLAN interface.</li><li>• This VLAN interface should be used for IPL only.</li></ul>

## keep-alive-interval

**keep-alive-interval <value>**  
**no keep-alive-interval**

Configures the interval during which keep-alive messages are issued between the MLAG switches.

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

<b>Syntax Description</b>	value	Time in seconds. Range: 1-300.
<b>Default</b>	1 second	
<b>Configuration Mode</b>	Config MLAG	
<b>History</b>	3.3.4500	
<b>Role</b>	admin	
<b>Example</b>	<pre>switch (config mlag) # keep-alive-interval 1 switch (config mlag) #</pre>	
<b>Related Commands</b>		
<b>Note</b>	This parameter must be similar in all MLAG peers.	

## mlag-channel-group mode

```
mlag-channel-group <if-number> mode {on | active | passive}  
no mlag-channel-group
```

Binds an Ethernet port to the MLAG LAG.  
The no form of the command deletes the binding.

<b>Syntax Description</b>	if-number	Integer. Interface number range: 1-1000.
	on	Binds to static MLAG.
	active	Sets MLAG LAG in LACP active mode.
	passive	Sets MLAG LAG in LACP passive mode.
<b>Default</b>	N/A	
<b>Configuration Mode</b>	Config Interface Ethernet	
<b>History</b>	3.3.4500	
<b>Role</b>	admin	
<b>Example</b>	<pre>switch (config interface ethernet 1/1)# mlag-channel-group 1 mode on switch (config interface ethernet 1/1)#{/pre}</pre>	
<b>Related Commands</b>		
<b>Note</b>		

## mlag-vip

**mlag-vip <domain-name> ip [<ip-address> {<masklen> | netmask} [force]]**  
**no mlag-vip**

Sets the VIP domain and IP address for MLAG.

The no form of the command deletes the VIP domain and IP address.

Syntax Description	domain-name	MLAG group name
	<ip-address>	IP address
	<masklen>	Format example: /24. Note that a space is required between the IP address and the mask.
	<netmask>	Format example: 255.255.255.0. Note that a space is required between the IP address and the mask.
	force	Forces the IP address if another IP is already configured.
<b>Default</b>	N/A	
<b>Configuration Mode</b>	Config	
<b>History</b>	3.3.4500	
<b>Role</b>	admin	
<b>Example</b>	<pre>switch (config)# mlag-vip my-mlag-domain ip 10.10.10.254/24 switch (config)#</pre>	
<b>Related Commands</b>		
<b>Note</b>	<ul style="list-style-type: none"> <li>This IP address must be configured in one of the MLAG switches and must be in the box management subnet.</li> <li>Other switches in the MLAG must join the same domain name.</li> </ul>	

## reload-delay

**reload-delay <value>**  
**no reload-delay**

Specifies the amount of time that MLAG ports are disabled after system reboot.  
The no form of the command resets this parameter to its default value.

Syntax Description	value	Time in seconds. Range: 0-300.
<b>Default</b>	30 seconds	
<b>Configuration Mode</b>	Config MLAG	
<b>History</b>	3.3.4500	
<b>Role</b>	admin	
<b>Example</b>		<pre>switch (config mlag) # reload-delay 30 switch (config mlag) #</pre>
<b>Related Commands</b>		
<b>Note</b>	<ul style="list-style-type: none"><li>This interval allows the switch to learn the IPL topology to identify the master and sync the MAC address before opening the MLAG ports.</li><li>This parameter must be similar in all MLAG peers.</li></ul>	

## system-mac

```
system-mac <virtual-mac>
no system-mac <virtual-mac>
```

Configures virtual system MAC.

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

Syntax Description	virtual-mac	MAC address
<b>Default</b>	Default is calculated according to the MLAG-VIP name, using the base MAC as VRRP MAC prefix (00:00:5E:00:01:xx) with the suffix hashed from the mlag-vip name 0...255.	
<b>Configuration Mode</b>	Config MLAG	
<b>History</b>	3.4.2008	
<b>Role</b>	admin	
<b>Example</b>	<pre>switch (config mlag) # system-mac 00:00:5E:00:01:5D switch (config mlag) #</pre>	
<b>Related Commands</b>		
<b>Note</b>	This parameter must be configured the same in all MLAG peers.	

## upgrade-timeout

**upgrade-timeout <time>**  
**no upgrade-timeout**

Configures the time period during which an MLAG slave keeps its ports active while in upgrading state.

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

<b>Syntax Description</b>	time	Time in minutes. Range: 0-120 minutes.
<b>Default</b>	60	
<b>Configuration Mode</b>	Config MLAG	
<b>History</b>	3.4.2008	
<b>Role</b>	admin	
<b>Example</b>	<pre>switch (config mlag) # upgrade-timeout 60 switch (config mlag) #</pre>	
<b>Related Commands</b>		
<b>Note</b>	This parameter must be configured the same in all MLAG peers.	

## show mlag

### show mlag

Displays MLAG configuration and status.

<b>Syntax Description</b>	N/A	
<b>Default</b>	N/A	
<b>Configuration Mode</b>	Any Command Mode	
<b>History</b>	3.3.4500	
	3.3.5006	Updated example
	3.4.2008	Updated example with system MAC and upgrade timeout
	3.6.5000	Added note
<b>Role</b>	admin	
<b>Example</b>	<pre> SX2 [mellanox: master] (config)# show mlag Admin status: Enabled Operational status: Up Reload-delay: 1 sec Keepalive-interval: 30 sec Upgrade-timeout: 60 min System-mac: 00:00:5E:00:01:5D  MLAG Ports Configuration Summary: Configured: 1 Disabled: 0 Enabled: 1  MLAG Ports Status Summary: Inactive: 0 Active-partial: 0 Active-full: 1  MLAG IPLS Summary: ID      Group          Vlan       Operational   Local           Peer         Port-Channel    Interface   State         IP address     IP address ----- 1       Po1            1          Up           10.10.10.1   10.10.10.2  MLAG Members Summary: System-id          State   Hostname ----- F4:52:14:2D:9B:88  Up     &lt;SX2&gt; F4:52:14:2D:9B:08  Up     SX1 SX2 [mellanox: master] (config)# </pre>	

---

### Related Commands

**Note**

If run in the middle of an upgrade, the following message will appear in the output:  
\*Upgrading\* <hostname> --> \*Cluster upgrade in progress\*

---

## show mlag-vip

### show mlag-vip

Displays MLAG VIP configuration and status.

<b>Syntax Description</b>	N/A
<b>Default</b>	N/A
<b>Configuration Mode</b>	Any Command Mode
<b>History</b>	3.3.4500
<b>Role</b>	admin
<b>Example</b>	<pre>switch (config)# show mlag-vip MLAG VIP ===== MLAG group name: my-mlag-group MLAG VIP address: 1.1.1.1/30 Active nodes: 2        Hostname          VIP-State        IP Address -----+-----+-----+ SwitchA           master       10.10.10.1 SwitchB           standby     10.10.10.2 switch (config)#+</pre>
<b>Related Commands</b>	
<b>Note</b>	

## show interfaces mlag-port-channel

**show interfaces mlag-port-channel <if-number>**

Displays the MLAG LAG configuration and status.

<b>Syntax Description</b>	N/A
<b>Default</b>	N/A
<b>Configuration Mode</b>	Any Command Mode
<b>History</b>	3.3.4500 3.6.1002                          Added “error packets” counter to Tx 3.6.5000                          Added telemetry to output
<b>Role</b>	admin
<b>Example</b>	<pre>switch (config)# show interfaces mlag-port-channel 1 Mpo1     Admin state: Enabled     Operational state: Down     Description: N\A     Mac address: 00:00:00:00:00:00     MTU: 1500 bytes (Maximum packet size 1522 bytes)     Flow-control: receive off send off     Actual speed: 0 Gbps     Width reduction mode: disabled     Switchport mode: access     Telemetry sampling: Disabled   TCs: N\A     Telemetry threshold:Enabled   TCs: 3 (ucast), 1 (mcast)     Telemetry threshold level: 900     Last clearing of "show interface" counters : Never     60 seconds ingress rate: 0 bits/sec, 0 bytes/sec, 0 packets/sec     60 seconds egress rate: 0 bits/sec, 0 bytes/sec, 0 packets/sec Rx     0          packets     0          unicast packets     0          multicast packets     0          broadcast packets     0          bytes     0          error packets     0          discard packets Tx     0          packets     0          unicast packets     0          multicast packets     0          broadcast packets     0          bytes     0          error packets     0          discard packets</pre>

---

**Related Commands**

---

**Note**

---

## show interfaces mlag-port-channel counters

**show interfaces mlag-port-channel <if-number> counters**

Displays the extended counters for the interface.

<b>Syntax Description</b>	N/A
<b>Default</b>	N/A
<b>Configuration Mode</b>	Any Command Mode
<b>History</b>	3.6.1002
<b>Role</b>	admin
<b>Example</b>	<pre>switch (config)# show interfaces mlag-port-channel 3 counters  Rx  12          packets  0          unicast packets  12          multicast packets  0          broadcast packets  2700        bytes  0          packets of 64 bytes  0          packets of 65-127 bytes  12         packets of 128-255 bytes  0          packets of 256-511 bytes  0          packets of 512-1023 bytes  0          packets of 1024-1518 bytes  0          packets Jumbo  0          error packets  0          discard packets  0          fcs errors  0          undersize packets  0          oversize packets  0          pause packets  0          unknown control opcode  0          symbol errors  Tx  0          packets  0          unicast packets  0          multicast packets  0          broadcast packets  152100000000  bytes  100000000    error packets  0          discard packets  0          pause packets  switch (config)# </pre>

---

### Related Commands

---

### Note

## **show interfaces mlag-port-channel summary**

**show interfaces mlag-port-channel summary**

Displays MLAG summary table.

## show mlag statistics

### show mlag statistics

Displays the MLAG IPL counters.

<b>Syntax Description</b>	N/A
<b>Default</b>	N/A
<b>Configuration Mode</b>	Any Command Mode
<b>History</b>	3.3.4500 3.4.0000 Updated example
<b>Role</b>	admin
<b>Example</b>	<pre>switch (config)# show mlag statistics IPL 1: RX Heartbeat: 439908 TX Heartbeat: 439951 RX IGMP tunnel: 0 TX IGMP tunnel: 1 RX mlag-notification: 0 TX mlag-notification: 12 RX port-notification: 56 TX port-notification: 73 RX FDB sync: 424 TX FDB sync: 778 RX LACP manager: 38 TX LACP manager: 21</pre>
<b>Related Commands</b>	
<b>Note</b>	

## 5.9 QinQ

A QinQ VLAN tunnel enables a service provider (SP) to segregate the traffic of different customers in their infrastructure, while still giving the customer a full range of VLANs for their internal use by adding a second 802.1Q VLAN tag to an already tagged frame.

So let us assume for example that an SP exists which needs to offer L2 connectivity to two corporations, “X” and “Y”, that have campuses located in both “A”, “B”. All campuses run Ethernet LANs, and the customers intend to connect through the SP’s L2 VPN network so that their campuses are in the same LAN (L2 network). Hence, it would be desirable for “X”, “Y” to have a single LAN each in both “A”, “B” which could easily exceed the VLAN limit of 4096 of the 802.1Q specification.

### 5.9.1 QinQ Operation Modes

QinQ can be enabled on a port or according to predefined conditions.



C-VLAN is the VLAN tag assigned to the ingress traffic of a QinQ-enabled interface.  
S-VLAN is the VLAN tag assigned to the egress traffic of a QinQ-enabled interface.

- ACL-mode: Adding and removing S-VLAN is determined by an ACL-dependent action
- Port-mode: All ingress traffic to a specific QinQ-enabled interface is tagged with an additional VLAN 802.1Q tag (also known as S-VLAN). The S-VLAN ID is equal to that interface’s PVID (access VLAN).

The S-VLAN tag is added regardless of whether the traffic is tagged or untagged. Traffic coming out from this port, has the S-VLAN stripped from it.

### 5.9.2 Configuring QinQ

➤ *To configure QinQ:*

**Step 1.** Create the C-VLAN. Run:

```
switch (config) # vlan 200
switch (config vlan 200) # exit
```

**Step 2.** Enter the configuration mode of an Ethernet, LAG, or MLAG interface. Run:

```
switch (config) # interface port-channel 100
```

**Step 3.** Change the switchport mode of the interface to enable QinQ. Run:

```
switch (config interface port-channel 100) # switchport mode dot1q-tunnel
```

**Step 4.** Change its port VLAN ID (PVID). This configures the S-VLAN. Run:

```
switch (config interface port-channel 100) # switchport access vlan 200
```

**Step 5.** Verify the configuration. Run:

```
switch (config interface port-channel 100) # show interface port-channel 100
```

```
Po100
```

```

Admin state: Enabled
Operational state: Up
Description: N\A
Mac address: 00:00:00:00:00:00
    MTU: 1500 bytes(Maximum packet size 1522 bytes)
    lacp-individual mode: Disabled
    Flow-control: receive off send off
    Actual speed: 1 X 40 Gbps
    Width reduction mode: disabled
    Switchport mode: dot1q-tunnel
    QoS mode: uniform
    MAC learning mode: Enabled
    Last clearing of "show interface" counters : Never
    60 seconds ingress rate: 0 bits/sec, 0 bytes/sec, 0 packets/sec
    60 seconds egress rate: 0 bits/sec, 0 bytes/sec, 0 packets/sec

Rx
0 packets
0 unicast packets
0 multicast packets
0 broadcast packets
0 bytes
0 error packets
0 discard packets

Tx
0 packets
0 unicast packets
0 multicast packets
0 broadcast packets
0 bytes
0 discard packets
switch (config interface port-channel 100) #

```

**Step 6.** Verify the configuration. Run:

```

switch (config interface port-channel 100) # show interfaces switchport
Interface      Mode       Access vlan     Allowed vlans
-----
Eth1/1         access     1
Eth1/2         access     1
Eth1/3         access     1
Eth1/4         access     1
Eth1/5         access     1
Eth1/6         access     1
...
Eth1/27        access     1
Eth1/33        access     1
Eth1/34        access     1
Eth1/35        access     1
Eth1/36        access     1
Po400          dot1q-tunnel 200

```

### 5.9.3 Commands

#### **switchport dot1q-tunnel qos-mode**

**switchport dot1q-tunnel qos-mode {pipe | uniform}**  
**no switchport dot1q-tunnel qos-mode**

Assigns QoS to the service provider's traffic.

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

<b>Syntax Description</b>	pipe	Gives the service provider's traffic the same QoS as the customer's traffic
	uniform	Gives the service provider's traffic QoS 0
<b>Default</b>	pipe	
<b>Configuration Mode</b>	Config Interface Ethernet Config Interface Port Channel Config Interface MLAG Port Channel	
<b>History</b>	3.4.3000	
<b>Role</b>	admin	
<b>Example</b>	<pre>switch (config interface ethernet 1/1) # switchport dot1q-tunnel qos- mode uniform switch (config interface ethernet 1/1) #</pre>	
<b>Related Commands</b>	show vlan show interfaces switchport switchport access vlan switchport [trunk   hybrid] allowed-vlan vlan	
<b>Note</b>		

## 5.10 Access Control List

An Access Control List (ACL) is a list of permissions attached to an object, to filter or match switches packets. When the pattern is matched at the hardware lookup engine, a specified action (e.g. permit/deny) is applied. The rule fields represent flow characteristics such as source and destination addresses, protocol and VLAN ID.

ACL support currently allows actions of *permit* or *deny* rules, and supports only ingress direction. ACL search pattern can be taken from either L2 or L3 fields, e.g L2/L3 source and destination addresses, protocol, VLAN ID and priority or TCP port.

### 5.10.1 Configuring Access Control List

Access Control List (ACL) is configured by the user and is applied to a port once the ACL search engine matches search criteria with a received packet.

➤ **To configure ACL:**

**Step 1.** Log in as admin.

**Step 2.** Enter config mode. Run:

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

**Step 3.** Create a MAC / IPv4 ACL (access-list) entity.

```
switch (config) mac access-list mac-acl
switch (config mac access-list mac-acl) #
```

**Step 4.** Add a MAC / IP rules to the appropriate access-list.

```
switch (config mac access-list mac-acl) seq-number 10 deny 0a:0a:0a:0a:0a:0a mask
ff:ff:ff:ff:ff:ff any vlan 6 cos 2 protocol 80
switch (config mac access-list mac-acl) #
```

**Step 5.** Bind the created access-list to an interface (slot/port or port-channel).

```
switch (config)
switch (config) # interface ethernet 1/1
switch (config interface ethernet 1/1) # mac port access-group mac-acl
```

### 5.10.2 ACL Actions

An ACL action is a set of actions can be activated in case the packet hits the ACL rule.

➤ **To modify the VLAN tag of the egress traffic as part of the ACL “permit” rule:**

**Step 1.** Create access-list action profile:

**Step 1a.** Create an action access-list profile using the command `access-list action <action-profile-name>`.

**Step 1b.** Add rule to map a VLAN using the command `vlan-map <vlan-id>` within the action profile configuration mode.

**Step 1c.** Add action on a rule to strip the VLAN from a packet using the command `vlan-pop` within the action profile configuration mode.

**Step 1d.** Add action on a rule to append a VLAN to a packet using the command `vlan-push` within the action profile configuration mode.

**Step 2.** Create an access-list and bind the action rule:

- a.Create an access-list profile using the command  
`{ ipv4/ipv4-udk/ipv6/mac/mac-udk } access-list`.
- b.Add access list rule using the command `deny/permit (action <action profile name>)`.

**Step 3.** Bind the access-list to an interface using the command

`{ ipv4/ipv4-udk/ipv6/mac/mac-udk } port access-group`.

Create an action profile and add vlan mapping action:

```
switch (config)# access-list action my-action
switch (config access-list action my-action)# vlan-map 20
switch (config access-list action my-action)# exit
```

Create an access list and bind rules:

```
switch (config)# mac access-list my-list
switch (config mac access-list my-list)# permit any any action my-action
switch (config mac access-list my-list)# exit
```

Bind an access-list to a port:

```
switch (config)# interface ethernet 1/1
switch (config interface ethernet 1/1)# mac access-list my-list
```

### 5.10.3 ACL Logging

A strong insight into the system is given by ACL logging. ACLs can log packets that pass through the switch, so the flows can later be analyzed.

A packet that hits an ACL with a log clause is passed to the logger. The logger writes the partial header of the packet (L2 or L3) to the syslog, with a timestamp and some additional information such as ingress interface and the VLAN to which the packet belongs.

To protect the system memory, a limited number of flows are collected for each time interval. If the number of flows for a specific time interval is exceeded, then no packets are logged for this time interval.

To further protect the system, a rate-limiter controls the number of packets passed to the CPU.



Only packets traversing the switch are logged. Packets that are passed to the CPU are not.

## 5.10.4 ACL Capability Summary

Table 54 summarizes the ACL capabilities supported by MLNX-OS®.

**Table 54 - Summary of ACL Capability**

ACL Table	Policy	Protocol	Keys	Actions	Supported Interfaces (Ingress Bind Point Only)	Scale
MAC	Permit Deny Remark <sup>1</sup>	N/A	DST MAC (with mask) SRC MAC (with mask) Protocol CoS VLAN-ID VLAN-group	VLAN map VLAN pop VLAN push Counter per rule Shared counter to rules Log	L2 port LAG MLAG RIF VLAN interface	18K
IPv4	Permit Deny Remark <sup>1</sup>	IP	DST IP (incl. subnets) SRC IP (incl. subnets)	VLAN map VLAN pop VLAN push Counter per rule Shared counter to rules Log	L2 port LAG MLAG RIF VLAN interface	9K
		TCP	DST IP (incl. subnets) SRC IP (incl. subnets) L4 DST port (incl. range) L4 SRC port (incl. range) TCP flags Establish flow			
		UDP	DST IP (incl. subnets) SRC IP (incl. subnets) L4 DST port (incl. range) L4 SRC port (incl. range)			
		TCP-UDP	DST IP (incl. subnets) SRC IP (incl. subnets) L4 DST port (incl. range) L4 SRC port (incl. range)			
		ICMP	DST IP (incl. subnets) SRC IP (incl. subnets) Code Type			
IPv6	Permit Deny Remark <sup>1</sup>	IPv6	DST IPv6 (incl. subnets) SRC IPv6 (incl. subnets)	VLAN map VLAN pop VLAN push Counter per rule Shared counter to rules Log	L2 port LAG MLAG RIF VLAN interface	6K
		TCP	DST IPv6 (incl. subnets) SRC IPv6 (incl. subnets) L4 DST port (incl. range) L4 SRC port (incl. range) TCP flags Establish flow			
		UDP	DST IPv6 (incl. subnets) SRC IPv6 (incl. subnets) L4 DST port (incl. range) L4 SRC port (incl. range)			
		TCP-UDP	DST IPv6 (incl. subnets) SRC IPv6 (incl. subnets) L4 DST port (incl. range) L4 SRC port (incl. range)			
		ICMPv6	DST IPv6 (incl. subnets) SRC IPv6 (incl. subnets) Code Type			

**Table 54 - Summary of ACL Capability (Continued)**

ACL Table	Policy	Protocol	Keys	Actions	Supported Interfaces (Ingress Bind Point Only)	Scale
MAC-UDK	Permit Deny Remark <sup>1</sup>	N/A	DST MAC (with mask) SRC MAC (with mask) Protocol CoS VLAN-ID VLAN-group UDK1 (up to 4 bytes) UDK2 (up to 4 bytes) UDK3 (up to 4 bytes) UDK4 (up to 4 bytes)	VLAN map VLAN pop VLAN push Counter per rule Shared counter to rules Log	L2 port LAG MLAG RIF VLAN interface	9K
IPv4-UDK	Permit Deny Remark <sup>1</sup>	IP	DST IP (incl. subnets) SRC IP (incl. subnets) UDK1 (up to 4 bytes) UDK2 (up to 4 bytes) UDK3 (up to 4 bytes) UDK4 (up to 4 bytes)	VLAN map VLAN pop VLAN push Counter per rule Shared counter to rules Log	L2 port LAG MLAG RIF VLAN interface	6K
		TCP	DST IP (incl. subnets) SRC IP (incl. subnets) L4 DST port (incl. range) L4 SRC port (incl. range) TCP flags Establish flow UDK1 (up to 4 bytes) UDK2 (up to 4 bytes) UDK3 (up to 4 bytes) UDK4 (up to 4 bytes)			
		UDP	DST IP (incl. subnets) SRC IP (incl. subnets) L4 DST port (incl. range) L4 SRC port (incl. range) UDK1 (up to 4 bytes) UDK2 (up to 4 bytes) UDK3 (up to 4 bytes) UDK4 (up to 4 bytes)			
		TCP-UDP	DST IP (incl. subnets) SRC IP (incl. subnets) L4 DST port (incl. range) L4 SRC port (incl. range) UDK1 (up to 4 bytes) UDK2 (up to 4 bytes) UDK3 (up to 4 bytes) UDK4 (up to 4 bytes)			
		ICMP	DST IP (incl. subnets) SRC IP (incl. subnets) Code Type UDK1 (up to 4 bytes) UDK2 (up to 4 bytes) UDK3 (up to 4 bytes) UDK4 (up to 4 bytes)			

1. No keys &amp; actions

## 5.10.5 Commands

### {ipv4/ipv6/mac/ipv4-udk/mac-udk} access-list

**{ipv4 | ipv6 | mac | ipv4-udk | mac-udk} access-list <acl-name>**  
**no {ipv4 | ipv6 | mac | ipv4-udk | mac-udk} access-list <acl-name>**

Creates an ACL table and enters its configuration mode.  
The no form of the command deletes the ACL table.

<b>Syntax Description</b>	ipv4   mac	IPv4 or MAC – access list
	acl-name	User-defined string for the ACL
<b>Default</b>	No ACL available by default.	
<b>Configuration Mode</b>	Config	
<b>History</b>	3.1.1400	
	3.6.5000	Added ipv6, ipv4-udk, and mac-udk parameters
<b>Role</b>	admin	
<b>Example</b>	<pre>switch (config)# mac access-list my-mac-list switch (config mac access-list my-mac-list)# </pre>	
<b>Related Commands</b>	ipv4/port access-group	
<b>Note</b>	<ul style="list-style-type: none"> <li>• Each table has its own set of predefine keys</li> <li>• The mac-udk and ipv4-udk options add an extra UDK to the standard MAC and IPv4 tables</li> <li>• When a new access-list is created, its default bind port is L2 port</li> </ul>	

## bind-point rif

**bind-point rif**  
**no bind-point rif**

Changes the ACL table bind point from L2 port mode to L3 port.  
The no form of the command resets this parameter to its default.

<b>Syntax Description</b>	N/A
<b>Default</b>	L2 port
<b>Configuration Mode</b>	Config MAC Access-List
<b>History</b>	3.6.5000
<b>Role</b>	admin
<b>Example</b>	<pre>switch (config mac access-list my-mac-list)# bind-point rif</pre>
<b>Related Commands</b>	ipv4/ipv6/mac/ipv4-udk/mac-udk access-list
<b>Note</b>	<ul style="list-style-type: none"><li>The bind point may only be changed when an ACL table is empty (no rules) and unbound</li><li>This command is used to attach ACLs to interface VLANs only</li></ul>

## remark

```
[<seq-number>] remark <string>
no [<seq-number>] remark <string>
```

Creates a remark rule from an ACL table.

The no form of the command deletes a remark rule from an ACL table.

<b>Syntax Description</b>	N/A
<b>Default</b>	N/A
<b>Configuration Mode</b>	Config MAC Access-List
<b>History</b>	3.6.5000
<b>Role</b>	admin
<b>Example</b>	<pre>switch (config mac access-list my-mac-list)# remark "1st group"</pre>
<b>Related Commands</b>	<pre>ipv4/ipv6/mac/ipv4-udk/mac-udk access-list</pre>
<b>Note</b>	<ul style="list-style-type: none"><li>• The remark rule has a sequence number like standard rules and it can be displayed when showing all rules of ACL table</li><li>• This rule has no effect on traffic and it is only for management purposes</li></ul>

## shared-counter

```
shared-counter <counter-name>
no shared-counter <counter-name>
```

Creates a shared counter.

The no form of the command deletes a shared counter.

Syntax Description	counter-name	Shared counter name
<b>Default</b>	N/A	
<b>Configuration Mode</b>	Config MAC Access-List	
<b>History</b>	3.6.5000	
<b>Role</b>	admin	
<b>Example</b>	switch (config mac access-list my-mac-list)# shared-counter myCounter	
<b>Related Commands</b>	ipv4/ipv6/mac/ipv4-udk/mac-udk access-list	
<b>Note</b>	<ul style="list-style-type: none"><li>When creating a new shared counter, it is created only in the scope of the ACL table it has been initially created on and cannot be shared across multiple ACL tables</li><li>A shared counter cannot be deleted when attached to rules</li></ul>	

## clear shared-counters

**clear shared-counters [<counter-name>]**

Resets all shared counters in ACL table or a specific shared counter.

<b>Syntax Description</b>	counter-name	Shared counter name
<b>Default</b>	N/A	
<b>Configuration Mode</b>	Config MAC Access-List	
<b>History</b>	3.6.5000	
<b>Role</b>	admin	
<b>Example</b>	switch (config mac access-list my-mac-list)# clear shared-counters	
<b>Related Commands</b>	ipv4/ipv6/mac/ipv4-udk/mac-udk access-list shared-counter	
<b>Note</b>		

## clear counters

**clear counters [<seq-number>]**

Resets all counters (including shared counters) in ACL table or a specific counter.

<b>Syntax Description</b>	seq-number	The sequence number of the rule whose counter to reset
<b>Default</b>	N/A	
<b>Configuration Mode</b>	Config MAC Access-List	
<b>History</b>	3.6.5000	
<b>Role</b>	admin	
<b>Example</b>	switch (config mac access-list my-mac-list)# clear counters 10	
<b>Related Commands</b>	ipv4/ipv6/mac/ipv4-udk/mac-udk access-list shared-counter	
<b>Note</b>		

## {ipv4/ipv6/mac/ipv4-udk/mac-udk} access-list clear counters

**{ipv4 | ipv6 | mac | ipv4-udk | mac-udk} access-list clear counters**

Resets all counters (including shared counters) on all ACL tables of the same type.

<b>Syntax Description</b>	N/A
<b>Default</b>	N/A
<b>Configuration Mode</b>	Config MAC Access-List
<b>History</b>	3.6.5000
<b>Role</b>	admin
<b>Example</b>	<pre>switch (config)# ipv4 access-list clear counters</pre>
<b>Related Commands</b>	ipv4/ipv6/mac/ipv4-udk/mac-udk access-list shared-counter
<b>Note</b>	

## {ipv4/ipv6/mac/ipv4-udk/mac-udk} port access-group

**{ipv4 | ipv6 | mac | ipv4-udk | mac-udk} port access-group <acl-name>**  
**no {ipv4 | ipv6 | mac | ipv4-udk | mac-udk} port access-group <acl-name>**

Binds an ACL to the interface.

The no form of the command unbinds the ACL from the interface.

<b>Syntax Description</b>	ipv4   mac	IPv4 or MAC – access list
	acl-name	ACL name
<b>Default</b>	No ACL is bind by default.	
<b>Configuration Mode</b>	Config Interface Ethernet Config Interface Port Channel Config Interface MLAG Port Channel	
<b>History</b>	3.1.1400  3.3.4500  3.6.5000	Added MLAG port-channel configuration mode  Added new parameters
<b>Role</b>	admin	
<b>Example</b>	<pre>switch (config interface ethernet 1/1) # mac port access-group my-list switch (config interface ethernet 1/1) #</pre>	
<b>Related Commands</b>	{ipv4/ipv4-udk/ipv6/mac/mac-udk} access-list	
<b>Note</b>	The access control list should be defined prior to the binding action.	

## deny/permit (MAC ACL rule)

```
[seq-number <sequence-number>] {permit | deny} ip {<source-mac> mask
<mac_mask> | any} {<dest-mac> mask <mac_mask> | any} [protocol <proto-
col_num>] [cos <cos>] [vlan <vlan_id>] [vlan-mask <vlan-mask>] [action
<action-name>] [log] [counter | shared-counter <name>]
no <sequence-number>
```

Creates a rule for MAC ACL.

The no form of the command deletes a rule from the MAC ACL.

<b>Syntax Description</b>	sequence-number	Optional parameter to set a specific sequence number for the rule. Range is:1-65535.								
	deny	Drop all matching traffic								
	permit	Allow matching traffic to pass								
	<source-mac> mask <mac_mask>   any	Sets source MAC and optionally sets a mask for that MAC. The “any” option will cause the rule not to check the source MAC.								
	<dest-mac> mask <mac_mask>   any	Sets destination MAC and optionally sets a mask for that MAC. The “any” option will cause the rule not to check the destination MAC.								
	protocol	Sets the Ethertype filed value from the MAC address. Range: 0x0000-0xffff.								
	cos	Sets the COS (priority bit) field. Range is: 0-7.								
	vlan <vlan_id>	Sets the VLAN ID field. Range is 1-4094.								
	vlan-mask <vlan-mask>	Sets VLAN group. Range: 0x0000-0x0FFF.								
	action	Action name (free string)								
	log	Enable the log option								
	counter	Attach a unique counter to rule								
	shared-counter	Attach a predefined shared-counter to rule								
<b>Default</b>	No rule is added by default to access control list. Default sequence number is in multiple of 10.									
<b>Configuration Mode</b>	Config MAC ACL									
<b>History</b>	<table> <tr> <td>3.1.1400</td> <td></td> </tr> <tr> <td>3.3.4500</td> <td>Added vlan-mask parameter</td> </tr> <tr> <td>3.5.1000</td> <td>Updated seq-number parameter</td> </tr> <tr> <td>3.6.5000</td> <td>Added log, counter, and shared-counter parameters</td> </tr> </table>		3.1.1400		3.3.4500	Added vlan-mask parameter	3.5.1000	Updated seq-number parameter	3.6.5000	Added log, counter, and shared-counter parameters
3.1.1400										
3.3.4500	Added vlan-mask parameter									
3.5.1000	Updated seq-number parameter									
3.6.5000	Added log, counter, and shared-counter parameters									

<b>Role</b>	admin
<b>Example</b>	<pre>switch (config mac access-list my-list) # seq-number 10 deny 0a:0a:0a:0a:0a:0a mask ff:ff:ff:ff:ff:ff any vlan 6 cos 2 protocol 80 switch (config mac access-list my-list) #</pre>
<b>Related Commands</b>	{ipv4/ipv4-udk/ipv6/mac/mac-udk} access-list {ipv4/ipv4-udk/ipv6/mac/mac-udk} port access-group
<b>Note</b>	VLAN and VLAN group cannot be used in the same command

## deny/permit (IPv4 ACL rule)

```
[seq-number <sequence-number>] {permit | deny} ip {<source-ip> mask <ip> |  

[any]} {<dest-ip> mask <ip> | [any]} [action <action-id>] [log] [counter | shared-  

counter <name>]  

no <sequence-number>
```

Creates a rule for IPv4 ACL.

The no form of the command deletes a rule from the IPv4 ACL.

<b>Syntax Description</b>	sequence-number	Optional parameter to set a specific sequence number for the rule. Range is: 1-65535.
	deny	Drop all matching traffic
	permit	Allow matching traffic to pass
	{any   <source-ip> mask <ip>}	Sets source IP and optionally sets a mask for that IP address. The “any” option causes the rule to not check the source IP. Range: 0-255.
	{any   <destination-ip> mask <ip>}	Sets destination IP and optionally sets a mask for that MAC. The “any” option causes the rule to not check the destination MAC.
	action	Action needs to be defined before attaching to rule
	log	Enable the log option
	counter	Attach a unique counter to rule
	shared-counter	Attach a predefined shared-counter to rule
<b>Default</b>	No rule is added by default to access control list. Default sequence number is in multiple of 10.	
<b>Configuration Mode</b>	Config IPv4 ACL	
<b>History</b>	3.1.1400 3.3.4302                  Updated syntax description of mask <ip> parameter 3.5.1000                  Updated seq-number parameter 3.6.5000                  Added log, counter, and shared-counter parameters	
<b>Role</b>	admin	

<b>Example</b>	<pre>switch (config ipv4 access-list my-list) # deny ip any any action act shared-counter</pre>
<b>Related Commands</b>	<pre>{ipv4/ipv4-udk/ipv6/mac/mac-udk} access-list {ipv4/ipv4-udk/ipv6/mac/mac-udk} port access-group</pre>
<b>Note</b>	<ul style="list-style-type: none"><li>• User cannot attach a shared counter defined on a different ACL table</li><li>• The parameter shared-counter must be defined before attaching it to the scope of the ACL table</li></ul>

## deny/permit (IPv4 TCP ACL rule)

```
[seq-number <sequence-number>] {deny | permit} tcp {<source-ip> mask <ip> | any} {<dest-ip> mask <ip> | any} [src-port <src-port> | eq-source <src-port> | src-port-range <from> <to>] [dest-port <dest-port> | eq-destination <dest-port> | dest-port-range <from> <to>] [action <action-id>] [established | [ack {0 | 1}] | [urg {0 | 1}] | [rst {0 | 1}] | [syn {0 | 1}] | [fin {0 | 1}] | [psh {0 | 1}]] | [log] | [counter] | shared-counter <name>]
no <sequence-number>
```

Creates a rule for IPv4 TCP ACL.

The no form of the command deletes a rule from the ACL.

<b>Syntax Description</b>	sequence-number	Optional parameter to set a specific sequence number for the rule. Range is: 1-65535.
	deny	Drop all matching traffic
	permit	Allow matching traffic to pass
	<source-ip> mask <ip>   any	Sets source IP and optionally sets a mask for that IP address. The “any” option will cause the rule not to check the source IP.
	<dest-ip> mask <ip>   any	Sets destination IP and optionally sets a mask for that IP. The “any” option will cause the rule not to check the destination IP.
	src-port	L4 source port. Note: User may only choose one of the following options to configure source port: src-port; eq-source.
	eq-source <src-port>	TCP source port number. Range: 0-65535.
	src-port-range	Sets a range of L4 source ports to match. Note: User may configure either a single source port or a range.
	dest-port	L4 destination port. Note: User may only choose one of the following options to configure destination port: dest-port; eq-destination.
	eq-destination <dest-port>	TCP destination port number. Range: 0-65535.
	dest-port-range	Sets a range of L4 destination ports to match. Note: User may configure either a single destination port or a range.
	action	Action needs to be defined before attaching to rule
	established	Matches flows which are in established state (“ack” or “rst” flags are set)
	ack	Matches flows with ack flag. Possible match: 0 or 1.

urg	Matches flows with urg flag. Possible match: 0 or 1.
rst	Matches flows with rst flag. Possible match: 0 or 1.
syn	Matches flows with syn flag. Possible match: 0 or 1.
fin	Matches flows with fin flag. Possible match: 0 or 1.
psh	Matches flows with psh flag. Possible match: 0 or 1.
log	Enables the log option
counter	Attaches a unique counter to rule
shared-counter	Attaches a predefined shared-counter to rule
<b>Default</b>	No rule is added by default to access control list Default sequence number is in multiple of 10
<b>Configuration Mode</b>	Config IPv4 ACL
<b>History</b>	3.1.1400 3.5.1000                  Updated seq-number parameter 3.6.5000                  Updated command syntax
<b>Role</b>	admin
<b>Example</b>	switch (config ipv4 access-list my-list)# permit tcp any any src-port 200 dest-port-range 200 400 established
<b>Related Commands</b>	{ipv4/ipv4-udk/ipv6/mac/mac-udk} access-list {ipv4/ipv4-udk/ipv6/mac/mac-udk} port access-group
<b>Notes</b>	L4 ports are valid

## deny/permit (IPv4 TCP-UDP/UDP ACL rule)

```
[seq-number <sequence-number>] {deny | permit} {tcp-udp | udp} {<source-ip>
mask <ip> | any} {<dest-ip> mask <ip> | any} [src-port <src-port> | eq-source
<src-port> | src-port-range <from> <to>] [dest-port <dest-port> | eq-destination
<dest-port> | dest-port-range <from> <to>] [action <action-id>] [log] [counter |
shared-counter <name>]
no <sequence-number>
```

Creates a rule for IPv4 TCP-UDP/UDP ACL.

The no form of the command deletes a rule from the ACL.

<b>Syntax Description</b>	sequence-number	Optional parameter to set a specific sequence number for the rule. Range: 1-65535.
	deny	Drop all matching traffic
	permit	Allow matching traffic to pass
	<source-ip> mask <ip>   any	Sets source IP and optionally sets a mask for that IP address. The “any” option will cause the rule not to check the source IP.
	<dest-ip> mask <ip>   any	Sets destination IP and optionally sets a mask for that IP. The “any” option will cause the rule not to check the destination IP.
	src-port	L4 source port. Note: User may only choose one of the following options to configure source port: src-port; eq-source.
	eq-source <src-port>	TCP-UDP/UDP source port number. Range: 0-65535.
	src-port-range	Sets a range of L4 source ports to match. Note: User may configure either a single source port or a range.
	dest-port	L4 destination port. Note: User may only choose one of the following options to configure destination port: dest-port; eq-destination.
	eq-destination <dest-port>	TCP-UDP/UDP destination port number Range: 0-65535
	dest-port-range	Sets a range of L4 destination ports to match. Note: User may configure either a single destination port or a range.
	action	Action needs to be defined before attaching to rule
	log	Enables the log option
	counter	Attaches a unique counter to rule
	shared-counter	Attaches a predefined shared-counter to rule

<b>Default</b>	No rule is added by default to access control list Default sequence number is in multiple of 10
<b>Configuration Mode</b>	Config IPv4 ACL
<b>History</b>	3.1.1400 3.5.1000 Updated seq-number parameter 3.6.5000 Updated command syntax
<b>Role</b>	admin
<b>Example</b>	<pre>switch (config ipv4 access-list my-list)# permit tcp-udp any any eq-destination 100 eq-source 300 switch (config ipv4 access-list my-list)# permit udp any any eq-destination 100 eq-source 300</pre>
<b>Related Commands</b>	{ipv4/ipv4-udk/ipv6/mac/mac-udk} access-list {ipv4/ipv4-udk/ipv6/mac/mac-udk} port access-group
<b>Notes</b>	

## deny/permit (IPv4 ICMP ACL rule)

```
[seq-number <sequence-number>] {deny | permit} icmp {<source-ip> mask <ip> | any} {<dest-ip> mask <ip> | any} [eq-code <icmp-code>] [eq-type <icmp-type>] [log] [counter | shared-counter <name>]  
no <sequence-number>
```

Creates a rule for IPv4 ICMP ACL.

The no form of the command deletes a rule from the ACL.

<b>Syntax Description</b>	sequence-number	Optional parameter to set a specific sequence number for the rule. Range: 1-65535.
	deny	Drop all matching traffic
	permit	Allow matching traffic to pass
	<source-ip> mask <ip>   any	Sets source IP and optionally sets a mask for that IP address. The “any” option will cause the rule not to check the source IP.
	<dest-ip> mask <ip>   any	Sets destination IP and optionally sets a mask for that IP. The “any” option will cause the rule not to check the destination IP.
	eq-code	Matches ICMP code value. Range: 0-255.
	eq-type	Matches ICMP type value. Range: 0-255.
	log	Enables the log option
	counter	Attaches a unique counter to rule
	shared-counter	Attaches a predefined shared-counter to rule
<b>Default</b>	No rule is added by default to access control list Default sequence number is in multiple of 10	
<b>Configuration Mode</b>	Config IPv4 ACL	
<b>History</b>	3.1.1400 3.5.1000                  Updated seq-number parameter 3.6.2002                  Added ICMP parameters 3.6.5000                  Updated command syntax	
<b>Role</b>	admin	
<b>Example</b>	switch (config ipv4 access-list my-list)# permit icmp any any eq-code 10 eq-type 155	

**Related Commands**

{ipv4/ipv4-udk/ipv6/mac/mac-udk} access-list  
{ipv4/ipv4-udk/ipv6/mac/mac-udk} port access-group

**Notes**

- ICMP code must be specified in conjunction with an ICMP type. If ICMP type is specified but no ICMP code is specified, the rule matches all ICMP packets of the given type.
- If no ICMP type or code are specified, the rule matches all ICMP packets from the specified source/destination address.

## deny/permit (IPv6 ACL rule)

```
[seq-number <sequence-number>] {permit | deny} ip {<src-ipv6>/<mask-len> |
any} {<dest-ipv6>/<mask-len> | any} [action <action-id>] [log] [counter |
shared-counter <name>]
no <sequence-number>
```

Creates an IPv6 ACL rule with a specific protocol.

The no form of the command deletes a rule from the IPv6 ACL.

<b>Syntax Description</b>	sequence-number	Optional parameter to set a specific sequence number for the rule. Range: 1-65535.
	deny	Drop all matching traffic
	permit	Allow matching traffic to pass
	<src-ipv6>/<mask-len>   any	Sets source IP and optionally sets a mask for that IP address. The parameter “any” ignores the source IP.
	<dest-ipv6>/<mask-len>   any	Sets destination IP and optionally sets a mask for that IP. The parameter “any” ignores the destination IP.
	action	Action needs to be defined before attaching to rule
	log	Enables the log option
	counter	Attaches a unique counter to rule
	shared-counter	Attaches a predefined shared-counter to rule
<b>Default</b>	No rule is added by default to access control list Default sequence number is in multiple of 10	
<b>Configuration Mode</b>	Config IPv6 ACL	
<b>History</b>	3.6.5000	
<b>Role</b>	admin	
<b>Example</b>	switch (config ipv6 access-list my-list) # permit ip 2:2::/32 any	
<b>Related Commands</b>		
<b>Note</b>	<ul style="list-style-type: none"> <li>IPv6 address format is as follows: &lt;A:B:C:D:E:F:G:H&gt;/mask_len</li> <li>The fields eq-code (icmp-code) and eq-type (eq-type) are valid only for ICMP rules</li> </ul>	

## deny/permit (IPv6 TCP ACL rule)

```
[seq-number <sequence-number>] {permit | deny} tcp {<source-ipv6> /<mask-len> | any} {<dest-ipv6> /<mask-len> | any} [src-port <src-port> | src-port-range <from> <to>] [dest-port <dest-port> | dest-port-range <from> <to>] [established | ack {0 | 1} | urg {0 | 1} | rst {0 | 1} | syn {0 | 1} | fin {0 | 1} | psh {0 | 1}] [log | counter | shared-counter <name>] [action <action-id>]
no <sequence-number>
```

Creates an IPv6 ACL rule with a specific protocol.

The no form of the command deletes a rule from the IPv6 ACL.

<b>Syntax Description</b>	sequence-number	Optional parameter to set a specific sequence number for the rule. Range: 1-65535.
	deny	Drop all matching traffic
	permit	Allow matching traffic to pass
	<source-ipv6> /<mask-len>   any	Sets source IP and optionally sets a mask for that IP address. The “any” option will cause the rule not to check the source IP.
	<dest-ipv6> /<mask-len>   any	Sets destination IP and optionally sets a mask for that IP. The “any” option will cause the rule not to check the destination IP.
	src-port	L4 source port. Note: User may only choose one of the following options to configure source port: src-port; eq-source.
	src-port-range	Sets a range of L4 source ports to match. Note: User may configure either a single source port or a range.
	dest-port	L4 destination port. Note: User may only choose one of the following options to configure destination port: dest-port; eq-destination.
	dest-port-range	Sets a range of L4 destination ports to match. Note: User may configure either a single destination port or a range.
	action	Action needs to be defined before attaching to rule
	established	Matches flows which are in established state (“ack” or “rst” flags are set)
	ack	Matches flows with ack flag. Possible match: 0 or 1.
	urg	Matches flows with urg flag. Possible match: 0 or 1.
	rst	Matches flows with rst flag. Possible match: 0 or 1.
	syn	Matches flows with syn flag. Possible match: 0 or 1.

fin	Matches flows with fin flag. Possible match: 0 or 1.
psh	Matches flows with psh flag. Possible match: 0 or 1.
log	Enables the log option
counter	Attaches a unique counter to rule
shared-counter	Attaches a predefined shared-counter to rule
<b>Default</b>	No rule is added by default to access control list Default sequence number is in multiple of 10
<b>Configuration Mode</b>	Config IPv6 ACL
<b>History</b>	3.6.5000
<b>Role</b>	admin
<b>Example</b>	switch (config ipv6 access-list my-list) # permit tcp any 10:10:12::/48
<b>Related Commands</b>	
<b>Note</b>	IPv6 address format is as follows: <A:B:C:D:E:F:G:H>/mask_len

## deny/permit (IPv6 TCP-UDP/UDP ACL rule)

```
[seq-number <sequence-number>] {permit | deny} {tcp-udp | udp} {<source-ipv6> /<mask-len> | any} {<dest-ipv6> /<mask-len> | any} [src-port <src-port> | src-port-range <from> <to>] [dest-port <dest-port> | dest-port-range <from> <to>] [log] [counter | shared-counter <name>] [action <action-id>] no <sequence-number>
```

Creates an IPv6 ACL rule with a specific protocol.

The no form of the command deletes a rule from the IPv6 ACL.

<b>Syntax Description</b>	sequence-number	Optional parameter to set a specific sequence number for the rule. Range: 1-65535.
	deny	Drop all matching traffic
	permit	Allow matching traffic to pass
	<source-ipv6> /<mask-len>   any	Sets source IP and optionally sets a mask for that IP address. The “any” option will cause the rule not to check the source IP.
	<dest-ipv6> /<mask-len>   any	Sets destination IP and optionally sets a mask for that IP. The “any” option will cause the rule not to check the destination IP.
	src-port	L4 source port. Note: User may only choose one of the following options to configure source port: src-port; eq-source.
	src-port-range	Sets a range of L4 source ports to match. Note: User may configure either a single source port or a range.
	dest-port	L4 destination port. Note: User may only choose one of the following options to configure destination port: dest-port; eq-destination.
	dest-port-range	Sets a range of L4 destination ports to match. Note: User may configure either a single destination port or a range.
	action	Action needs to be defined before attaching to rule
	log	Enables the log option
	counter	Attaches a unique counter to rule
	shared-counter	Attaches a predefined shared-counter to rule
<b>Default</b>	No rule is added by default to access control list Default sequence number is in multiple of 10	
<b>Configuration Mode</b>	Config IPv6 ACL	

<b>History</b>	3.6.5000
<b>Role</b>	admin
<b>Example</b>	<pre>switch (config ipv6 access-list my-list) # permit udp 2::2::/32 10::10:12::/48</pre>
<b>Related Commands</b>	
<b>Note</b>	IPv6 address format is as follows: <A:B:C:D:E:F:G:H>/mask_len

## deny/permit (IPv6 ICMPv6 ACL rule)

```
[seq-number <sequence-number>] {permit | deny} icmpv6 {<source-ipv6> / 
<mask-len> | any} {<dest-ipv6> /<mask-len> | any} [code <icmp-code>] [type 
<icmp-type>] [log] [counter | shared-counter <name>] [action <action-id>]
no <sequence-number>
```

Creates an IPv6 ACL rule with a specific protocol.

The no form of the command deletes a rule from the IPv6 ACL.

<b>Syntax Description</b>	sequence-number	Optional parameter to set a specific sequence number for the rule. Range: 1-65535.
	deny	Drop all matching traffic
	permit	Allow matching traffic to pass
	<source-ipv6> /<mask-len>   any	Sets source IP and optionally sets a mask for that IP address. The “any” option will cause the rule not to check the source IP.
	<dest-ipv6> /<mask-len>   any	Sets destination IP and optionally sets a mask for that IP. The “any” option will cause the rule not to check the destination IP.
	eq-code	Matches ICMP code value Range: 0-255
	eq-type	Matches ICMP type value Range: 0-255
	action	Action needs to be defined before attaching to rule
	log	Enables the log option
	counter	Attaches a unique counter to rule
	shared-counter	Attaches a predefined shared-counter to rule
<b>Default</b>	No rule is added by default to access control list Default sequence number is in multiple of 10	
<b>Configuration Mode</b>	Config IPv6 ACL	
<b>History</b>	3.6.5000	
<b>Role</b>	admin	
<b>Example</b>	switch (config ipv6 access-list my-list) # permit icmpv6 any any eq-code 10 eq-type 155	
<b>Related Commands</b>		
<b>Note</b>	IPv6 address format is as follows: <A:B:C:D:E:F:G:H>/mask_len	

## deny/permit (MAC UDK ACL rule)

```
[seq-number <sequence-number>] {deny | permit} {<source-mac> mask <mac-mask> | any} {<dest-mac> mask <mac-mask> | any} [protocol <protocol-num>]
[cos <cos>] [vlan <vlan-id>] [vlan-mask <vlan_mask>] [action <action-name>]
[log] [counter | shared-counter <name>] [udk <udk1> <val> [mask <mask>]]]
[<udk2> <val> [mask <mask>]] [<udk3> <val> [mask <mask>]] [<udk4> <val>
[mask <mask>]]
no <sequence-number>
```

Creates a MAC-UDK ACL rule.

The no form of the command deletes a rule from MAC UDK ACL.

<b>Syntax Description</b>	sequence-number	Optional parameter to set a specific sequence number for the rule. Range:1-65535.
	deny	Drop all matching traffic
	permit	Allow matching traffic to pass
	<source-mac> mask <mac-mask>   any	Sets source MAC and optionally sets a mask for that MAC. The “any” option will cause the rule not to check the source MAC.
	<dest-mac> mask <mac-mask>   any	Sets destination MAC and optionally sets a mask for that MAC. The “any” option will cause the rule not to check the destination MAC.
	protocol	Sets the Ethertype filed value from the MAC address Range: 0x0000-0xffff
	cos	Sets the COS (priority bit) field. Range: 0-7.
	vlan <vlan-id>	Sets the VLAN ID field. Range: 1-4094.
	vlan-mask <vlan-mask>	Sets VLAN group. Range: 0x0000-0x0FFF.
	action	Action name (free string)
	log	Enable the log option
	counter	Attach a unique counter to rule
	shared-counter	Attach a predefined shared-counter to rule
	udk	UDK name must be set by user before the rule configuration
	val	The value of the UDK (up to 4 bytes)
	mask	Mask for the UDK value
<b>Default</b>	No rule is added by default to access control list Default sequence number is in multiple of 10	

<b>Configuration Mode</b>	Config MAC-UDK ACL
<b>History</b>	3.6.5000
<b>Role</b>	admin
<b>Example</b>	<pre>switch (config mac-udk access-list mac_udk_acl) # permit any any udk myUdk 10 mask 0xff</pre>

### Related Commands

- Note**
- User cannot attach a shared counter defined on a different ACL table
  - The parameter shared-counter must be defined before attaching it to the scope of the ACL table
  - UDK fields must come at the end of the rule configuration
  - The default mask is 0xff–0xffffffff (depends on value length)
  - UDK cannot be deleted while it is attached to a rule
  - 1-4 UDKs per rule may be configured
  - Values and masks of the UDK can be decimal or hexadecimal
- 
-

## deny/permit (IPv4 UDK ACL rule)

```
[seq-number <sequence-number>] {permit | deny} ip {<source-ip> mask <ip> | any} {<dest-ip> mask <ip> | any} [action <action-id>] [log] [counter | shared-counter <name>] [udk <udk1> <val> [mask <mask>]] [<udk2> <val> [mask <mask>]] [<udk3> <val> [mask <mask>]] [<udk4> <val> [mask <mask>]] no <sequence-number>
```

Creates a rule for IPv4 ACL.

The no form of the command deletes a rule from the IPv4 ACL.

<b>Syntax Description</b>	sequence-number	Optional parameter to set a specific sequence number for the rule. Range is: 1-65535.
	deny	Drop all matching traffic
	permit	Allow matching traffic to pass
	{any   <source-ip> mask <ip>}	Sets source IP and optionally sets a mask for that IP address. The “any” option causes the rule to not check the source IP. Range: 0-255.
	{any   <destination-ip> mask <ip>}	Sets destination IP and optionally sets a mask for that MAC. The “any” option causes the rule to not check the destination MAC.
	action	Action needs to be defined before attaching to rule
	log	Enable the log option
	counter	Attach a unique counter to rule
	shared-counter	Attach a predefined shared-counter to rule
	udk	UDK name must be set by user before the rule configuration
	val	The value of the UDK (up to 4 bytes)
	mask	Mask for the UDK value
<b>Default</b>	No rule is added by default to access control list. Default sequence number is in multiple of 10.	
<b>Configuration Mode</b>	Config IPv4 ACL	
<b>History</b>	3.6.5000	
<b>Role</b>	admin	

<b>Example</b>	<pre>switch (config ipv4 access-list my-list) # deny ip any any action act shared-counter</pre>
<b>Related Commands</b>	<pre>{ipv4/ipv4-udk/ipv6/mac/mac-udk} access-list {ipv4/ipv4-udk/ipv6/mac/mac-udk} port access-group</pre>
<b>Note</b>	<ul style="list-style-type: none"><li>• User cannot attach a shared counter defined on a different ACL table</li><li>• The parameter shared-counter must be defined before attaching it to the scope of the ACL table</li><li>• UDK fields must come at the end of the rule configuration</li><li>• The default mask is 0xff–0xffffffff (depends on value length)</li><li>• UDK cannot be deleted while it is attached to a rule</li><li>• 1-4 UDKs per rule may be configured</li><li>• Values and masks of the UDK can be decimal or hexadecimal</li></ul>

## deny/permit (IPv4 TCP UDK ACL rule)

```
[seq-number <sequence-number>] {deny | permit} tcp {<source-ip> mask <ip> | any} {<dest-ip> mask <ip> | any} [src-port <src-port> | eq-source <src-port> | src-port-range <from> <to>] [dest-port <dest-port> | eq-destination <dest-port> | dest-port-range <from> <to>] [action <action-id>] [established | [ack {0 | 1}] | [urg {0 | 1}] | [rst {0 | 1}] | [syn {0 | 1}] | [fin {0 | 1}] | [psh {0 | 1}]] | [log] | [counter | shared-counter <name>] | [udk <udk1> <val> | [mask <mask>]] | [<udk2> <val> | [mask <mask>]] | [<udk3> <val> | [mask <mask>]] | [<udk4> <val> | [mask <mask>]]]
```

Creates a rule for IPv4 TCP ACL.

The no form of the command deletes a rule from the ACL.

<b>Syntax Description</b>	sequence-number	Optional parameter to set a specific sequence number for the rule. Range is: 1-65535.
deny		Drop all matching traffic
permit		Allow matching traffic to pass
<source-ip> [mask <ip>]   any		Sets source IP and optionally sets a mask for that IP address. The “any” option will cause the rule not to check the source IP.
<dest-ip> [mask <ip>]   any		Sets destination IP and optionally sets a mask for that IP. The “any” option will cause the rule not to check the destination IP.
src-port		L4 source port. Note: User may only choose one of the following options to configure source port: src-port; eq-source.
eq-source <src-port>		TCP source port number. Range: 0-65535.
src-port-range		Sets a range of L4 source ports to match. Note: User may configure either a single source port or a range.
dest-port		L4 destination port. Note: User may only choose one of the following options to configure destination port: dest-port; eq-destination.
eq-destination <dest-port>		TCP destination port number. Range: 0-65535.
dest-port-range		Sets a range of L4 destination ports to match. Note: User may configure either a single destination port or a range.
action		Action needs to be defined before attaching to rule
established		Matches flows which are in established state (“ack” or “rst” flags are set)

ack	Matches flows with ack flag. Possible match: 0 or 1.
urg	Matches flows with urg flag. Possible match: 0 or 1.
rst	Matches flows with rst flag. Possible match: 0 or 1.
syn	Matches flows with syn flag. Possible match: 0 or 1.
fin	Matches flows with fin flag. Possible match: 0 or 1.
psh	Matches flows with psh flag. Possible match: 0 or 1.
log	Enables the log option
counter	Attaches a unique counter to rule
shared-counter	Attaches a predefined shared-counter to rule
udk	UDK name must be set by user before the rule configuration
val	The value of the UDK (up to 4 bytes)
mask	Mask for the UDK value
<b>Default</b>	No rule is added by default to access control list Default sequence number is in multiple of 10
<b>Configuration Mode</b>	Config IPv4 ACL
<b>History</b>	3.6.5000
<b>Role</b>	admin
<b>Example</b>	<pre>switch (config ipv4 access-list my-list)# permit tcp any any src-port 200 dest-port-range 200 400 established</pre>
<b>Related Commands</b>	{ipv4/ipv4-udk/ipv6/mac/mac-udk} access-list {ipv4/ipv4-udk/ipv6/mac/mac-udk} port access-group
<b>Notes</b>	<ul style="list-style-type: none"> <li>UDK fields must come at the end of the rule configuration</li> <li>The default mask is 0xff–0xffffffff (depends on value length)</li> <li>UDK cannot be deleted while it is attached to a rule</li> <li>1-4 UDKs per rule may be configured</li> </ul>

## deny/permit (IPv4 TCP-UDP/UDP UDK ACL rule)

```
[seq-number <sequence-number>] {deny | permit} {tcp-udp | udp} {<source-ip>
mask <ip> | any} {<dest-ip> mask <ip> | any} [src-port <src-port> | eq-source
<src-port> | src-port-range <from> <to>] [dest-port <dest-port> | eq-destination
<dest-port> | dest-port-range <from> <to>] [action <action-id>] [log] [counter |
shared-counter <name>] [udk <udk1> <val> [mask <mask>]] [<udk2> <val>
[mask <mask>]] [<udk3> <val> [mask <mask>]] [<udk4> <val> [mask
<mask>]]]
no <sequence-number>
```

Creates a rule for IPv4 TCP-UDP/UDP ACL.

The no form of the command deletes a rule from the ACL.

<b>Syntax Description</b>	sequence-number	Optional parameter to set a specific sequence number for the rule. Range: 1-65535.
deny		Drop all matching traffic
permit		Allow matching traffic to pass
<source-ip> mask <ip>   any		Sets source IP and optionally sets a mask for that IP address. The “any” option will cause the rule not to check the source IP.
<dest-ip> mask <ip>   any		Sets destination IP and optionally sets a mask for that IP. The “any” option will cause the rule not to check the destination IP.
src-port		L4 source port. Note: User may only choose one of the following options to configure source port: src-port; eq-source.
eq-source <src-port>		TCP-UDP/UDP source port number. Range: 0-65535.
src-port-range		Sets a range of L4 source ports to match. Note: User may configure either a single source port or a range.
dest-port		L4 destination port. Note: User may only choose one of the following options to configure destination port: dest-port; eq-destination.
eq-destination <dest-port>		TCP-UDP/UDP destination port number Range: 0-65535
dest-port-range		Sets a range of L4 destination ports to match. Note: User may configure either a single destination port or a range.
action		Action needs to be defined before attaching to rule
log		Enables the log option
counter		Attaches a unique counter to rule

	shared-counter	Attaches a predefined shared-counter to rule
	udk	UDK name must be set by user before the rule configuration
	val	The value of the UDK (up to 4 bytes)
	mask	Mask for the UDK value
<b>Default</b>		No rule is added by default to access control list Default sequence number is in multiple of 10
<b>Configuration Mode</b>		Config IPv4 ACL
<b>History</b>		3.6.5000
<b>Role</b>		admin
<b>Example</b>		<pre>switch (config ipv4 access-list my-list)# permit tcp-udp any any eq- destination 100 eq-source 300 switch (config ipv4 access-list my-list)# permit udp any any eq-desti- nation 100 eq-source 300</pre>
<b>Related Commands</b>		{ipv4/ipv4-udk/ipv6/mac/mac-udk} access-list {ipv4/ipv4-udk/ipv6/mac/mac-udk} port access-group
<b>Notes</b>		<ul style="list-style-type: none"> <li>UDK fields must come at the end of the rule configuration</li> <li>The default mask is 0xff-0xffffffff (depends on value length)</li> <li>UDK cannot be deleted while it is attached to a rule</li> <li>1-4 UDKs per rule may be configured</li> </ul>

## deny/permit (IPv4 ICMP UDK ACL rule)

```
[seq-number <sequence-number>] {deny | permit} icmp {<source-ip> mask <ip> | any} {<dest-ip> mask <ip> | any} [eq-code <icmp-code>] [eq-type <icmp-type>] [log] [counter | shared-counter <name>] [udk <udk1> <val> [mask <mask>]] [<udk2> <val> [mask <mask>]] [<udk3> <val> [mask <mask>]] [<udk4> <val> [mask <mask>]] no <sequence-number>
```

Creates a rule for IPv4 ICMP ACL.

The no form of the command deletes a rule from the ACL.

<b>Syntax Description</b>	sequence-number	Optional parameter to set a specific sequence number for the rule. Range: 1-65535.
	deny	Drop all matching traffic
	permit	Allow matching traffic to pass
	<source-ip> mask <ip>   any	Sets source IP and optionally sets a mask for that IP address. The “any” option will cause the rule not to check the source IP.
	<dest-ip> mask <ip>   any	Sets destination IP and optionally sets a mask for that IP. The “any” option will cause the rule not to check the destination IP.
	eq-code	Matches ICMP code value. Range: 0-255.
	eq-type	Matches ICMP type value. Range: 0-255.
	log	Enables the log option
	counter	Attaches a unique counter to rule
	shared-counter	Attaches a predefined shared-counter to rule
	udk	UDK name must be set by user before the rule configuration
	val	The value of the UDK (up to 4 bytes)
	mask	Mask for the UDK value
<b>Default</b>	No rule is added by default to access control list Default sequence number is in multiple of 10	
<b>Configuration Mode</b>	Config IPv4 ACL	
<b>History</b>	3.6.5000	
<b>Role</b>	admin	
<b>Example</b>	switch (config ipv4 access-list my-list)# permit icmp any any eq-code 10 eq-type 155	

**Related Commands**

{ipv4/ipv4-udk/ipv6/mac/mac-udk} access-list  
{ipv4/ipv4-udk/ipv6/mac/mac-udk} port access-group

**Notes**

- ICMP code must be specified in conjunction with an ICMP type. If ICMP type is specified but no ICMP code is specified, the rule matches all ICMP packets of the given type.
- If no ICMP type or code are specified, the rule matches all ICMP packets from the specified source/destination address.
- UDK fields must come at the end of the rule configuration
- The default mask is 0xff-0xffffffff (depends on value length)
- UDK cannot be deleted while it is attached to a rule
- 1-4 UDKs per rule may be configured

## port access-group (IPv4/IPv4 UDK/IPv6/MAC/MAC UDK)

```
{ipv4 | ipv4-udk | ipv6 | mac | mac-udk} port access-group <acl-name>
no {mac | ipv4 | ipv6 | mac-udk | ipv4-udk} port access-group
```

Attaches an ACL table with bind-point RIF to a VLAN interface.  
The no form of the command unmaps ACL table with bind-point RIF from a VLAN interface.

<b>Syntax Description</b>	acl-name	ACL table name
<b>Default</b>	N/A	
<b>Configuration Mode</b>	Config Interface VLAN	
<b>History</b>	3.6.5000	
<b>Role</b>	admin	
<b>Example</b>	switch (config interface vlan 10)# ipv4 port access-group ipv4_acl2	
<b>Related Commands</b>	show access list summary	
<b>Note</b>	<ul style="list-style-type: none"><li>Only ACL tables with bind-point set to RIF can be attached to a VLAN interface</li><li>Interface VLAN must be configured before binding operation</li></ul>	

## access-list action

```
access-list action <action-profile-name>
no access-list action <action-profile-name>
```

Creates access-list action profile and entering the action profile configuration mode.  
The no form of the command deletes the action profile.

Syntax Description	action-profile-name	Given name for the profile.
<b>Default</b>	N/A	
<b>Configuration Mode</b>	Config	
<b>History</b>	3.2.0230	
<b>Role</b>	admin	
<b>Example</b>		switch (config)# access-list action my-action switch (config access-list action my-action)#
<b>Related Commands</b>		
<b>Note</b>		

## access-list log

**access-list log [interval <int\_num>] [memory <packet\_num>] [syslog <packet\_num>]**

**no access-list log [interval <int\_num>] [memory <packet\_num>] [syslog <packet\_num>]**

Configures access list logger.

The no form of the command resets parameters for access list logger.

<b>Syntax Description</b>	interval memory syslog	Logging interval length in minutes Range: 1min-24hrs  Maximal number of packets to save in memory Range: 1-3600  Maximal number of packets to show in syslog Range: 1-3600
<b>Default</b>	N/A	
<b>Configuration Mode</b>	Config	
<b>History</b>	3.6.5000	
<b>Role</b>	admin	
<b>Example</b>	<pre>switch (config)# access-list log interval 10 switch (config)# access-list log memory 300 switch (config)# access-list log syslog 200</pre>	
<b>Related Commands</b>		
<b>Note</b>	<ul style="list-style-type: none"> <li>The packet number in syslog configuration must not be greater than the maximal packets number in memory</li> <li>When configuring interval, the interval will restart resulting in a log dump to syslog and memory clear</li> </ul>	

## vlan-map

**vlan-map <vlan-id>**  
**no vlan-map**

Adds action to map a new VLAN to the packet (in the ingress port or VLAN).  
The no form of the command removes the action to map a new VLAN.

<b>Syntax Description</b>	vlan-id	1-4094.		
<b>Default</b>	N/A			
<b>Configuration Mode</b>	Config ACL Action			
<b>History</b>	3.2.0230			
<b>Role</b>	admin			
<b>Example</b>	switch (config access-list action my-action)# vlan-map 10			
<b>Related Commands</b>				
<b>Note</b>				

## vlan-pop

### vlan-pop

Pops VLAN frames from traffic.

<b>Syntax Description</b>	vlan-id	VLAN ID: 1-4094.
<b>Default</b>	N/A	
<b>Configuration Mode</b>	Config ACL Action	
<b>History</b>	3.4.3000	
<b>Role</b>	admin	
<b>Example</b>	switch (config access-list action my-action)# vlan-pop	
<b>Related Commands</b>		
<b>Note</b>		

## vlan-push

**vlan-push <vlan-id>**

Pushes (or adds) VLAN frames to traffic.

<b>Syntax Description</b>	vlan-id	VLAN ID: 1-4094
<b>Default</b>	N/A	
<b>Configuration Mode</b>	Config ACL Action	
<b>History</b>	3.4.3000	
<b>Role</b>	admin	
<b>Example</b>	switch (config access-list action my-action)# vlan-push 10	
<b>Related Commands</b>		
<b>Note</b>		

## show access-lists (ipv4/ipv4-udk/ipv6/mac/mac-udk)

**show {ipv4 | ipv4-udk | ipv6 | mac | mac-udk} access-lists <access-list-name>**

Displays all configuration of all rules in a specific table.

<b>Syntax Description</b>	access-list-name	ACL name																						
<b>Default</b>	N/A																							
<b>Configuration Mode</b>	Any Command Mode																							
<b>History</b>	3.1.1400																							
	3.3.4500	Updated output																						
	3.6.5000	Updated output and syntax																						
<b>Role</b>	admin																							
<b>Example</b>	<pre>switch (config mac access-list my-list) # show mac access-lists mac_acl mac access-list mac_acl: Bind-point: port</pre> <table border="1"> <thead> <tr> <th>seq-number</th> <th>p/d</th> <th>smac</th> <th>dmac</th> <th>protocol</th> <th>cos</th> <th>vlan</th> <th>vlan-mask</th> <th>action</th> <th>counter</th> <th>Packets</th> </tr> </thead> <tbody> <tr> <td>10</td> <td>permit</td> <td>any</td> <td>any</td> <td>0x8100</td> <td>5</td> <td>1000</td> <td>N/A</td> <td>none</td> <td>N/A</td> <td>0</td> </tr> </tbody> </table>		seq-number	p/d	smac	dmac	protocol	cos	vlan	vlan-mask	action	counter	Packets	10	permit	any	any	0x8100	5	1000	N/A	none	N/A	0
seq-number	p/d	smac	dmac	protocol	cos	vlan	vlan-mask	action	counter	Packets														
10	permit	any	any	0x8100	5	1000	N/A	none	N/A	0														
<b>Related Commands</b>	deny/permit {ipv4/ipv4-udk/ipv6/mac/mac-udk} access-list {ipv4/ipv4-udk/ipv6/mac/mac-udk} port access-group																							
<b>Note</b>																								

## show access-lists action

**show access-lists action <action-profile-name>**

Displays the access-list action profiles summary.

<b>Syntax Description</b>	action-profile-name summary	Filter the table according to the action profile name. Display summary of the action list.
<b>Default</b>	N/A	
<b>Configuration Mode</b>	Any Command Mode	
<b>History</b>	3.2.0230	
<b>Role</b>	admin	
<b>Example</b>	<pre>witch (config)# show access-lists action my-action Access-list Action my-action Mapped_Vlan_ID   Mapped_port   Counter_set   Policer_ID   ===== 10             N/A            N/A            N/A           </pre>	
<b>Related Commands</b>		
<b>Note</b>		

## show access-lists shared-counters (ipv4/ipv4-udk/ipv6/mac/mac-udk)

```
show {ipv4 | ipv4-udk | ipv6 | mac | mac-udk} access-lists <access-list-name>
shared-counters
```

Displays all configured shared-counters on a specific ACL table.

Syntax Description	access-list-name	ACL name
<b>Default</b>	N/A	
<b>Configuration Mode</b>	Any Command Mode	
<b>History</b>	3.6.5000	
<b>Role</b>	admin	
<b>Example</b>	<pre>switch (config mac access-list my-list) # show mac access-lists mac_acl shared-counters ----- counter      packets      total Rules      rule IDs ----- cnt1          0            3           20 30 40 cnt2          0            2           50 60 cnt3          0            1           70</pre>	
<b>Related Commands</b>		
<b>Note</b>	<ul style="list-style-type: none"> <li>For each configured shared counter it also displays the counter value (packets), the number of rules attached to this counter and the rule IDs</li> <li>Up to 5 rule IDs are displayed even though there is no limitation on how many rules can be attached to a counter</li> </ul>	

## show access-lists summary

**show [ipv4 | mac | ipv6 | ipv4-udk | mac-udk] access-lists summary**

Displays the summary of number of rules per ACL, and the interfaces attached.

<b>Syntax Description</b>	N/A																												
<b>Default</b>	N/A																												
<b>Configuration Mode</b>	Any Command Mode																												
<b>History</b>	3.1.1400																												
	3.6.5000	Updated output																											
<b>Role</b>	admin																												
<b>Example</b>	<pre>switch (config) # show access-lists summary</pre> <hr/> <table><thead><tr><th>Table type</th><th>Table Name</th><th>Bind type</th><th>Total entries</th><th>Bound to interfaces</th></tr></thead><tbody><tr><td>mac</td><td>aaa</td><td>port</td><td>0</td><td>Mpo55</td></tr><tr><td>ipv4</td><td>ddd</td><td>port</td><td>1</td><td>Eth1/3, Po1</td></tr><tr><td>ipv4</td><td>ggg</td><td>rif</td><td>0</td><td>VlanIf555</td></tr><tr><td>ipv6</td><td>table1</td><td>port</td><td>9</td><td>Eth1/9</td></tr></tbody></table>				Table type	Table Name	Bind type	Total entries	Bound to interfaces	mac	aaa	port	0	Mpo55	ipv4	ddd	port	1	Eth1/3, Po1	ipv4	ggg	rif	0	VlanIf555	ipv6	table1	port	9	Eth1/9
Table type	Table Name	Bind type	Total entries	Bound to interfaces																									
mac	aaa	port	0	Mpo55																									
ipv4	ddd	port	1	Eth1/3, Po1																									
ipv4	ggg	rif	0	VlanIf555																									
ipv6	table1	port	9	Eth1/9																									
<b>Related Commands</b>																													
<b>Note</b>																													

## show access-lists log

**show access-lists log [last <num>]**

Displays captured packets on all access list rules.

<b>Syntax Description</b>	num	Number of packets to show
<b>Default</b>	N/A	
<b>Configuration Mode</b>	Any Command Mode	
<b>History</b>	3.6.5000	
<b>Role</b>	admin	
<b>Example</b>	<pre>switch (config) # show access-lists log Log status: Normal  Log MAC rules: ----- IF      Table(rule)        Source MAC          Dest MAC          Ethertype VLAN Hits ----- 1/2    mac_al_log(10)      44:44:44:44:44:44 22:22:22:22:22:22 IPv4      N/A      5  Log IPv4 rules: ----- IF      Table(rule)        Source IPv4        Dest IPv4        Protocol Source Dest Hits  port      port ----- 1/3    ipv4_al_lo(10)      1.1.1.1           2.2.2.2        UDP       44     33     11</pre>	

### Related Commands

#### Note

## show access-lists log config

### show access-lists log config

Displays configuration of access-list logger.

<b>Syntax Description</b>	N/A
<b>Default</b>	N/A
<b>Configuration Mode</b>	Any Command Mode
<b>History</b>	3.6.5000
<b>Role</b>	admin
<b>Example</b>	<pre>switch (config) # show access-lists log config access-list log configuration:     Memory packets:      1000     Syslog packets:     10     Interval (minutes): 60</pre>
<b>Related Commands</b>	
<b>Note</b>	

## 5.11 OpenFlow

MLNX-OS® supports OpenFlow 1.0 (on SwitchX®) and 1.3 (on Spectrum™). OpenFlow is a network protocol that facilitates direct communication between network systems via Ethernet. Software Defined Networks (SDN) allows a centralist management of network equipment. OpenFlow allows the SDN controller to manage SDN equipment. The OpenFlow protocol allows communication between the OpenFlow controller and OpenFlow agent.

OpenFlow is useful to manage switches and allow applications running on the OpenFlow controller to have access to the switch's data path and provide functionality such as flow steering, security enhancement, traffic monitoring and more.

The OpenFlow controller communicates with the OpenFlow switch over secured channel using OpenFlow protocol.

An OpenFlow switch contains a flow table which contains flows inserted by the OpenFlow controller. And the OpenFlow switch performs packet lookup and forwarding according to those rules.

Mellanox OpenFlow switch implementation is based on the hybrid model, allowing the coexistence of an OpenFlow pipeline and a normal pipeline. In this model, a packet is forwarded according to OpenFlow configuration, if such configuration is matched with the packet parameters. Otherwise, the packet is handled by the normal (regular forwarding/routing) pipeline.

The OpenFlow specification defines:

“OpenFlow-hybrid switches support both OpenFlow operation and normal Ethernet switching operation, i.e. traditional L2 Ethernet switching, VLAN isolation, L3 routing (IPv4 routing, IPv6 routing...), ACL and QoS processing. Those switches must provide a classification mechanism outside of OpenFlow that routes traffic to either the OpenFlow pipeline or the normal pipeline. For example, a switch may use the VLAN tag or input port of the packet to decide whether to process the packet using one pipeline or the other, or it may direct all packets to the OpenFlow pipeline.”

Utilizing the built-in capabilities of the hybrid switch/router is the main benefit of the hybrid mode. It increases network performance and efficiency – faster processing of new flows as well as lower load on the controllers. The hybrid switch processes non-OpenFlow data through its local management plane and achieve better efficiency and use of resources, compared to the pure OpenFlow switch.

### 5.11.1 Flow Table

The flow table contains flows which are used to perform packet lookup, modification and forwarding. Each flow has a 12 tuple key. The key is used in order to classify a packet into a certain flow. The key contains the flowing fields: ingress port, source MAC, destination MAC, Ether-Type, VLAN ID, PCP, source IP, destination IP, IP protocol, IP ToS bits, TCP/UDP source port and TCP/UDP destination port.

The flow key can have a specific value for each field or wildcard which signals to the switch to ignore this part of the key.

Each packet passes through the flow table once a match is found; the switch performs the actions configured to the specific flow by the OpenFlow controller.

Upkeeping a flow table enables the switch to forward incoming traffic with a simple lookup on its flow table entries. OpenFlow switches perform a check for matching entries on, or ignore using a wildcard, specific fields of the ingress traffic. If the entry exists, the switch performs the action associated with that flow entry. Packets without a flow entry match are forwarded according to the normal pipeline (hybrid switch).

Every flow entry contains one of the following parameters:

1. Header fields for matching purposes with each entry containing a specific value or a wildcard which could match all entries.
2. Matching packet counters which are useful for statistical purposes, in order to keep track of the number of packets.
3. Actions which specify the manner in which to handle the packets of a flow which can be any of the following:
  - Forwarding the packet
  - Dropping the packet
  - Forwarding the packet to the OpenFlow controller
  - Modifying the VLAN, VLAN priority (PCP), and/or stripping the VLAN header



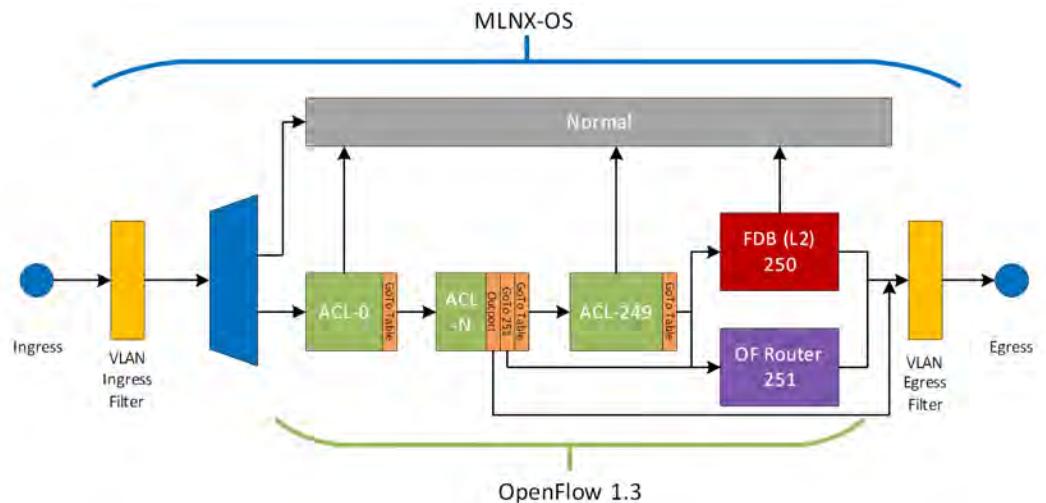
The flow table on SwitchX® supports up to 1000 flows.

### 5.11.2 OpenFlow 1.3 Support

The OpenFlow (OF) pipeline is deployed in parallel to the usual MLNX-OS® pipeline.

The ingress port must be deployed in hybrid mode so as to serve both the OF and normal MLNX-OS pipeline.

**Figure 24: MLNX-OS and OpenFlow Pipeline**



The ingress packet which passes the VLAN filter and is a match to the user ACL tables either progresses to the regular MLNX-OS flow, or the OpenFlow pipeline depending on the port coupling.

Table 55 presents a general summary of the capabilities of the OpenFlow 1.3 pipeline, which are described in detail further on in the document.

**Table 55 - OpenFlow 1.3 Pipeline Capabilities Summary Table**

Table	Match	Actions	Group	Meters
ACLs [0-249]	<ul style="list-style-type: none"> <li>• in_port</li> <li>• dl_src</li> <li>• dl_dst</li> <li>• dl_type</li> <li>• vlan_vid</li> <li>• vlan_pcp</li> <li>• ip_src</li> <li>• ip_dst</li> <li>• ipv6_dst</li> <li>• ipv6_src</li> <li>• ip_proto</li> <li>• ip_dscp</li> <li>• ip_ecn</li> <li>• ip_ttl</li> <li>• 14_src_poert</li> <li>• 14_dst_port</li> <li>• metadata 0xFFFF (Dynamic key) (Arbitrary mask)</li> </ul>	<ul style="list-style-type: none"> <li>• Push/pop</li> <li>• VLAN</li> <li>• SET_TTL</li> <li>• DEC_TTL</li> <li>• Set queue</li> <li>• Eth SRC/DST MAC</li> <li>• VLAN ID</li> <li>• PCP</li> <li>• DSCP</li> <li>• ECN</li> <li>• Output</li> <li>• Group</li> <li>• Meters</li> <li>• Normal</li> </ul>	<ul style="list-style-type: none"> <li>• ALL - Output ports</li> <li>• Select - {weights}</li> <li>Output ports (without LAG)</li> <li>• FF - Output ports</li> </ul>	<ul style="list-style-type: none"> <li>• KBPS/ PKTS - {Burst}</li> <li>• Drop</li> </ul>
FDB [250]	<ul style="list-style-type: none"> <li>• vlan_vid</li> <li>• dl_dst (Exact match)</li> </ul>	<ul style="list-style-type: none"> <li>• OUTPUT</li> <li>• DROP</li> <li>• Normal</li> </ul>	Select - {Weights} Output ports (without LAG)	N/A
Router [251]	<ul style="list-style-type: none"> <li>• ipv4_dst</li> <li>• ipv6_dst (LPM)</li> </ul>	<ul style="list-style-type: none"> <li>• DEC_TTL</li> <li>• SET_DMCA</li> <li>• OUTPUT</li> <li>• DROP</li> <li>(Must have DEC_TTL and SET_DMCA when Output action is implemented)</li> </ul>	Select - {Weights} Output ports + set_d-mac + dec_tll	N/A

### 5.11.2.1 ACL Rule Tables (0-249)

An Access Control List (ACL) is a list of permissions attached to an object, to filter or match switches packets. When the pattern is matched at the hardware lookup engine, a specified action (e.g. permit/deny) is applied. The rule fields represent flow characteristics such as source and destination addresses, protocol and VLAN ID.

ACL support currently allows actions of permit or deny rules, and supports only ingress direction. ACL search pattern can be taken from either L2 or L3 fields.

### 5.11.2.1.1 Supported ACL Matching Rules

Ingress packets, arriving the ACL, are matched against any combination of the following parameters (defined as the key):

- OXM\_OF\_METADATA – matches according to metadata
- OXM\_OF\_IN\_PORT – matches according to ingress port (exact match or wildcard)
- OXM\_OF\_ETH\_SRC – matches source MAC address
- OXM\_OF\_ETH\_DST – matches destination MAC address
- OXM\_OF\_ETH\_TYPE – matches EtherType



When match rule is set to match eth\_type 9100, VLAN ID matching does not work.

- OXM\_OF\_VLAN\_VID – matches VLAN ID
- OXM\_OF\_VLAN\_PCP – matches priority level
- OXM\_OF\_IPV4\_SRC – matches source IPv4 address
- OXM\_OF\_IPV4\_DST – matches destination IPv4 address
- OXM\_OF\_IPV6\_SRC – matches source IPv6 address
- OXM\_OF\_IPV6\_DST – matches destination IPv6 address
- OXM\_OF\_IPV6\_ND\_TARGET



OXM\_OF\_IPV6\_ND\_TARGET match rule is not supported.

- OXM\_OF\_IP\_PROTO – matches IP protocols (exact match or wildcard)
- OXM\_OF\_IP\_DSCP – matches IP DSCP field (exact match or wildcard)
- OXM\_OF\_IP\_ECN – matches network ECN (exact match or wildcard)
- OXM\_OF\_NW\_TTL – matches network TTL (exact match or wildcard)
- OXM\_OF\_TCP\_SRC – matches source TCP
- OXM\_OF\_TCP\_DST – matches destination TCP
- OXM\_OF\_UDP\_SRC – matches source UDP
- OXM\_OF\_UDP\_DST – matches destination UDP
- OXM\_OF\_SCTP\_SRC – matches source SCTP
- OXM\_OF\_SCTP\_DST – matches destination SCTP
- OXM\_OF\_ICMPV4\_TYPE – matches ICMP type
- OXM\_OF\_ICMPV4\_CODE – matches ICMP code
- OXM\_OF\_ARP\_OP – matches ARP OP code
- OXM\_OF\_ARP\_SPA – matches sender protocol address
- OXM\_OF\_ARP\_TPA – matches target protocol address

There is a default set of match keys configured. To see what it is, please run the command “show openflow table match-keys” on your machine. To alter it, please use the command “openflow table match-keys”.

#### 5.11.2.1.2 Supported Rule Table Instructions

The intercepted packet is processed according to the instructions on the rule tables. The supported instructions are as follows:

- DROP - drops packet
- OFPIT\_GOTO\_TABLE – sends the packet for processing by another rule table
- OFPIT\_METER - policer function; drops packet if it exceeds kbps/pkts limit
- OFPIT\_WRITE\_METADATA – writes meta-data with mask <METADATA>/0xFFFF
- OFPIT\_EXPERIMENTE – sends the packet for processing by another controller
- OFPIT\_APPLY\_ACTIONS – applies certain actions specified in the section below

#### 5.11.2.1.3 Supported ACL Apply Actions

The following actions are applied on ingress packets once a match is achieved on the ACL table:

- OFPAT\_OUTPUT – the packet is sent out to a port (may also be a controller port)
- OFPAT\_GROUP – the packet is sent out to a group

3 types of group ports are supported:

- All: The packet is broadcasted on all ports which are part of the defined group
- Selected: The packets are distributed toward the group ports according to a weight mechanism
- Fast-Failover (FF): FF is a group of ports, one of which is defined as the primary port through which the packets are transported. In a failure scenario (defined as part of the group definition), traffic becomes transported through the most eligible backup port (from the list of backup ports). Once the failure scenario ends, traffic is routed again through the primary port
- OFPAT\_POP\_VLAN – strips 802.1Q (VLAN) tag from the packet
- OFPAT\_PUSH\_VLAN – adds 802.1Q (VLAN) tag from the packet
- OFPAT\_SET\_NW\_TTL – modifies network TTL
- OFPAT\_DEC\_NW\_TTL – decrements network TTL
- OFPAT\_SET\_FIELD – ACL set fields detailed in section below
- Normal

#### 5.11.2.1.4 Supported ACL Set Fields

The following modifications may be implemented on ingress packets:

- OXM\_OF\_ETH\_SRC – sets the source MAC address of the packet
- OXM\_OF\_ETH\_DST – sets the destination MAC address of the packet
- OXM\_OF\_VLAN\_VID – sets the VLAN ID of the packet

- OXM\_OF\_VLAN\_PCP – sets the VLAN priority code point (PCP; 0-7)
- OXM\_OF\_IP\_DSCP – sets IP DSCP
- OXM\_OF\_IP\_ECN – sets network ECN

#### 5.11.2.1.5 Supported ACL Meters

- ACL tables support up to 968 meters with 1 band (drop) per meter.
  - Valid meter ID range: 1-969
  - Only the rate or the burst size fields can be modified using OFPMC MODIFY
  - OFPMF\_BURST meter type can be OFPMF\_KBPS (KB/s) or OFPMF\_PKTPS (number of packets per second) but not both
- Meter actions:
- OFPMBT\_DROP – drops packet according to meter configuration

#### 5.11.2.2 FDB Table (250)

The FDB table is the same one shared with regular MLNX-OS® configuration (e.g. learning, static macs, etc). The cumulative number of supported FDB rules is 88KB. FDB may only configure rules with priority of 0x8000. Hard timeout is supported for FDB table rules. FDB rules cannot have wildcard on VID/ETH\_DST.

The default action for the FDB table is normal and this cannot be changed by the user.

#### 5.11.2.2.1 Supported FDB Apply Actions

- OFPAT\_OUTPUT – the packet is sent out to a port (may be controller port)
- DROP – drops packet
- Normal

#### 5.11.2.2.2 Supported FDB Matching Rules

- OXM\_OF\_VLAN\_VID – matches VLAN ID
- OXM\_OF\_ETH\_DST – matches destination MAC address

#### 5.11.2.3 Router Table (251)

The OpenFlow router table and the regular MLNX-OS router table share the same HW resources, but are separated logically.

The cumulative number of supported FDB & router rules is 88K. Hard timeout, where the switch removes a rule after a configured timer expires, is supported for router table rules. Switch systems ignore rule priority and configure rules according to masklen in DST IPv4/IPv6 match. A rule with action output must have SET\_FIELD with ETH\_DST and DEC\_NW\_TTL. The default action for the router table is DROP.

Set DMAC can be assigned only to one output port. When a new rule with a set DMAC and a new output port is configured, the previous rules are removed from the HW. Later, if the new configuration is deleted, the previous rules get reinstalled in HW.

Note that all sent packets from the Router Table are without a VLAN header (untagged).

#### 5.11.2.3.1 Supported Router Apply Actions

- OFPAT\_OUTPUT – the packet is sent out to a port (may be controller port)
- OFPAT\_DEC\_NW\_TTL – decrements network TTL
- OFPAT\_SET\_DMAC – OFPAT\_SET\_FIELD with OFPXMT\_OFB\_ETH\_DST
- DROP – drops packet



When an output action is implemented, DEC\_TTL and SET\_DMAC must also be set.

#### 5.11.2.3.2 Supported Router Set Fields

- OXM\_OF\_ETH\_DST – sets the destination MAC address of the packet

#### 5.11.2.3.3 Supported Router Matching Rules

- OXM\_OF\_IPV4\_DST – matches destination IPv4 address
- OXM\_OF\_IPV6\_DST – matches destination IPv6 address

### 5.11.3 Configuring OpenFlow

➤ **To run OpenFlow on a switch:**

**Step 1.** Unlock the OpenFlow CLI commands. Run:

```
switch (config) # protocol openflow
```

**Step 2.** Configure interfaces to be managed by OpenFlow. Run:

```
switch (config) # interface ethernet 1/1-1/4 openflow mode hybrid
```

**Step 3.** Configure the OpenFlow controller IP and TCP port. Run:

```
switch (config) # openflow controller-ip 10.209.0.205 tcp-port 6633
```



Spectrum™ based systems do not support a different controller port other than the default (6633).

**Step 4.** (Optional) Verify the OpenFlow configuration. Run:

```
switch (config) # show openflow
OpenFlow version: OF VERSION 1.0
Table size: 1000, 0 in use
Active controller ip: 10.209.0.205 port: 6633
Connection status: HANDSHAKE_COMPLETE (CONNECTED)
Forward-to-controller: ospf lldp arp-unicast arp-broadcast (all)
Enabled ports: Eth1/1      Eth1/2      Eth1/3      Eth1/4
switch (config) #
```



To be able to configure the switch using the controller, you should see the following line in the output:  
Connection status must be: HANDSHAKE\_COMPLETE (CONNECTED).

#### 5.11.4 Configuring Secure Connection to OpenFlow

Since OpenFlow requires a certificate signed by the certificate authority (CA), the default certificate, which is self-signed, must be replaced.

➤ *Changing default certificate for secure OpenFlow connection:*

**Step 1.** Import the certificate to be used. Run:

```
switch (config) # crypto certificate name my-openflow public-cert pem "-----BEGIN CERTIFICATE-----
> MIIDYzCCAksCCQC9EPbMuxjNBzANBgkqhkiG9w0BAQsFADBeMQswCQYDVQQGEwJJ
...
> fEt2ui9taBldl9480xDsGUxwUDX4Y0s/bQDjp99z+cKXUe2eYzeEwnTdrCzPZuQo
> -----END CERTIFICATE-----"
Successfully installed certificate with name 'my-openflow'
```

**Step 2.** Import key of certificate. Run:

```
switch (config) # crypto certificate name my-openflow private-key pem "-----BEGIN RSA PRIVATE KEY-----
> MIIEpAIBAAKCAQEApJnZkbhmt71Kf/M06cy7QmWWHhCozzWRwuWGKse+MxSmfC
...
> QAuPOVR1lSyIEnYU+X0rMhc/9tgUh/8C7mBKwj7dccMmnRWz2djsjg==
> -----END RSA PRIVATE KEY-----"
```

**Step 3.** Designate “my-openflow” as the global default certificate for authentication of this system to clients. Run:

```
switch (config) # crypto certificate default-cert name my-openflow
```

**Step 4.** Import the CA certificate which signed for the controller. Run:

```
switch (config) # # crypto certificate name rootCA public-cert pem "-----BEGIN CERTIFICATE-----
> MIIDjzCCAnegAwIBAgIJALVou4mcQtxlMA0GCSqGSIb3DQEBCwUAMF4xCzAJBgNV
...
> +ZfQIOCF8gY4BDq73W4ugr38mqIA8UXXAMPwgjCbk4Ny0h0rJ1P6WT8fYzvunct
> -----END CERTIFICATE-----"
Successfully installed certificate with name 'rootCA'
```

**Step 5.** Adds the “rootCA” to the default CA certificate list. Run:

```
switch (config) # crypto certificate ca-list default-ca-list name rootCA
```

**Step 6.** Save configuration. Run:

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

**Step 7.** Reboot the switch. Run:

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

**Step 8.** Verify configuration. Run:

```
switch (config) # show crypto certificate
Certificate with name 'system-self-signed'
    Comment:                                     system-generated self-signed certificate
    Private Key:                                present
    Serial Number:                             0x543e2efc3a5ecdbe18b5b5e744598424
    SHA-1 Fingerprint:                         14e1d36035c7a5fea9f7f0f423572c9954cb9fac

    Validity:
        Starts:                               2016/09/12 12:44:10
        Expires:                             2017/09/12 12:44:10

    Subject:
        Common Name:                      switch
        Country:                           IS
        State or Province:                TBD
        Locality:                          TBD
        Organization:                     TBD
        Organizational Unit:              TBD
        E-mail Address:                   TBD

    Issuer:
        Common Name:                      switch
        Country:                           IS
        State or Province:                TBD
        Locality:                          TBD
        Organization:                     TBD
        Organizational Unit:              TBD
        E-mail Address:                   TBD
```

```
Certificate with name 'my-openflow' (default-cert)
  Private Key: present
  Serial Number: 0xbd10f6ccb18cd07
  SHA-1 Fingerprint: 1e0e3302182ab56f2cbd3ca21722dec55299d670

  Validity:
    Starts: 2016/09/12 15:16:48
    Expires: 2018/01/25 14:16:48

  Subject:
    Common Name: switch
    Country: *
    State or Province: Some-State
    Locality: *
    Organization: Mlnx
    Organizational Unit: e2e
    E-mail Address: none@nowhere.com

  Issuer:
    Common Name: ca
    Country: *
    State or Province: Some-State
    Locality: *
    Organization: Mlnx
    Organizational Unit: e2e

Certificate with name 'rootCA'
  Private Key: not present
  Serial Number: 0xb568bb899c42dc65
  SHA-1 Fingerprint: 9855536f6ee0177356ffbd54ffe803bc83fb4c6

  Validity:
    Starts: 2016/09/08 10:34:23
    Expires: 2019/06/29 10:34:23

  Subject:
    Common Name: ca
    Country: *
    State or Province: Some-State
    Locality: *
    Organization: Mlnx
    Organizational Unit: e2e

  Issuer:
    Common Name: ca
    Country: *
    State or Province: Some-State
    Locality: *
    Organization: Mlnx
    Organizational Unit: e2e
```

**Step 9.** Configure secure controller IP connection. Run:

```
switch (config) # controller-ip 10.10.10.10 tls
```

## 5.11.5 Commands

### protocol openflow

**protocol openflow**  
**no protocol openflow**

Unhides the OpenFlow commands.

The no form of the command hides the OpenFlow commands.

---

**Syntax Description** N/A

**Default** no protocol openflow

**Configuration Mode** Config

**History** 3.3.4200

**Role** admin

**Example**  
switch (config) # protocol openflow  
switch (config) #

---

**Related Commands**

---

**Note**

## openflow description (SwitchX)

**openflow description <string>**

Sets the OpenFlow description.

<b>Syntax Description</b>	string	Free string.
<b>Default</b>	N/A	
<b>Configuration Mode</b>	Config	
<b>History</b>	3.3.4302	
	3.6.1002	Updated Note
<b>Role</b>	admin	
<b>Example</b>	<pre>switch (config) # openflow description OF-switch-104 switch (config) # show openflow detail OpenFlow version: OF VERSION 1.0 Table size: 1000, 0 in use Active controller ip: 10.209.1.39 port: 6633 Connection status: HANDSHAKE_COMPLETE (CONNECTED) Forward-to-controller: ospf lldp arp-unicast arp-broadcast (all) Enabled ports: Eth1/10 Eth1/11 Eth1/13 Eth1/19 Echo period: 10 sec Keep alive period: 30 sec Messages in (last session): 86290 Messages out (last session): 47984 Disconnect count: 0 Openflow description: OF-switch-104 Datapath ID: 00:00:00:02:c9:a8:e3:50 Not supporting buffering Not supporting emergency flows Not supporting port statistics Not supporting IP reassemble Supporting spanning tree Not supporting queue statistics switch (config) #</pre>	
<b>Related Commands</b>		
<b>Note</b>	Not supported on Spectrum based switch systems	

## openflow mode hybrid

**openflow mode hybrid**  
**no openflow mode**

Enables OpenFlow on the port.

The no form of the command returns the port to its default state.

<b>Syntax Description</b>	N/A
<b>Default</b>	no openflow mode
<b>Configuration Mode</b>	Config Interface Ethernet
<b>History</b>	3.3.4200
	3.6.2100 Updated Note section
<b>Role</b>	admin
<b>Example</b>	<pre>switch (config interface etherent 1/1)# openflow mode hybrid switch (config interface etherent 1/1)#+</pre>
<b>Related Commands</b>	
<b>Note</b>	On Spectrum™ based systems, it is possible to run “interface port-channel <port number> openflow mode hybrid”.

## openflow add-flows

**openflow add-flows <FLOW ID> [FLOW-TEXT]**

The command adds OpenFlow Flow.  
If FLOW-TEXT is not provided the commands deletes the configured OpenFlow flows.

<b>Syntax Description</b>	FLOW ID Range: 0 - 65535
	FLOW-TEXT Text of the flow configuration
<b>Default</b>	N/A
<b>Configuration Mode</b>	Config Interface Ethernet
<b>History</b>	3.6.4006
<b>Role</b>	admin
<b>Example</b>	<pre>switch (config interface etherent 1/1)# openflow add-flows switch (config interface etherent 1/1)#{</pre>
<b>Related Commands</b>	
<b>Note</b>	

## openflow add-group

**openflow add-group <GROUP-TEXT>**

The command Adds OpenFlow Group.

<b>Syntax Description</b>	GROUP-TEXT	Text of the group configuration		
<b>Default</b>	N/A			
<b>Configuration Mode</b>	Config Interface Ethernet			
<b>History</b>	3.6.4006			
<b>Role</b>	admin			
<b>Example</b>	<pre>switch (config interface etherent 1/1)# openflow add-group switch (config interface etherent 1/1)#{</pre>			
<hr/>				
<b>Related Commands</b>				
<hr/>				
<b>Note</b>				
<hr/>				

## openflow mod-group

**openflow mod-group <GROUP-TEXT>**

The command modifies matching OpenFlow GROUP ID.

<b>Syntax Description</b>	GROUP-TEXT	Text of the group configuration		
<b>Default</b>	N/A			
<b>Configuration Mode</b>	Config Interface Ethernet			
<b>History</b>	3.6.4006			
<b>Role</b>	admin			
<b>Example</b>	<pre>switch (config interface etherent 1/1)# openflow mod-group switch (config interface etherent 1/1)#{</pre>			
<hr/>				
<b>Related Commands</b>				
<hr/>				
<b>Note</b>				
<hr/>				

## openflow del-group

**openflow del-group <GROUP-TEXT>**

The command deletes matching OpenFlow GROUP ID.

<b>Syntax Description</b>	GROUP-TEXT	Text of the group configuration		
<b>Default</b>	N/A			
<b>Configuration Mode</b>	Config Interface Ethernet			
<b>History</b>	3.6.4006			
<b>Role</b>	admin			
<b>Example</b>	<pre>switch (config interface etherent 1/1)# openflow del-group switch (config interface etherent 1/1)#{</pre>			
<hr/>				
<b>Related Commands</b>				
<hr/>				
<b>Note</b>				
<hr/>				

## openflow add-meter

**openflow add-meter <METER-TEXT>**

The command adds OpenFlow Meter.

<b>Syntax Description</b>	METER-TEXT	Text of the meter configuration		
<b>Default</b>	N/A			
<b>Configuration Mode</b>	Config Interface Ethernet			
<b>History</b>	3.6.4006			
<b>Role</b>	admin			
<b>Example</b>	<pre>switch (config interface etherent 1/1)# openflow add-meter switch (config interface etherent 1/1)#{</pre>			
<hr/>				
<b>Related Commands</b>				
<hr/>				
<b>Note</b>				
<hr/>				

## openflow mod-meter

**openflow mod-meter <METER-TEXT>**

The command modifies matching OpenFlow METER ID.

<b>Syntax Description</b>	METER-TEXT	Text of the meter configuration		
<b>Default</b>	N/A			
<b>Configuration Mode</b>	Config Interface Ethernet			
<b>History</b>	3.6.4006			
<b>Role</b>	admin			
<b>Example</b>	<pre>switch (config interface etherent 1/1)# openflow mod-meter switch (config interface etherent 1/1)#{</pre>			
<hr/>				
<b>Related Commands</b>				
<hr/>				
<b>Note</b>				
<hr/>				

## openflow del-meter

**openflow del-meter <METER-TEXT>**

The command deletes matching OpenFlow METER ID.

<b>Syntax Description</b>	METER-TEXT	Text of the meter configuration		
<b>Default</b>	N/A			
<b>Configuration Mode</b>	Config Interface Ethernet			
<b>History</b>	3.6.4006			
<b>Role</b>	admin			
<b>Example</b>	<pre>switch (config interface etherent 1/1)# openflow del-meter switch (config interface etherent 1/1)#{</pre>			
<hr/>				
<b>Related Commands</b>				
<hr/>				
<b>Note</b>				
<hr/>				

## openflow re-apply flows

**openflow re-apply flows <FLOW-ID>**

The command re-applies matching FLOW ID.

<b>Syntax Description</b>	FLOW-ID	Range: 0 - 65535		
<b>Default</b>	N/A			
<b>Configuration Mode</b>	Config Interface Ethernet			
<b>History</b>	3.6.4006			
<b>Role</b>	admin			
<b>Example</b>	switch (config interface etherent 1/1)# openflow re-apply flows switch (config interface etherent 1/1)#{/td} <td data-kind="ghost"></td>			
<b>Related Commands</b>				
<b>Note</b>				

## openflow re-apply groups

**openflow re-apply groups <GROUP-ID>**

The command re-applies matching GROUP ID.

<b>Syntax Description</b>	GROUP-ID	Range: 0 - 65535		
<b>Default</b>	N/A			
<b>Configuration Mode</b>	Config Interface Ethernet			
<b>History</b>	3.6.4006			
<b>Role</b>	admin			
<b>Example</b>	switch (config interface etherent 1/1)# openflow re-apply groups switch (config interface etherent 1/1)#{/td} <td data-kind="ghost"></td>			
<b>Related Commands</b>				
<b>Note</b>				

## openflow re-apply meters

**openflow re-apply meters <METER-ID>**

The command re-applies matching METER ID.

<b>Syntax Description</b>	METER-ID	Range: 0 - 65535		
<b>Default</b>	N/A			
<b>Configuration Mode</b>	Config Interface Ethernet			
<b>History</b>	3.6.4006			
<b>Role</b>	admin			
<b>Example</b>	switch (config interface etherent 1/1)# openflow re-apply meters switch (config interface etherent 1/1)#{			
<b>Related Commands</b>				
<b>Note</b>				

## controller-ip

```
openflow controller-ip <ip-address> [tls] [tcp-port <tcp-port>]  
no openflow controller-ip <ip-address>
```

Sets the OpenFlow controller's IP & TCP port.

The no form of the command sets the parameter to its default.

<b>Syntax Description</b>	ip-address	The IPv4 address of the OpenFlow controller
	tls	Configures secure connection to OpenFlow controller
	tcp-port	Sets the TCP port number of the OpenFlow controller
<b>Default</b>	TCP port 6633	
<b>Configuration Mode</b>	Config OpenFlow	
<b>History</b>	3.6.1002	
	3.6.2002	Added “tls” parameter
<b>Role</b>	admin	
<b>Example</b>	switch (config openflow) # controller-ip 10.10.10.10 tls tcp-port 6633	
<b>Related Commands</b>		
<b>Note</b>	This command is only supported on Spectrum™ based switch systems	

## controller-ip

```
openflow controller-ip <ip-address> [tcp-port <tcp-port>]  
no openflow controller-ip [tcp-port <tcp-port>]
```

Sets the OpenFlow controller's IP & TCP port.  
The no form of the command sets the parameter to its default.

<b>Syntax Description</b>	ip-address	The IPv4 address of the OpenFlow controller
	tcp-port	Sets the TCP port number of the OpenFlow controller
<b>Default</b>	TCP port 6633	
<b>Configuration Mode</b>	Config OpenFlow	
<b>History</b>	3.3.4200	
<b>Role</b>	admin	
<b>Example</b>	switch (config openflow) # controller-ip 10.10.10.10 tcp-port 6633	
<b>Related Commands</b>		
<b>Note</b>	This command is only supported on SwitchX based switch systems	

## datapath-id

**datapath-id <value>**  
**no datapath-id**

Sets a specific identifier for the switch with which the controller is communicating.  
The no form of the command resets the parameter to its default value.

<b>Syntax Description</b>	value	The most significant 16 bits of the agent data-path ID. Range is 0x0000-0xFFFF in hexa.		
<b>Default</b>	0x0000			
<b>Configuration Mode</b>	Config OpenFlow			
<b>History</b>	3.3.4200			
<b>Role</b>	admin			
<b>Example</b>	<pre>switch (config openflow) # datapath-id 0x1234 switch (config openflow) #</pre>			
<b>Related Commands</b>				
<b>Note</b>				

## forward-to-controller

**forward-to-controller {[ospf] [lldp] [arp-unicast] [arp-broadcast] all | none}**

Forwards the selected traffic types to the controller from all the ports on which OpenFlow enabled.

<b>Syntax Description</b>	ospf	Forwards OSPF traffic to the controller
	lldp	Forwards LLDP traffic to the controller
	arp-unicast	Forwards ARP-unicast traffic to the controller
	arp-broadcast	Forwards ARP-broadcast traffic to the controller
	all	Forwards all traffic types to the controller
	none	Forwards no traffic to the controller
<b>Default</b>	None	
<b>Configuration Mode</b>	Config OpenFlow	
<b>History</b>	3.3.4200	
<b>Role</b>	admin	
<b>Example</b>	<pre>switch (config openflow) # forward-to-controller all switch (config openflow) #</pre>	
<b>Related Commands</b>		
<b>Note</b>	This command is only supported on SwitchX based switch systems	

## openflow table match-keys

```
openflow table <table_id[-table_id]> match-keys <key_list>
no openflow table <table_id[-table_id]> match-keys [<key_list>]
```

Adds ACL keys to an OpenFlow table.

The no form of the command removes ACL keys from the OpenFlow table.

<b>Syntax Description</b>	table_id	OpenFlow table ID for adding/removing key values. Can be one ID or range. Valid values: 0-249.
	key_list	Key value(s)
<b>Default</b>	N/A	
<b>Configuration Mode</b>	Any Command Mode	
<b>History</b>	3.6.3004	
<b>Role</b>	admin	
<b>Example</b>	switch (config) # openflow table 1 match-keys metadata ip_proto	
<b>Related Commands</b>		
<b>Note</b>	<ul style="list-style-type: none"><li>• OpenFlow match rules are installed according to the configured match keys</li><li>• New match keys are configured only when the table is empty (i.e. does not contain any rules)</li><li>• This command is only supported on Spectrum™ based switch systems</li></ul>	

## show openflow

### show openflow

Displays general information about the OpenFlow protocol configuration.

<b>Syntax Description</b>	N/A
<b>Default</b>	None
<b>Configuration Mode</b>	Any Command Mode
<b>History</b>	3.3.4200 3.3.4302                          Removed flow-id parameter 3.6.1002                          Updated Example
<b>Role</b>	admin
<b>Example</b>	<pre> switch (config) # show openflow OpenFlow Version: OpenFlow 1.3 Datapath ID: ffff7cfce90e600c0 Controllers Information: Controller                State                Role                Changed (sec)    Last Error -----                -----                -----                -----            ----- tcp:1.1.1.1:6633        BACKOFF            other              3                Connection timed out tcp:10.10.10.10:6633    ACTIVE            other             2067            N/A tcp:10.10.10.30:6633    ACTIVE            other             2067            N/A  Mapping of OpenFlow ports to their OpenFlow numbers: Interface    OF-Port -----        ----- Eth1/12        OF107 Eth1/9         OF109 Eth1/10        OF111 Eth1/7         OF113 Eth1/8         OF115 Eth1/3         OF121 Eth1/4         OF123 </pre>
<b>Related Commands</b>	
<b>Note</b>	This command is only supported on Spectrum™ based switch systems

## show openflow detail

### show openflow detail

Displays detailed information about the OpenFlow protocol.

<b>Syntax Description</b>	N/A	
<b>Default</b>	None	
<b>Configuration Mode</b>	Any Command Mode	
<b>History</b>	3.3.4200	
	3.6.1002	Updated Example
<b>Role</b>	admin	
<b>Example</b>	<pre>switch (config) # show openflow detail Echo period: 0 sec Keep alive period: 0 sec Messages in (last session): 0 Messages out (last session): 0 Disconnect count: 0 Openflow description: Datapath ID: 02:10:e4:52:14:5d:76:70 Not supporting buffering Not supporting emergency flows Not supporting port statistics Not supporting IP reassemble Supporting spanning tree Not supporting queue statistics</pre>	
<b>Related Commands</b>		
<b>Note</b>	This command is only supported on SwitchX® based switch systems	

## show openflow flows

### show openflow flows

Displays information about the OpenFlow flows.

<b>Syntax Description</b>	N/A
<b>Default</b>	None
<b>Configuration Mode</b>	Any Command Mode
<b>History</b>	3.3.4302
	3.6.1002 Updated Example
<b>Role</b>	admin
<b>Example</b>	<pre>switch (config) # show openflow flows OFPST_FLOW reply (OF1.3) (xid=0x2): cookie=0x0, duration=467.993s, table=0, n_packets=0, n_bytes=0, send_flow_rem priority=8,in_port=125 actions=output:123 cookie=0x0, duration=439.218s, table=0, n_packets=0, n_bytes=0, send_flow_rem priority=9999,in_port=125 actions=output:123 cookie=0x0, duration=467.984s, table=0, n_packets=0, n_bytes=0, send_flow_rem priority=1000 actions=drop cookie=0x0, duration=467.975s, table=0, n_packets=0, n_bytes=0, send_flow_rem priority=200,dl_vlan=222 actions=pop_vlan,output:123 cookie=0x0, duration=467.987s, table=0, n_packets=0, n_bytes=0, send_flow_rem priority=10,dl_vlan=10 actions=output:123 cookie=0x0, duration=468.013s, table=0, n_packets=0, n_bytes=0, send_flow_rem priority=8,dl_dst=01:01:01:01:01:01 actions=output:123 cookie=0x0, duration=467.991s, table=0, n_packets=0, n_bytes=0, send_flow_rem priority=8,dl_src=01:01:01:01:01:01 actions=output:123 cookie=0x0, duration=467.992s, table=0, n_packets=0, n_bytes=0, send_flow_rem priority=5,arp actions=output:123</pre>
<b>Related Commands</b>	
<b>Note</b>	

## show openflow flows ethernet-names

**show openflow flows < |cookie|table > ethernet-names**

Displays openflow flows configuration with interface names.

<b>Syntax Description</b>	N/A
<b>Default</b>	None
<b>Configuration Mode</b>	Config
<b>History</b>	3.6.4006
<b>Role</b>	admin
<b>Example</b>	<pre>switch (config) # show openflow flows ethernet-names OFPST_FLOW reply (OF1.3) (xid=0x2): cookie=0x0, duration=911.531s, table=0, n_packets=0, n_bytes=0, priority=0 actions=NORMAL cookie=0x0, duration=80.662s, table=1, n_packets=0, n_bytes=0, priority=0,in_port=0,dl_src=02:00:00:00:00:00 actions=output:Eth1/ 13,output:123,output:127 cookie=0x0, duration=80.530s, table=1, n_packets=0, n_bytes=0, priority=1,in_port=1,dl_src=02:01:00:00:00:00 actions=output:Eth1/ 13,output:123,output:127 cookie=0x0, duration=80.414s, table=1, n_packets=0, n_bytes=0, priority=2,in_port=2,dl_src=02:02:00:00:00:00 actions=output:Eth1/ 13,output:123,output:127 cookie=0x0, duration=80.296s, table=1, n_packets=0, n_bytes=0, priority=3,in_port=3,dl_src=02:03:00:00:00:00 actions=output:Eth1/ 13,output:123,output:127 cookie=0x0, duration=80.180s, table=1, n_packets=0, n_bytes=0, priority=4,in_port=4,dl_src=02:04:00:00:00:00 actions=output:Eth1/ 13,output:123,output:127 cookie=0x0, duration=80.064s, table=1, n_packets=0, n_bytes=0, priority=5,in_port=5,dl_src=02:05:00:00:00:00 actions=output:Eth1/ 13,output:123,output:127 cookie=0x0, duration=79.948s, table=1, n_packets=0, n_bytes=0, priority=6,in_port=6,dl_src=02:06:00:00:00:00 actions=output:Eth1/ 13,output:123,output:127 cookie=0x0, duration=79.831s, table=1, n_packets=0, n_bytes=0, priority=7,in_port=7,dl_src=02:07:00:00:00:00 actions=output:Eth1/ 13,output:123,output:127 cookie=0x0, duration=79.711s, table=1, n_packets=0, n_bytes=0, priority=8,in_port=8,dl_src=02:08:00:00:00:00 actions=output:Eth1/ 13,output:123,output:127 cookie=0x0, duration=79.591s, table=1, n_packets=0, n_bytes=0, priority=9,in_port=9,dl_src=02:09:00:00:00:00 actions=output:Eth1/ 13,output:123,output:127 cookie=0x0, duration=79.467s, table=1, n_packets=0, n_bytes=0, priority=10,in_port=10,dl_src=02:0a:00:00:00:00 actions=output:Eth1/ 13,output:123,output:127</pre>

### Related Commands

---

**Note**

---

## show openflow statistics

### show openflow statistics

Displays information about the OpenFlow flows.

<b>Syntax Description</b>	N/A	
<b>Default</b>	None	
<b>Configuration Mode</b>	Any Command Mode	
<b>History</b>	3.3.4302	
	3.6.1002	Updated Example
<b>Role</b>	admin	
<b>Example</b>	switch (config) # show openflow statistics	
<b>Related Commands</b>		
<b>Note</b>	This command is only supported on SwitchX® based switch systems	

## show openflow tables

### show openflow tables

Displays information about the OpenFlow tables (size, type, etc.).

<b>Syntax Description</b>	N/A
<b>Default</b>	None
<b>Configuration Mode</b>	Any Command Mode
<b>History</b>	3.3.4200 3.6.1002                          Added Example
<b>Role</b>	admin
<b>Example</b>	<pre>switch (config) # show openflow tables Table id: 0 Maximum table size: 1000, 0 in use Key: 12 tuple ACL Supported actions: Modify VID, Mofify PCP, Strip VID</pre>
<b>Related Commands</b>	
<b>Note</b>	This command is only supported on SwitchX® based switch systems

## show openflow

**show openflow [detail | tables | flows <id>]**

Displays general information about the OpenFlow protocol configuration.

<b>Syntax Description</b>	detail	Displays detailed information about the OpenFlow protocol.
	tables	Displays information about the OpenFlow tables (size, type, etc.).
	flows <id>	Displays specific flows inside the OpenFlow tables. ID may be a range (e.g. 1-10).
	statistics	Displays OpenFlow statistics.
<b>Default</b>	None	
<b>Configuration Mode</b>	Any Command Mode	
<b>History</b>	3.3.4200	
	3.3.4302	Removed flow-id parameter Added “flows” and “statistics” parameters
<b>Role</b>	admin	
<b>Example</b>	switch (config) # show openflow flows	
<b>Related Commands</b>		
<b>Note</b>	This command is only supported on SwitchX® based switch systems	

## show openflow groups

### show openflow groups

Displays all the configured OpenFlow groups.

<b>Syntax Description</b>	N/A
<b>Default</b>	N/A
<b>Configuration Mode</b>	Any Command Mode
<b>History</b>	3.6.3004
<b>Role</b>	admin
<b>Example</b>	<pre>switch (config) # show openflow groups OFPST_GROUP_DESC reply (OF1.3) (xid=0x2): group_id=5566,type=select,bucket=weight:5,actions=output:1,bucket=weight:7,actions=output:2,bucket=weight:22,actions=output:3</pre>
<b>Related Commands</b>	
<b>Note</b>	This command is only supported on Spectrum™ based switch systems

## show openflow groups ethernet-names

### show openflow groups ethernet-names

Displays all the configured OpenFlow groups with their interface names.

<b>Syntax Description</b>	N/A
<b>Default</b>	N/A
<b>Configuration Mode</b>	Config
<b>History</b>	3.6.4006
<b>Role</b>	admin
<b>Example</b>	<pre>switch (config) # show openflow groups OFPST_GROUP_DESC reply (OF1.3) (xid=0x2): group_id=4,type=all,bucket=actions=output:Eth1/13,output:123 group_id=1,type=select,bucket=actions=output:Eth1/7,output:Eth1/8,output:Eth1/5,output:123,set_field:11:22:33:44:00:00-&gt;eth_dst group_id=2,type=select,bucket=actions=output:Eth1/13 group_id=3,type=all,bucket=actions=output:Eth1/13,output:123,set_field:11:22:33:44:00:00-&gt;eth_dst</pre>
<b>Related Commands</b>	
<b>Note</b>	This command is only supported on Spectrum™ based switch systems

## show openflow meters

**show openflow meters [<ID>]**

Displays all/specified OpenFlow meters.

<b>Syntax Description</b>	ID	Requested meter ID
<b>Default</b>	N/A	
<b>Configuration Mode</b>	Any Command Mode	
<b>History</b>	3.6.3004	
<b>Role</b>	admin	
<b>Example</b>	<pre>switch (config) # show openflow meters OFPST_METER_CONFIG reply (OF1.3) (xid=0x2): meter=20 kbps bands= type=drop rate=300  meter=100 kbps bands= type=drop rate=500  meter=200 kbps bands= type=drop rate=500  switch (config) # show openflow meters 20 OFPST_METER_CONFIG reply (OF1.3) (xid=0x2): meter=20 kbps bands= type=drop rate=300</pre>	
<b>Related Commands</b>		
<b>Note</b>	This command is only supported on Spectrum™ based switch systems	

## show openflow flows table

**show openflow flows table <NUM> [summary]**

Displays information/summary of a given OpenFlow flows table.

<b>Syntax Description</b>	NUM summary	NUM range: 0-252 Displays given OpenFlow flow table summary
<b>Default</b>	N/A	
<b>Configuration Mode</b>	Any Command Mode	
<b>History</b>	3.6.3004	
<b>Role</b>	admin	
<b>Example</b>	<pre>switch (config) # show openflow flows table 1 OFPST_FLOW reply (OF1.3) (xid=0x2): cookie=0x0, duration=6.344s, table=1, n_packets=0, n_bytes=0, in_port=127 actions=drop  switch (config) # show openflow flows table 1 summary OFPST_AGGREGATE reply (OF1.3) (xid=0x2): packet_count=0 byte_count=0 flow_count=1</pre>	
<b>Related Commands</b>		
<b>Note</b>	This command is only supported on Spectrum™ based switch systems	

## show openflow flows cookie

**show openflow flows cookie <cookie> [summary]**

Displays information/summary of a given OpenFlow flows cookie.

<b>Syntax Description</b>	cookie	Requested cookie ID in the following format: cook- ie_id.cookie_id/mask_id (e.g. 0x2A, 0x12/0x2)
<b>Default</b>	N/A	
<b>Configuration Mode</b>	Any Command Mode	
<b>History</b>	3.6.3004	
<b>Role</b>	admin	
<b>Example</b>	<pre>switch (config) # show openflow flows cookie 0x11 OFPST_FLOW reply (OF1.3) (xid=0x2): cookie=0x11, duration=2.699s, table=0, n_packets=0, n_bytes=0, actions=NORMAL switch (config) # show openflow flows cookie 0x22 OFPST_FLOW reply (OF1.3) (xid=0x2): cookie=0x22, duration=3.970s, table=1, n_packets=0, n_bytes=0, in_port=127 actions=drop</pre>	
<b>Related Commands</b>		
<b>Note</b>	<p>A cookie may be associated with a flow using the add-flows, and mod-flows commands. This command is only supported on Spectrum™ based switch systems</p>	

## show openflow table match-keys

**show openflow table <table\_id[-table\_id]> match-keys**

Displays configured ACL keys in OpenFlow table.

<b>Syntax Description</b>	table_id	OpenFlow table ID for adding/removing key values. Can be one ID or range. Valid values: 0-249.																																
<b>Default</b>	N/A																																	
<b>Configuration Mode</b>	Any Command Mode																																	
<b>History</b>	3.6.3004																																	
<b>Role</b>	admin																																	
<b>Example</b>	<pre>switch (config) # show openflow table 2 match-keys</pre> <p>Table: 2</p> <p>Pending keys:</p> <table> <thead> <tr> <th>Key name</th> <th>Description</th> </tr> </thead> <tbody> <tr><td>in_port</td><td>Source port</td></tr> <tr><td>dl_src</td><td>Source MAC address</td></tr> <tr><td>dl_dst</td><td>Destination MAC address</td></tr> <tr><td>dl_type</td><td>Ethernet protocol type</td></tr> <tr><td>vlan_vid</td><td>Virtual LAN tag</td></tr> <tr><td>vlan_pcp</td><td>Priority Code Point</td></tr> <tr><td>ip_src</td><td>Source IPv4 address</td></tr> <tr><td>ip_dst</td><td>Destination IPv4 address</td></tr> <tr><td>ip_proto</td><td>IPV4 - Next protocol, IPV6 - Next header</td></tr> <tr><td>ip_dscp</td><td>IP ToS/DSCP or IPV6 traffic class field dscp</td></tr> <tr><td>ip_ecn</td><td>ECN bits from IP header</td></tr> <tr><td>ip_ttl</td><td>IP TTL or IPv6 hop limit</td></tr> <tr><td>l4_src_port</td><td>Source L4 port</td></tr> <tr><td>l4_dst_port</td><td>Destination L4 port</td></tr> <tr><td>metadata</td><td>Matches value in the metadata field</td></tr> </tbody> </table>		Key name	Description	in_port	Source port	dl_src	Source MAC address	dl_dst	Destination MAC address	dl_type	Ethernet protocol type	vlan_vid	Virtual LAN tag	vlan_pcp	Priority Code Point	ip_src	Source IPv4 address	ip_dst	Destination IPv4 address	ip_proto	IPV4 - Next protocol, IPV6 - Next header	ip_dscp	IP ToS/DSCP or IPV6 traffic class field dscp	ip_ecn	ECN bits from IP header	ip_ttl	IP TTL or IPv6 hop limit	l4_src_port	Source L4 port	l4_dst_port	Destination L4 port	metadata	Matches value in the metadata field
Key name	Description																																	
in_port	Source port																																	
dl_src	Source MAC address																																	
dl_dst	Destination MAC address																																	
dl_type	Ethernet protocol type																																	
vlan_vid	Virtual LAN tag																																	
vlan_pcp	Priority Code Point																																	
ip_src	Source IPv4 address																																	
ip_dst	Destination IPv4 address																																	
ip_proto	IPV4 - Next protocol, IPV6 - Next header																																	
ip_dscp	IP ToS/DSCP or IPV6 traffic class field dscp																																	
ip_ecn	ECN bits from IP header																																	
ip_ttl	IP TTL or IPv6 hop limit																																	
l4_src_port	Source L4 port																																	
l4_dst_port	Destination L4 port																																	
metadata	Matches value in the metadata field																																	
<b>Related Commands</b>																																		
<b>Note</b>	This command is only supported on Spectrum™ based switch systems																																	

## show openflow table match-keys supported

**show openflow table <table\_id[-table\_id]> match-keys supported**

Displays list of ACL keys which can be configured in OpenFlow table.

<b>Syntax Description</b>	table_id	OpenFlow table ID for adding/removing key values. Can be one ID or range. Valid values: 0-249.																																						
<b>Default</b>	N/A																																							
<b>Configuration Mode</b>	Any Command Mode																																							
<b>History</b>	3.6.3004																																							
<b>Role</b>	admin																																							
<b>Example</b>	<pre>switch (config) # show openflow table 2 match-keys supported</pre> <table> <thead> <tr> <th>Key name</th> <th>Description</th> </tr> </thead> <tbody> <tr><td>-----</td><td>-----</td></tr> <tr><td>in_port</td><td>Source port</td></tr> <tr><td>dl_src</td><td>Source MAC address</td></tr> <tr><td>dl_dst</td><td>Destination MAC address</td></tr> <tr><td>dl_type</td><td>Ethernet protocol type</td></tr> <tr><td>vlan_vid</td><td>Virtual LAN tag</td></tr> <tr><td>vlan_pcp</td><td>Priority Code Point</td></tr> <tr><td>ip_src</td><td>Source IPv4 address</td></tr> <tr><td>ip_dst</td><td>Destination IPv4 address</td></tr> <tr><td>ipv6_dst</td><td>Destination IPv6 address</td></tr> <tr><td>ipv6_src</td><td>Source IPv6 address</td></tr> <tr><td>ip_proto</td><td>IPV4 - Next protocol, IPV6 - Next header</td></tr> <tr><td>ip_dscp</td><td>IP ToS/DSCP or IPv6 traffic class field dscp</td></tr> <tr><td>ip_ecn</td><td>ECN bits from IP header</td></tr> <tr><td>ip_ttl</td><td>IP TTL or IPv6 hop limit</td></tr> <tr><td>l4_src_port</td><td>Source L4 port</td></tr> <tr><td>l4_dst_port</td><td>Destination L4 port</td></tr> <tr><td>metadata</td><td>Matches value in the metadata field</td></tr> </tbody> </table>		Key name	Description	-----	-----	in_port	Source port	dl_src	Source MAC address	dl_dst	Destination MAC address	dl_type	Ethernet protocol type	vlan_vid	Virtual LAN tag	vlan_pcp	Priority Code Point	ip_src	Source IPv4 address	ip_dst	Destination IPv4 address	ipv6_dst	Destination IPv6 address	ipv6_src	Source IPv6 address	ip_proto	IPV4 - Next protocol, IPV6 - Next header	ip_dscp	IP ToS/DSCP or IPv6 traffic class field dscp	ip_ecn	ECN bits from IP header	ip_ttl	IP TTL or IPv6 hop limit	l4_src_port	Source L4 port	l4_dst_port	Destination L4 port	metadata	Matches value in the metadata field
Key name	Description																																							
-----	-----																																							
in_port	Source port																																							
dl_src	Source MAC address																																							
dl_dst	Destination MAC address																																							
dl_type	Ethernet protocol type																																							
vlan_vid	Virtual LAN tag																																							
vlan_pcp	Priority Code Point																																							
ip_src	Source IPv4 address																																							
ip_dst	Destination IPv4 address																																							
ipv6_dst	Destination IPv6 address																																							
ipv6_src	Source IPv6 address																																							
ip_proto	IPV4 - Next protocol, IPV6 - Next header																																							
ip_dscp	IP ToS/DSCP or IPv6 traffic class field dscp																																							
ip_ecn	ECN bits from IP header																																							
ip_ttl	IP TTL or IPv6 hop limit																																							
l4_src_port	Source L4 port																																							
l4_dst_port	Destination L4 port																																							
metadata	Matches value in the metadata field																																							
<b>Related Commands</b>																																								
<b>Note</b>	This command is only supported on Spectrum™ based switch systems																																							

## 5.12 VXLAN

Data centers are being increasingly consolidated and outsourced in an effort to improve the deployment time of applications and reduce operational costs, and applications are constantly raising demand for compute, storage, and network resource. Thus, in order to scale compute, storage, and network resources, physical resources are being abstracted from their logical representation, in what is referred to as server, storage, and network virtualization. Virtualization can be implemented in various layers of computer systems or networks.

Multi-tenant data centers are taking advantage of the benefits of server virtualization to provide a new kind of hosting—a virtual hosted data center. Multi-tenant data centers are ones where individual tenants could belong to a different company or a different department. To a tenant, virtual data centers are similar to their physical counterparts, consisting of end-stations attached to a network, complete with services such as load balancers and firewalls. To tenant systems, a virtual network looks like a normal network, except that the only end-stations connected to the virtual network are those belonging to a tenant's specific virtual network.

How a virtual network is implemented does not generally matter to the tenant; what matters is that the service provided (Layer 2 (L2) or Layer 3 (L3)) has the right semantics, performance, etc. It could be implemented via a pure routed network, a pure bridged network, or a combination of bridged and routed networks.

VXLAN (Virtual eXtensible Local Area Network) addresses the above requirements of the L2 and L3 data center network infrastructure in the presence of virtual networks in a multi-tenant environment. It runs over the existing networking infrastructure and provides a means to “stretch” an L2 network. Each overlay bridge is called a VXLAN segment. Only machines within the same VXLAN segment can communicate with each other. Each VXLAN segment is identified through a 24-bit segment ID called “VXLAN Network Identifier (VNI)”. A network endpoint that performs a conversion from virtual to physical network and back is called VXLAN Tunnel End-Point or VTEP.

In virtual environments, it is typically required to use logical switches to forward traffic between different virtual machines (VMs) on the same physical host, between virtual machines and the physical machines and between networks. Virtual switch environments use an OVSDB management protocol for configuration and state discovery of the virtual networks. OVSDB protocol allows programmable access to the database of virtual switch configuration.

### 5.12.1 Configuring VXLAN

➤ **To enable VXLAN:**

**Step 1.** Configure jumbo frames for NVE ports:

```
switch (config)# interface ethernet 1/1-1/4 mtu 9216 force
```

**Step 2.** Configure jumbo frames for underlay-facing ports:

```
switch (config)# interface ethernet 1/17 mtu 9216 force
```

**Step 3.** Create VLAN for all VXLAN traffic:

```
switch (config)# vlan 3
```

**Step 4.** Configure Overlay interfaces with VXLAN VLAN:

```
switch (config)# interface ethernet 1/17 switchport access vlan 3
```

**Step 5.** Enable IP routing:

```
switch (config)# ip routing vrf default
```

**Step 6.** Configure interface on the VXLAN VLAN and configure an IP address for it:

```
switch (config)# interface vlan 3
switch (config interface vlan 3)# ip address 33.33.33.254 255.255.255.0
switch (config interface vlan 3)# interface vlan 3 mtu 9216
```

**Step 7.** Enable NVE protocol:

```
switch (config)# protocol nve
```

**Step 8.** Configure interface NVE:

```
switch (config)# interface nve 1
```

**Step 9.** Create loopback interface to terminate the VXLAN tunnel. The IP address of the interface will be a VTEP endpoint address, and needs to be reachable in the underlay network:

```
switch (config)# interface loopback 1
switch (config interface loopback 1)# ip address 1.2.3.4 255.255.255.255
switch (config)# interface nve 1 vxlan source interface loopback 1
```

**Step 10.** Configure routing to other VTEP devices:

```
switch (config)# ip route vrf default 1.2.3.5 /32 33.33.33.253
switch (config)# ip route vrf default 1.2.3.6 /32 33.33.33.252
```

**Step 11.** Configure overlay-facing ports for NVE mode:

```
switch (config)# interface ethernet 1/1 nve mode only force
switch (config)# interface ethernet 1/2 nve mode only force
switch (config)# interface ethernet 1/3 nve mode only force
switch (config)# interface ethernet 1/4 nve mode only force
```

➤ *For deployments with a controller, set up OVSDB:*

**Step 12.** Start OVSDB server:

```
switch (config)# ovs ovsdb server
```

**Step 13.** Configure the OVSDB manager to an IP address of a controller:

```
switch (config)# ovs ovsdb manager remote ssl ip address 10.130.250.5
```

➤ *For controller-less deployments, configure the bridging from the CLI directly:*

**Step 14.** Create bridges:

```
switch (config)# interface nve 1 nve bridge 7777
switch (config)# interface ethernet 1/1 nve vlan 10 bridge 7777
```

**Step 15.** Configure source-node replication:

```
switch (config)# no interface nve 1 nve fdb flood load-balance
```

**Step 16.** Configure flood addresses for BUM traffic:

```
switch (config)# interface nve 1 nve fdb flood bridge 7777 address 1.2.3.5
switch (config)# interface nve 1 nve fdb flood bridge 7777 address 1.2.3.6
```

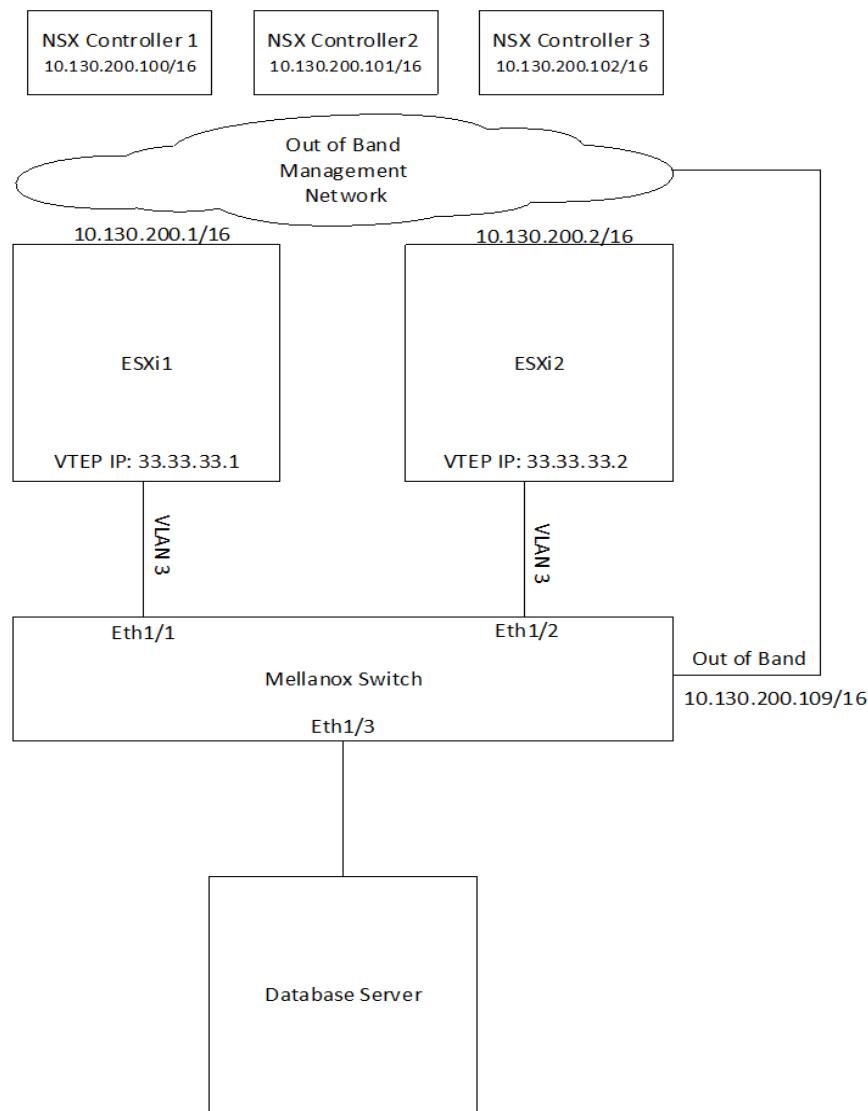
**Step 17.** Configure FDB remote learning:

```
switch (config)# interface nve 1 nve fdb learning remote
```

## 5.12.2 VMware Network Virtualization and Security Platform (NSX) Configuration

### 5.12.2.1 Hardware Topology

- 2 ESXi servers pre-configured with VXLAN networking using VMware NSX
- 3 NSX Controllers available for VXLAN unicast type logical switches
- 1 Mellanox switch connected to the ESXi servers and to a physical database server
- Out-of-band network for management and a VLAN network to carry VXLAN traffic



### 5.12.2.2 Switch Configuration

- Step 1.** Configure jumbo frames on ESXi and Database server facing interfaces:

```
switch (config)# interface ethernet 1/1-1/3 mtu 9216 force
```

- Step 2.** Create VLAN 3 to carry VXLAN traffic (if it does not exist yet):

```
switch (config)# vlan 3
```

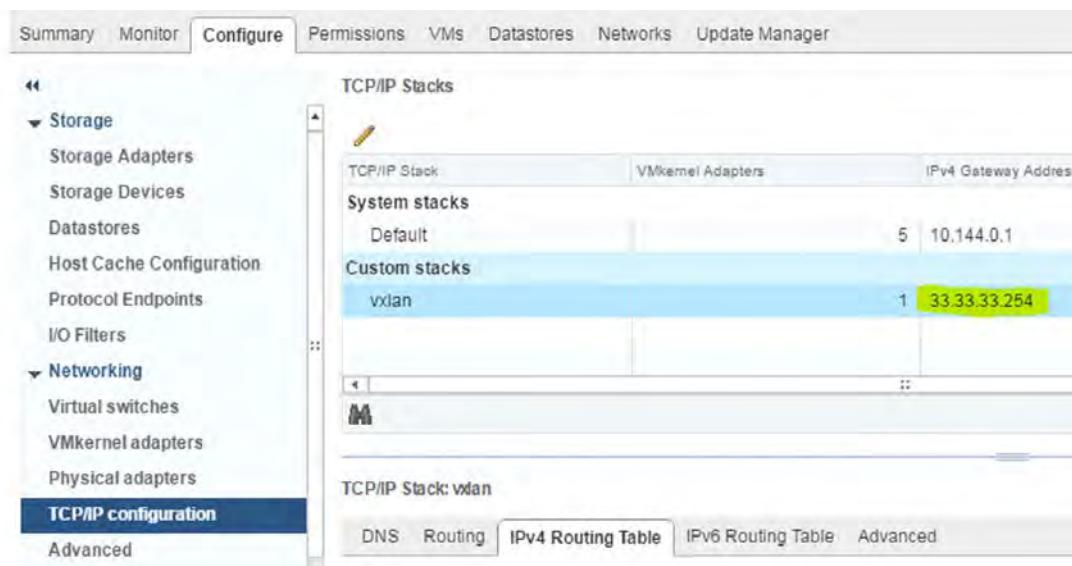
- Step 3.** Enable IP routing:

```
switch (config)# ip routing vrf default
```

- Step 4.** Create an interface on VLAN 3 and assign an IP address to it.

The IP address must be the default gateway of the VXLAN netstack created by NSX after enabling VXLAN traffic on the hosts.

To check the default gateway in vSphere web client select an ESXi host and go to:  
Configure -> TCP/IP configuration .



```
switch (config)# interface vlan 3
switch (config interface vlan 3)# ip address 33.33.33.254 255.255.255.0
switch (config interface vlan 3)# interface vlan 3 mtu 9216
```

- Step 5.** Create a loopback interface to communicate with VTEPs on the ESXi servers by routing through “interface vlan 3”. This interface will be the VTEP IP assigned to the switch

```
switch (config)# interface loopback 1
switch (config interface loopback 1)# ip address 1.2.3.4 255.255.255.255
```

- Step 6.** Enable NVE protocol:

```
switch (config)# protocol nve
```

- Step 7.** Configure interface NVE:

```
switch (config)# interface nve 1
```

**Step 8.** Configure the source of the NVE interface to be the loopback created above:

```
switch (config)# interface nve 1 vxlan source interface loopback 1
```

**Step 9.** Start the OVSDB server and connect it to the NSX Controllers

```
switch (config)# ovs ovsdb server
switch (config)# ovs ovsdb manager remote ssl ip address 10.130.200.100
switch (config)# ovs ovsdb manager remote ssl ip address 10.144.200.101
switch (config)# ovs ovsdb manager remote ssl ip address 10.144.200.102
```

**Step 10.** Configure the port facing the Database server as an NVE port

```
switch (config)# interface ethernet 1/3 nve mode only force
```

**Step 11.** Get the switch certificate for later configuration in the NSX Manager.

```
switch (config)# show crypto certificate name system-self-signed public-pem
```

Copy the certificate starting with the line:

```
-----BEGIN CERTIFICATE-----
```

until the line:

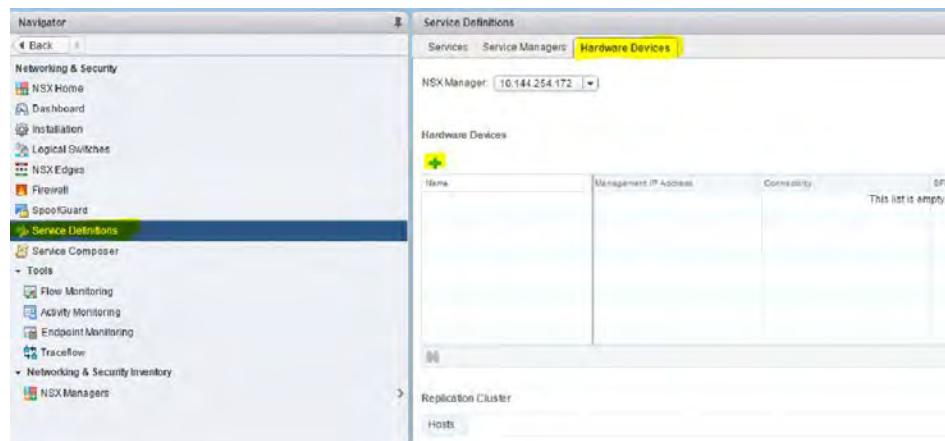
```
-----END CERTIFICATE-----
```

Make sure to include both of those lines.

**Warning!** NSX Manager Configuration

**Warning!** Adding Hosts to Replication Cluster

**Warning!** In NSX Manager, go to “Service Definitions” “Hardware Devices”.



**Step 12.** Under “Replication Cluster” click Edit.

**Step 13.** Add both of the ESXi servers to the replication cluster.

All hosts added to the replication cluster can replicate BUM (Broadcast, Unknown unicast and Multicast) traffic to other ESXi servers.

When the switch needs to send BUM traffic to a virtual machine, it will select one of the hosts in the replication cluster and send the traffic to it, the host will then replicate it to all other ESXi hosts.

It is recommended to add at least 2 ESXi servers to the replication cluster for redundancy.

### 5.12.2.3 Adding the Mellanox Switch to NSX

- Step 1.** Under Hardware Devices click the + sign to add a new hardware device.
- Step 2.** Fill in a name for the new hardware device.
- Step 3.** Fill in the switch certificate we got earlier.
- Step 4.** Click OK.



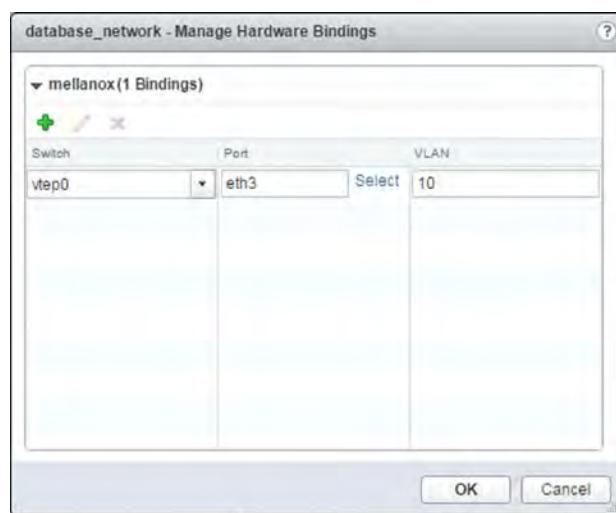
- Step 5.** Wait until the new switch is showing as “UP” under the connectivity column, you may need to refresh vSphere client a few times.

Name	Management IP Address	Connectivity	BFD Enabled	Logical Switches
mellanox	10.130.200.109	Up	✓	0

### 5.12.3 Mapping a Logical Switch to a Physical Switch Port

- Step 1.** In NSX Manager go to “Logical Switches”
- Step 2.** Right click the logical switch you wish to map to the physical switch port and select “Manage Hardware Bindings”

- Step 3.** Click the “+” sign to add a new mapping instance
- Step 4.** Click Select under the port column and select port “eth3”, this corresponds to “interface ethernet 1/3” we configured earlier as an NVE port in the switch.
- Step 5.** Under the VLAN column, set the VLAN that will map this logical switch to this specific switch port, you can have multiple logical switches mapped to the same port on a different VLAN (for example to connect a firewall appliance to logical switches). For "access" configuration (no VLAN is required on the host connected to the physical switch port) use VLAN 1.
- Step 6.** Click OK



## 5.12.4 Commands

### protocol nve

**protocol nve**  
**no protocol nve**

Enables NVE functionality and displays NVE commands.  
The no form of the command hides the NVE commands and deletes its database.

<b>Syntax Description</b>	N/A
<b>Default</b>	N/A
<b>Configuration Mode</b>	Config
<b>History</b>	3.6.3004
<b>Role</b>	admin
<b>Example</b>	switch (config) # protocol nve
<b>Related Commands</b>	
<b>Note</b>	This command is only supported on Spectrum™ based switch systems

## interface nve

```
interface nve <nve-id>
no interface nve <nve-id>
```

Creates VXLAN tunnel.

The no form of the command destroys VXLAN tunnel.

<b>Syntax Description</b>	nve-id	NVE ID range: 1-64
<b>Default</b>	N/A	
<b>Configuration Mode</b>	Config	
<b>History</b>	3.6.3004	
<b>Role</b>	admin	
<b>Example</b>	<pre>switch (config) # interface nve 1 switch (config interface nve 1) #</pre>	
<b>Related Commands</b>	protocol nve	
<b>Note</b>	This command is only supported on Spectrum™ based switch systems	

## nve bridge

```
nve bridge <vni-id> [name <bridge-name>]  
no nve bridge <vni-id>
```

creates an NVE bridge with a given VNI.  
The no form of the command removes NVE bridge.

<b>Syntax Description</b>	vni-id	VXLAN network identifier range: 0-16777216
<b>Default</b>	bridge-name	“bridge-<vni-id>”
<b>Configuration Mode</b>	Config Interface NVE	
<b>History</b>	3.6.3550 3.6.3212	
<b>Role</b>	admin	
<b>Example</b>	switch (config interface nve 1) # nve bridge 25	
<b>Related Commands</b>		
<b>Note</b>	Number of bridges limited to 500	

## nve fdb flood bridge address

```
nve fdb flood bridge <vni-id> address <ip-address>
no nve fdb flood bridge <vni-id> address [ip-address]
```

Adds an IP address of a remote VTEP to be used for BUM traffic.

The no form of the command has two input options:

- Entering an IP address removes a specific remote address
- No IP address removes all addresses

<b>Syntax Description</b>	vni-id	VXLAN network identifier range: 0-16777216
<b>Default</b>	N/A	
<b>Configuration Mode</b>	Config Interface NVE	
<b>History</b>	3.6.3550 3.6.3212	
<b>Role</b>	admin	
<b>Example</b>		<pre>switch (config)interface ethernet 1/1 switch (config interface ethernet 1/1) # nve mode only force switch (config interface ethernet 1/1) # nve vlan 2 bridge 25</pre>
<b>Related Commands</b>		
<b>Note</b>	Number of IP addesses limited to 750	

## shutdown

**shutdown**  
**no shutdown**

Disables VXLAN tunnel.

The no form of the command enables VXLAN tunnel.

<b>Syntax Description</b>	N/A
<b>Default</b>	Enabled
<b>Configuration Mode</b>	Config Interface NVE
<b>History</b>	3.6.3004
<b>Role</b>	admin
<b>Example</b>	<pre>switch (config interface nve 1) # shutdown</pre>
<b>Related Commands</b>	<pre>interface nve protocol nve</pre>
<b>Note</b>	

## vxlan source interface loopback

```
vxlan source interface loopback <loopback-id>
no vxlan source interface loopback <loopback-id>
```

Binds VXLAN tunnel to a loopback interface.

The no form of the command unbinds VXLAN tunnel from the loopback interface.

<b>Syntax Description</b>	loopback-id	Loopback interface ID Valid range: 0-31
<b>Default</b>	N/A	
<b>Configuration Mode</b>	Config Interface NVE	
<b>History</b>	3.6.3004	
<b>Role</b>	admin	
<b>Example</b>	switch (config interface nve 1) # vxlan source interface loopback 14	
<b>Related Commands</b>	interface nve protocol nve	
<b>Note</b>	The configured loopback interface becomes the VXLAN tunnel endpoint (VTEP) This command is only supported on Spectrum™ based switch systems	

## nve mode only

**nve mode only [force]**  
**no nve mode only [force]**

Sets physical interface to NVE mode.

The no form of the command removes physical interface from NVE mode.

<b>Syntax Description</b>	force	Forces configuration while interface is admin up
<b>Default</b>	Not in NVE mode	
<b>Configuration Mode</b>	Config Interface Ethernet	
<b>History</b>	3.6.3004	
<b>Role</b>	admin	
<b>Example</b>	switch (config interface ethernet 1/1) # nve mode only	
<b>Related Commands</b>	interface ethernet	
<b>Note</b>	This command is only supported on Spectrum™ based switch systems	

## clear nve counters

### clear nve counters

Clears NVE counters.

<b>Syntax Description</b>	N/A
<b>Default</b>	N/A
<b>Configuration Mode</b>	Config Interface NVE
<b>History</b>	3.6.3004
<b>Role</b>	admin
<b>Example</b>	<pre>switch (config interface nve 1) # clear nve counters</pre>
<b>Related Commands</b>	interface nve protocol nve
<b>Note</b>	This command is only supported on Spectrum™ based switch systems

## show interfaces nve

**show interfaces nve [<nve-id>]**

Displays information about NVE interfaces.

<b>Syntax Description</b>	nve-id	NVE ID range: 1-64
<b>Default</b>	N/A	
<b>Configuration Mode</b>	Any Command Mode	
<b>History</b>	3.6.3004	
<b>Role</b>	admin	

**Example**

```
switch (config) # show interface nve

      Remote Manager IP Address          Port      Connection Type
-----  -----
      2.2.2.2                           200       tcp

      NVE member interfaces: Eth1/2, Eth1/7

      Interface NVE 1 status:
      Admin state: up
      Source interface: loopback 1

      17971      encapsulated (Tx) NVE packets
      0          decapsulated (Rx) NVE packets
      0          dropped NVE-encapsulated packets
      0          NVE-encapsulated packets with errors
```

---

### Related Commands

**Note** This command is only supported on Spectrum™ based switch systems

---

## show interfaces nve counters

**show interfaces nve <nve-id> counters**

Displays NVE counters.

<b>Syntax Description</b>	nve-id	NVE ID range: 1-64
<b>Default</b>	N/A	
<b>Configuration Mode</b>	Any Command Mode	
<b>History</b>	3.6.3004	
<b>Role</b>	admin	
<b>Example</b>	<pre>switch (config) # show interface nve 1 counters 18330          encapsulated (Tx) NVE packets 0              decapsulated (Rx) NVE packets 0              dropped NVE-encapsulated packets 0              NVE-encapsulated packets with errors</pre>	
<b>Related Commands</b>		
<b>Note</b>	This command is only supported on Spectrum™ based switch systems	

## show interfaces nve flood

**show interfaces nve <nve-id> flood [vni <vnid>]**

Displays remote VTEP endpoints configured for BUM (broadcast, unknown unicast, multicast) flooding.

<b>Syntax Description</b>	nve-id vni	NVE ID range: 1-64 Displays NVE flooding on specific VNI								
<b>Default</b>	N/A									
<b>Configuration Mode</b>	Any Command Mode									
<b>History</b>	3.6.3004									
<b>Role</b>	admin									
<b>Example</b>	<pre>switch (config) # show interface nve 1 flood</pre> <table> <thead> <tr> <th>NVE Interface</th> <th>Logical Switch</th> <th>VNI ID</th> <th>Flood IP Address</th> </tr> </thead> <tbody> <tr> <td>1</td> <td>ls7777</td> <td>7777</td> <td>1.2.3.5</td> </tr> </tbody> </table>		NVE Interface	Logical Switch	VNI ID	Flood IP Address	1	ls7777	7777	1.2.3.5
NVE Interface	Logical Switch	VNI ID	Flood IP Address							
1	ls7777	7777	1.2.3.5							
<b>Related Commands</b>										
<b>Note</b>	This command is only supported on Spectrum™ based switch systems									

## show interfaces nve mac-address-table

**show interfaces nve <nve-id> mac-address-table [vni <vni-id>]**

Displays MAC address table of NVE interface.

<b>Syntax Description</b>	nve-id vni	NVE ID range: 1-64 Displays MAC address table of NVE interface with specified VNI																		
<b>Default</b>	N/A																			
<b>Configuration Mode</b>	Any Command Mode																			
<b>History</b>	3.6.3004																			
<b>Role</b>	admin																			
<b>Example</b>	<pre>switch (config) # show interface nve 1 mac-address-table</pre> <table border="1"> <thead> <tr> <th>NVE Interface</th> <th>Logical Switch</th> <th>VNI ID</th> <th>Mac Address</th> <th>Address Type</th> <th>Remote Endpoint IP Address</th> </tr> </thead> <tbody> <tr> <td>1</td> <td>ls7777</td> <td>7777</td> <td>e4:1d:2d:a5:f2:0a</td> <td>local learned</td> <td>N/A</td> </tr> <tr> <td>1</td> <td>ls7777</td> <td>7777</td> <td>00:11:22:33:44:55</td> <td>remote configured</td> <td>1.2.3.5</td> </tr> </tbody> </table>		NVE Interface	Logical Switch	VNI ID	Mac Address	Address Type	Remote Endpoint IP Address	1	ls7777	7777	e4:1d:2d:a5:f2:0a	local learned	N/A	1	ls7777	7777	00:11:22:33:44:55	remote configured	1.2.3.5
NVE Interface	Logical Switch	VNI ID	Mac Address	Address Type	Remote Endpoint IP Address															
1	ls7777	7777	e4:1d:2d:a5:f2:0a	local learned	N/A															
1	ls7777	7777	00:11:22:33:44:55	remote configured	1.2.3.5															
<b>Related Commands</b>																				
<b>Note</b>	This command is only supported on Spectrum™ based switch systems																			

## show interfaces nve mac-address-table local learned unicast

**show interfaces nve <nve-id> mac-address-table local learned unicast [vni <vnid>]**

Displays only the locally-learned unicast MAC addresses.

<b>Syntax Description</b>	nve-id vni	NVE ID range: 1-64 Displays MAC addresses on the bridge with the given VNI												
<b>Default</b>	N/A													
<b>Configuration Mode</b>	Any Command Mode													
<b>History</b>	3.6.3004													
<b>Role</b>	admin													
<b>Example</b>	<pre>switch (config) # show interface nve 1 mac-address-table local learned unicast</pre> <table><thead><tr><th>NVE Interface</th><th>Logical Switch</th><th>VNI ID</th><th>Mac Address</th><th>Address Type</th><th>Remote Endpoint IP Address</th></tr></thead><tbody><tr><td>1</td><td>ls7777</td><td>7777</td><td>e7:3a:7e:a5:f2:1a</td><td>local learned</td><td>N/A</td></tr></tbody></table>		NVE Interface	Logical Switch	VNI ID	Mac Address	Address Type	Remote Endpoint IP Address	1	ls7777	7777	e7:3a:7e:a5:f2:1a	local learned	N/A
NVE Interface	Logical Switch	VNI ID	Mac Address	Address Type	Remote Endpoint IP Address									
1	ls7777	7777	e7:3a:7e:a5:f2:1a	local learned	N/A									
<b>Related Commands</b>														
<b>Note</b>	This command is only supported on Spectrum™ based switch systems													

## show interfaces nve mac-address-table remote configured multicast

**show interfaces nve <nve-id> mac-address-table remote configured multicast  
[vni <vni-id>]**

Displays only remotely-configured BUM addresses.

<b>Syntax Description</b>	nve-id vni	NVE ID range: 1-64 Displays only MAC addresses on the bridge with the given VNI												
<b>Default</b>	N/A													
<b>Configuration Mode</b>	Any Command Mode													
<b>History</b>	3.6.3004													
<b>Role</b>	admin													
<b>Example</b>	<pre>switch (config) # show interface nve 1 mac-address-table remote configured multicast</pre> <table> <thead> <tr> <th>NVE Interface</th> <th>Logical Switch</th> <th>VNI ID</th> <th>Mac Address</th> <th>Address Type</th> <th>Remote Endpoint IP Address</th> </tr> </thead> <tbody> <tr> <td>1</td> <td>ls7777</td> <td>7777</td> <td>00:11:22:33:44:55</td> <td>remote configured</td> <td>1.2.3.5</td> </tr> </tbody> </table>		NVE Interface	Logical Switch	VNI ID	Mac Address	Address Type	Remote Endpoint IP Address	1	ls7777	7777	00:11:22:33:44:55	remote configured	1.2.3.5
NVE Interface	Logical Switch	VNI ID	Mac Address	Address Type	Remote Endpoint IP Address									
1	ls7777	7777	00:11:22:33:44:55	remote configured	1.2.3.5									
<b>Related Commands</b>														
<b>Note</b>	This command is only supported on Spectrum™ based switch systems													

## show interfaces nve mac-address-table remote configured unicast

**show interfaces nve <nve-id> mac-address-table remote configured unicast [vni <vni-id>]**

Displays only remotely-configured unicast addresses.

<b>Syntax Description</b>	nve-id vni	NVE ID range: 1-64 Displays only MAC addresses on the bridge with the given VNI												
<b>Default</b>	N/A													
<b>Configuration Mode</b>	Any Command Mode													
<b>History</b>	3.6.3004													
<b>Role</b>	admin													
<b>Example</b>	<pre>switch (config) # show interface nve 1 mac-address-table remote configured unicast</pre> <table border="1"> <thead> <tr> <th>NVE Interface</th> <th>Logical Switch</th> <th>VNI ID</th> <th>Mac Address</th> <th>Address Type</th> <th>Remote Endpoint IP Address</th> </tr> </thead> <tbody> <tr> <td>1</td> <td>ls7777</td> <td>7777</td> <td>00:11:22:33:44:55</td> <td>remote configured</td> <td>1.2.3.5</td> </tr> </tbody> </table>		NVE Interface	Logical Switch	VNI ID	Mac Address	Address Type	Remote Endpoint IP Address	1	ls7777	7777	00:11:22:33:44:55	remote configured	1.2.3.5
NVE Interface	Logical Switch	VNI ID	Mac Address	Address Type	Remote Endpoint IP Address									
1	ls7777	7777	00:11:22:33:44:55	remote configured	1.2.3.5									
<b>Related Commands</b>														
<b>Note</b>	This command is only supported on Spectrum™ based switch systems													

## show interfaces nve peers

**show interfaces nve <nve-id> peers [vni <vni-id>]**

Displays all remote VTEPs.

<b>Syntax Description</b>	nve-id vni	NVE ID range: 1-64 Displays NVE peers on specific VNI								
<b>Default</b>	N/A									
<b>Configuration Mode</b>	Any Command Mode									
<b>History</b>	3.6.3004									
<b>Role</b>	admin									
<b>Example</b>	<pre>switch (config) # show interface nve 1 peers</pre> <table><thead><tr><th>NVE Interface</th><th>Logical Switch</th><th>VNI ID</th><th>Peer IP Address</th></tr></thead><tbody><tr><td>1</td><td>ls7777</td><td>7777</td><td>1.2.3.5</td></tr></tbody></table>		NVE Interface	Logical Switch	VNI ID	Peer IP Address	1	ls7777	7777	1.2.3.5
NVE Interface	Logical Switch	VNI ID	Peer IP Address							
1	ls7777	7777	1.2.3.5							
<b>Related Commands</b>										
<b>Note</b>	This command is only supported on Spectrum™ based switch systems									

## ovs ovsdb server

**ovs ovsdb server**  
**no ovs ovsdb server**

Runs OVSDB-server process and unhides OVS commands.  
The no form of the command deactivates OVSDB-server process and hides OVS commands.

<b>Syntax Description</b>	N/A
<b>Default</b>	N/A
<b>Configuration Mode</b>	Config
<b>History</b>	3.6.3004
<b>Role</b>	admin
<b>Example</b>	switch (config) # ovs ovsdb server
<b>Related Commands</b>	
<b>Note</b>	OVSDB server runs when "protocol openflow" or "protocol nve" are enabled, even when not enabled using this command

## ovs ovsdb manager remote

```
ovs ovsdb manager remote {tcp | ssl} ip-address <ip-address> port <tcp-port>
no ovs ovsdb manager remote {tcp | ssl} ip-address <ip-address> port <tcp-port>
```

Configures OVSDB to actively connect to a remote manager at a given IP address and TCP port, using either TCP or SSL.

The no form of the command disconnects OVSDB from a remote manager.

<b>Syntax Description</b>	SSL TCP	Connect with TCP protocol Connect with SSL protocol
	ip-address	IP address of remote manager
<b>Default</b>	N/A	
<b>Configuration Mode</b>	Config	
<b>History</b>	3.6.3004	
<b>Role</b>	admin	
<b>Example</b>	switch (config) # ovs ovsdb manager remote tcp ip-address 10.10.10.10 port 20	
<b>Related Commands</b>	ovs ovsdb server	
<b>Note</b>	This command is only supported on Spectrum™ based switch systems	

## ovs ovsdb server listen

```
ovs ovsdb server listen {tcp | ssl} port <tcp-port> local ip-address <ip-address>
no ovs ovsdb server listen {tcp | ssl} port <tcp-port> local ip-address <ip-
address>
```

Configures OVSDB to listen at a given port of an interface with a given (local) IP address.

The no form of the command disconnects OVSDB from a remote manager.

<b>Syntax Description</b>	SSL	Connect with TCP protocol
	TCP	Connect with SSL protocol
	ip-address	IP address of a given port
<b>Default</b>	N/A	
<b>Configuration Mode</b>	Config	
<b>History</b>	3.6.3004	
<b>Role</b>	admin	
<b>Example</b>	switch (config) # ovs ovsdb server listen tcp port 20 local ip-address 20.20.20.20	
<b>Related Commands</b>	ovs ovsdb server	
<b>Note</b>	This command is only supported on Spectrum™ based switch systems	

## 5.13 IGMP Snooping



While IGMPv3 is supported on SwitchX®, the source is not considered. So a “join” to a group from a specific source (S,G) is treated as a join to the group from all sources (\*,G).

The Internet Group Multicast Protocol (IGMP) is a communications protocol used by hosts and adjacent routers on IP networks to establish multicast group memberships. The host joins a multicast-group by sending a join request message towards the network router, and responds to queries sent from the network router by dispatching a join report.

A given port can be either manually configured to be a MRouter port or it can be dynamically manifested when having received a query, hence, the network router is connected to this port. All IGMP Snooping control packets received from hosts (joins/leaves) are forwarded to the MRouter port, and the MRouter port updates its multicast-group data-base accordingly. Each dynamically learned multicast group will be added to all of the MRouter ports on the switch.

As many as 5K multicast groups can be created on the switch.

### 5.13.1 Configuring IGMP Snooping

You can configure IGMP snooping to establish multicast group memberships.

➤ **To configure IGMP snooping:**

**Step 1.** Log in as admin.

**Step 2.** Enter config mode. Run:

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

**Step 3.** Enable IGMP snooping globally. Run:

```
switch (config) # ip igmp snooping  
switch (config) #
```

**Step 4.** Enable IGMP snooping on a VLAN. Run:

```
switch (config) # vlan 2  
switch (config vlan 2) # ip igmp snooping
```

### 5.13.2 Defining a Multicast Router Port on a VLAN

You can define a Multicast Router (MRouter) port on a VLAN in one of the following methods:

➤ **To change the interface switchport to trunk:**

**Step 1.** Log in as admin.

**Step 2.** Enter config mode. Run:

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

**Step 3.** Enable IGMP snooping globally. Run:

```
switch (config) # ip igmp snooping  
switch (config) #
```

**Step 4.** Change the interface switchport mode of the port (the interface is member of VLAN 1 by default). Run:

```
switch (config) # interface ethernet 1/1  
switch (config interface ethernet 1/1) # switchport mode trunk
```

**Step 5.** Change back to config mode. Run:

```
switch (config interface ethernet 1/1) # exit  
switch (config) #
```

**Step 6.** Define the MRouter port on the VLAN. Run:

```
switch (config) # vlan 2  
switch (config vlan 2) # ip igmp snooping mrouter interface ethernet 1/1  
switch (config vlan 2) #
```

➤ **To change the interface switchport to hybrid:**

**Step 1.** Log in as admin.

**Step 2.** Enter config mode. Run:

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

**Step 3.** Enable IGMP snooping globally. Run:

```
switch (config) # ip igmp snooping  
switch (config) #
```

**Step 4.** Create a VLAN. Run:

```
switch (config) # vlan 200  
switch (config vlan 200) #
```

**Step 5.** Change back to config mode. Run:

```
switch (config vlan 200) # exit  
switch (config) #
```

**Step 6.** Change the interface switchport mode of the port (the interface is member of VLAN 1 by default). Run:

```
switch (config) # interface ethernet 1/22  
switch (config interface ethernet 1/22) # switchport mode hybrid
```

**Step 7.** Attach the VLAN to the port's interface. Run:

```
switch (config interface ethernet 1/22) # switchport mode hybrid allowed-vlan 200  
switch (config interface ethernet 1/22) #
```

**Step 8.** Change to config mode again. Run:

```
switch (config interface ethernet 1/22) # exit  
switch (config) #
```

**Step 9.** Define the MRouter port on the VLAN. Run:

```
switch (config) # vlan 200
switch (config vlan 200) # ip igmp mrouter interface ethernet 1/22
switch (config vlan 200) #
```

### 5.13.3 IGMP Snooping Querier

IGMP Snooping Querier complements the IGMP snooping functionality. IGMP Snooping Querier is used to support IGMP snooping in a VLAN where PIM and IGMP are not configured because the multicast traffic does not need to be routed. When IGMP Snooping Querier is enabled, IGMP queries are sent out periodically by the switch through all ports in the VLAN and to which hosts wishing to receive IP multicast traffic respond with IGMP report messages. IGMP Snooping Querier must be used in conjunction with IGMP snooping as IGMP snooping listens to these IGMP reports to establish appropriate forwarding.

➤ **To configure IGMP Snooping Querier:**

**Step 1.** Enable the IGMP snooping on the switch. Run:

```
switch (config) # ip igmp snooping
```

**Step 2.** Enable the IGMP snooping querier on a specific VLAN. Run:

```
switch (config) # vlan 10
switch (config vlan 10)# ip igmp snooping querier
```

**Step 3.** Set the query interval time. Run:

```
switch (config vlan 10)# ip igmp snooping querier query-interval 25
```

**Step 4.** (Optional) Verify the IGMP snooping querier configuration. Run:

```
switch (config vlan 10)# show ip igmp snooping querier
Snooping querier information for VLAN 10
```

```
IGMP Querier Present
Querier IP address: 1.1.1.2
Query interval: 125
Response interval: 100
Group membership interval: 1
Robustness: 2
Version: 2
```

```
switch (config vlan 10)#

```

## 5.13.4 Commands

### ip igmp snooping (admin)

```
ip igmp snooping
no ip igmp snooping
```

Enables IGMP snooping globally or per VLAN.

The no form of the command disables IGMP snooping globally or per VLAN.

<b>Syntax Description</b>	N/A
<b>Default</b>	IGMP snooping is disabled, globally and per VLAN.
<b>Configuration Mode</b>	Config Config VLAN
<b>History</b>	3.1.1400
<b>Role</b>	admin
<b>Example</b>	<pre>switch (config) # ip igmp snooping switch (config) # vlan 10 switch (config vlan 10) # ip igmp snooping</pre>
<b>Related Commands</b>	show ip igmp snooping
<b>Note</b>	IGMP snooping has global admin state, and per VLAN admin state. Both states need to be enabled in order to enable the IGMP snooping on a specific VLAN.

## ip igmp snooping (config)

```
ip igmp snooping {last-member-query-interval <1-25> | proxy reporting mrouter-timeout <60-600> | port-purge-timeout <130-1225> | report-suppression-interval <1-25>}
```

```
no ip igmp snooping {last-member-query-interval | proxy reporting | mrouter-timeout | report-suppression-interval}
```

Configures IGMP global parameters.

The no form of the command resets the IGMP global parameters to default.

<b>Syntax Description</b>	last-member-query-interval <1-25>	Sets the time period (in seconds) with which the general queries are sent by the IGMP querier. After timeout expiration the port will be removed from the multicast group.
	proxy reporting	Enables proxy reporting
	mrouter-timeout <60-600>	Sets the IGMP snooping MRouter port purge time-out after which the port gets deleted if no IGMP router control packets are received. The default value is 125 seconds.
	port-purge-timeout <130-1225>	Sets the IGMP snooping port purge time interval after which the port gets deleted if no IGMP reports are received.
	report-suppression-interval <1-25>	Sets the IGMP snooping report-suppression time interval for which the IGMPv2 report messages for the same group will not get forwarded onto the MRouter ports. The default value is 5 seconds.
<b>Default</b>	last-member-query-interval – 1 second proxy reporting is disabled mrouter-timout – 125 port-purge-timeout – 260 seconds report-suppression-interval – 5 seconds	
<b>Configuration Mode</b>	Config	
<b>History</b>	3.1.1400	
<b>Role</b>	admin	
<b>Example</b>	switch (config) # ip igmp snooping report-suppression-interval 3	
<b>Related Commands</b>	ip igmp snooping (admin) show ip igmp snooping	
<b>Note</b>		

## ip igmp snooping clear counters

**ip igmp snooping clear counters [vlan <vlan-id>]**

Clears IGMP snooping counters.

<b>Syntax Description</b>	vlan	Clears IGMP snooping counters per VLAN
<b>Default</b>	N/A	
<b>Configuration Mode</b>	Config	
<b>History</b>	3.6.1002	
<b>Role</b>	admin	
<b>Example</b>	switch (config) # ip igmp snooping clear counters vlan 2	
<b>Related Commands</b>		
<b>Note</b>		

## **ip igmp snooping fast-leave**

```
ip igmp snooping fast-leave  
no ip igmp snooping fast-leave
```

Enables fast leave processing on a specific interface

The `no` form of the command disables fast leave processing on a specific interface.

## ip igmp snooping mrouter

```
ip igmp snooping mrouter interface <type> <number>
no ip igmp snooping mrouter interface <type> <number>
```

Creates a static multicast router port on a specific VLAN, on a specific interface.  
The no form of the command removes the static multicast router port from a specific VLAN.

<b>Syntax Description</b>	interface <type> <number>	Attaches the group to a specific interface. type - ethernet or port-channel.
<b>Default</b>	No static mrouters are configured.	
<b>Configuration Mode</b>	Config VLAN	
<b>History</b>	3.1.1400	
<b>Role</b>	admin	
<b>Example</b>	<pre>switch (config)# vlan 1 switch (config vlan 1) # ip igmp snooping mrouter interface ethernet 1/1</pre>	
<b>Related Commands</b>	show ip igmp snooping mrouter	
<b>Note</b>	The multicast router port can be created only if IGMP snooping is enabled both globally and on the VLAN.	

## ip igmp snooping static-group

**ip igmp snooping static-group <IP address> interface <type> <number> [source <source-IP>]**

**no ip igmp snooping static-group <IP address> interface <type> <number> [source <source-IP>]**

Creates a specified static multicast group for specified ports and from a specified source IP address.

The no form of the command deletes the interface from the multicast group.

<b>Syntax Description</b>	IP address	Multicast IP address <224.x.x.x - 239.255.255.255>
	interface	Attach the group to a specific interface
	type	Ethernet or port-channel
	source	Source IP address If omitted, a multicast group is created for all sources
<b>Default</b>	No static groups are configured.	
<b>Configuration Mode</b>	Config VLAN	
<b>History</b>	3.1.1400	
	3.6.2100	Added “source” parameter
<b>Role</b>	admin	
<b>Example</b>	switch (config vlan 1) # ip igmp snooping static-group 230.0.0.1 interface ethernet 1/1	
<b>Related Commands</b>	show ip igmp snooping groups	
<b>Note</b>	If the deleted interface is the last port, it deletes the entire multicast group.	

## ip igmp snooping unregistered multicast

```
ip igmp snooping unregistered multicast <options>
no ip igmp snooping unregistered multicast
```

Sets the behavior of the snooping switch for unregistered multicast traffic.  
The no form of the command sets it default.

<b>Syntax Description</b>	options	<ul style="list-style-type: none"><li>• flood</li><li>• forward-to-mrouter-ports</li></ul>
<b>Default</b>	flood	
<b>Configuration Mode</b>	Config	
<b>History</b>	3.2.0500	
<b>Role</b>	admin	
<b>Example</b>	switch (config) # ip igmp snooping unregistered multicast flood	
<b>Related Commands</b>	show ip igmp snooping	
<b>Note</b>		

## ip igmp snooping version

**ip igmp snooping version {2 | 3}**

Configures the default operating version to be used for newly created IGMP snooping instances.

<b>Syntax Description</b>	2	Enables IGMPv2
	3	Enables IGMPv3
<b>Default</b>	3	
<b>Configuration Mode</b>	Config Config VLAN	
<b>History</b>	3.6.1002	
	3.6.2100	Updated default
<b>Role</b>	admin	
<b>Example</b>	switch (config vlan 2)# ip igmp snooping version 3	
<b>Related Commands</b>		
<b>Note</b>		

## ip igmp snooping querier

```
ip igmp snooping querier
no ip igmp snooping querier
```

Enables the IGMP Snooping Querier on a VLAN.

The no form of the command disables the IGMP Snooping Querier on a VLAN.

<b>Syntax Description</b>	N/A
<b>Default</b>	Disable
<b>Configuration Mode</b>	Config VLAN
<b>History</b>	3.3.4200
<b>Role</b>	admin
<b>Example</b>	<pre>switch (config vlan 1)# ip igmp snooping querier switch (config vlan 1)#{/pre&gt;</pre>
<b>Related Commands</b>	igmp snooping querier query-interval show ip igmp snooping querier
<b>Note</b>	

## igmp snooping querier query-interval

```
igmp snooping querier query-interval <time>
no igmp snooping querier query-interval
```

Configures the query interval.

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

Syntax Description	time	Time interval between queries (in seconds).
<b>Default</b>	125 seconds	
<b>Configuration Mode</b>	Config VLAN	
<b>History</b>	3.3.4200	
<b>Role</b>	admin	
<b>Example</b>		switch (config vlan 1)# igmp snooping querier query-interval 20 switch (config vlan 1)#
<b>Related Commands</b>		igmp snooping querier query-interval show ip igmp snooping querier
<b>Note</b>		

## **show ip igmp snooping**

## **show ip igmp snooping**

Displays IGMP snooping information for all VLANs or a specific VLAN.

## show ip igmp snooping groups

**show ip igmp snooping groups [vlan <vlan ID> [group <group IP>]]**

Displays per VLAN the list of multicast groups attached (static or dynamic allocated) per port.

<b>Syntax Description</b>	N/A
vlan	VLAN ID
group	Multicast group IP address
<b>Default</b>	N/A
<b>Configuration Mode</b>	Any Command Mode
<b>History</b>	3.1.1400
	3.6.1002 Updated Example
	3.6.2100 Added “vlan” and “group” parameters and updated Example
<b>Role</b>	admin
<b>Example</b>	<pre>switch (config) # show ip igmp snooping groups Vlan ID      Source      St/Dyn      Ports -----      -----      -----      ----- 1           12.10.10.1  Dyn          Eth1/2 1           12.11.11.2  St           Eth1/1 Total Num of Dynamic Group Addresses 1 Total Num of Static Group Addresses 1  switch (config) # show ip igmp snooping groups vlan 1 group 224.5.5.5 Snooping group information for VLAN 1 and group 224.5.5.5  Filter Mode: INCLUDE Include sources: 1.2.3.4 V1/V2 Receiver Ports: None V3 Receiver Ports: Port Number: Eth1/1 Include sources: 1.2.3.4 Exclude sources: None</pre>
<b>Related Commands</b>	
<b>Note</b>	

## show ip igmp snooping interfaces

### show ip igmp snooping interfaces

Displays IGMP snooping interface information.

<b>Syntax Description</b>	N/A
<b>Default</b>	N/A
<b>Configuration Mode</b>	Any Command Mode
<b>History</b>	3.1.1400
<b>Role</b>	admin
<b>Example</b>	<pre>switch (config) # show ip igmp snooping interfaces interface      leave-mode ----- 1/1            Normal 1/2            Normal 1/3            Normal 1/4            Fast ... switch (config) #</pre>
<b>Related Commands</b>	
<b>Note</b>	

## show ip igmp snooping membership

**show ip igmp snooping membership [vlan <VID> [group <group IP>]]**

Displays IGMP snooping querier counters.

<b>Syntax Description</b>	vlan	Displays IGMP snooping querier counters on specific VLAN
	group	Multicast group IP address
<b>Default</b>	N/A	
<b>Configuration Mode</b>	Any Command Mode	
<b>History</b>	3.6.2100	
<b>Role</b>	admin	
<b>Example</b>	<pre>switch (config) # show ip igmp snooping membership vlan 1 group 224.5.5.5 Snooping membership information for VLAN 1 and group 224.5.5.5  Receiver Port: Eth1/1 Attached Host: 10.10.10.1 Version: 3 Mode: Include Sources: 10.10.10.100 Timeout since the host has been joined: 0:00:02 Expiry timeout: 0:04:18</pre>	
<b>Related Commands</b>		
<b>Note</b>		

## show ip igmp snooping mrouter

**show ip igmp snooping mrouter**

Displays IGMP snooping multicast router information.

<b>Syntax Description</b>	N/A
<b>Default</b>	N/A
<b>Configuration Mode</b>	Any Command Mode
<b>History</b>	3.1.1400
<b>Role</b>	admin
<b>Example</b>	<pre>switch (config) # show ip igmp snooping mrouter Vlan      Ports -----  ----- 1          Eth1/1(static) switch (config) #</pre>
<b>Related Commands</b>	
<b>Note</b>	

## show ip igmp snooping querier

**show ip igmp snooping querier [vlan <num>]**

Displays running IGMP snooping querier configuration on the VLANs.

<b>Syntax Description</b>	vlan <num>	Displays the IGMP snooping querier configuration running on the specified VLAN.
<b>Default</b>	N/A	
<b>Configuration Mode</b>	Any Command Mode	
<b>History</b>	3.3.4200	
	3.6.2100	Updated Example
<b>Role</b>	admin	
<b>Example</b>	<pre>switch (config) # show ip igmp snooping querier vlan 1 Snooping querier information for VLAN 1  IGMP Querier Present Querier IP address: 10.10.10.10 Query interval: 125 Response interval: 100 Group membership interval: 1 Robustness: 2 Version: 3</pre>	
<b>Related Commands</b>		
<b>Note</b>		

## show ip igmp snooping querier counters

**show ip igmp snooping querier counters [vlan <num> [group <group-id>]]**

Displays IGMP snooping querier counters.

<b>Syntax Description</b>	vlan	Displays IGMP snooping querier counters on specific VLAN
	group	Multicast group IP address
<b>Default</b>	N/A	
<b>Configuration Mode</b>	Any Command Mode	
<b>History</b>	3.6.1002	
<b>Role</b>	admin	
<b>Example</b>	<pre>switch (config) # show ip igmp snooping querier counters vlan 10 Snooping querier counters for VLAN 10     General queries received: 0     General queries transmitted: 0     Group specific queries received : 0     Group specific queries transmitted : 0     Group source specific queries received : 0     Group source specific queries transmitted : 0     Leave messages received : 0     Leave messages transmitted : 0     V1/V2 reports received : 0     V1/V2 reports transmitted : 0     V3 reports received: 0     V3 reports transmitted: 0</pre>	
<b>Related Commands</b>		
<b>Note</b>		

## show ip igmp snooping statistics

### show ip igmp snooping statistics

Displays IGMP snooping statistical counters.

<b>Syntax Description</b>	N/A
<b>Default</b>	N/A
<b>Configuration Mode</b>	Any Command Mode
<b>History</b>	3.1.1400
	3.6.1002 Updated Example
	3.6.2100 Updated Example
<b>Role</b>	admin
<b>Example</b>	<pre>switch (config) # show ip igmp snooping statistics Snooping Statistics for VLAN 3770     General queries received : 3     General queries transmitted: 0     Group specific queries received : 0     Group specific queries transmitted: 0     Group and source specific queries received : 0     Group and source specific queries transmitted: 0     V1/V2 reports received : 0     V1/V2 reports transmitted : 0     Leave messages received : 0     Leave messages transmitted: 0     V3 reports received : 12     V3 reports transmitted : 0     Active Groups count: 2     Dropped packets: 0     Joins: 0</pre>
<b>Related Commands</b>	
<b>Note</b>	

## show ip igmp snooping vlan

**show ip igmp snooping vlan {<vlan/vlan-range> | all}**

Displays IGMP configuration per VLAN or VLAN range.

<b>Syntax Description</b>	vlan/vlan range	Displays IGMP VLAN configuration per specific VLAN or VLAN range.
	all	Display IGMP VLAN configuration on all VLAN.
<b>Default</b>	N/A	
<b>Configuration Mode</b>	Any Command Mode	
<b>History</b>	3.1.1400	
<b>Role</b>	admin	
<b>Example</b>	<pre>switch (config) # show ip igmp vlan 1 Vlan 1 configuration parameters:   IGMP snooping is enabled   IGMP version is V2   Snooping switch is acting as Non-Querier   mrouter static port list: Eth1/1   mrouter dynamic port list: none switch (config) #</pre>	
<b>Related Commands</b>		
<b>Note</b>		

## 5.14 Priority Flow Control

Priority Flow Control (PFC) provides an enhancement to the existing pause mechanism in Ethernet. The current Ethernet pause option stops all traffic on a link. PFC creates eight separate virtual links on the physical link and allows any of these links to be paused and restarted independently, enabling the network to create a no-drop class of service for an individual virtual link.

PFC offers the following features:

- Provides per-priority enabling or disabling of flow control
- Transmits PFC-PAUSE frames when the receive threshold for a particular traffic class is reached
- Provides the management capability for an administrator to configure the flow control properties on each port of the switch
- Keeps flow control disabled for all priorities on all ports by default
- Allows an administrator to enable or disable flow control per port and per priority level
- Supports flow control only on physical ports, not on logical interfaces such as tunnels or interfaces defined by sharing a physical port in multiple virtual switch contexts
- Uses the configured threshold values to set up the queue buffer spaces accordingly in the data-path
- Provides hardware abstraction layer call-outs for the following:
  - Enabling or disabling of flow control on each port for each priority
  - Configuring the queue depth for each priority on each port
- Provides trace logs for execution upon error conditions and for any event notifications from the hardware or data-path. These trace logs are a useful aid in troubleshooting.
- Allows the administrator to configure the minimum and maximum threshold values for flow control. These configurations are applied globally on all ports and priorities.

Priority Based Flow Control (PFC) provides an enhancement to the existing pause flow control mechanism as described in 802.1x.

➤ **To enable PFC globally:**

**Step 1.** Log in as admin.

**Step 2.** Enter config mode. Run:

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

**Step 3.** Enable PFC globally on the switch. Run:

```
switch (config) # dcb priority-flow-control enable
This action might cause traffic loss while shutting down a port with priority-flow-control mode on
Type 'yes' to confirm enable pfc globally: yes
```

➤ **To enable PFC per priority:**

**Step 1.** Log in as admin.

**Step 2.** Enter config mode. Run:

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

**Step 3.** Enable PFC globally on the switch. Run:

```
switch (config) # dcb priority-flow-control enable
# dcb priority-flow-control enable
This action might cause traffic loss while shutting down a port with priority-flow-control mode on
Type 'yes' to confirm enable pfc globally: yes
switch (config) #
```

**Step 4.** Choose the desirable priority you want to enable using the command `dcb priority-flow-control priority <pri[0..7]> enable`.

```
switch (config) # dcb priority-flow-control priority 5 enable
```

➤ **To enable PFC per interface:**

**Step 1.** Log in as admin.

**Step 2.** Change to config mode. Run:

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

**Step 3.** Enable PFC globally on the switch. Run:

```
switch (config) # dcb priority-flow-control enable
```

**Step 4.** Choose the desirable priority you want to enable using the command `dcb priority-flow-control priority <pri[0..7]> enable`

```
switch (config) # dcb priority-flow-control 5 enable
```

**Step 5.** Change to Interface mode. Run:

```
switch (config) #
switch (config) # interface ethernet 1/1
switch (config interface ethernet 1/1) #
```

**Step 6.** Enable PFC for the specific interface:

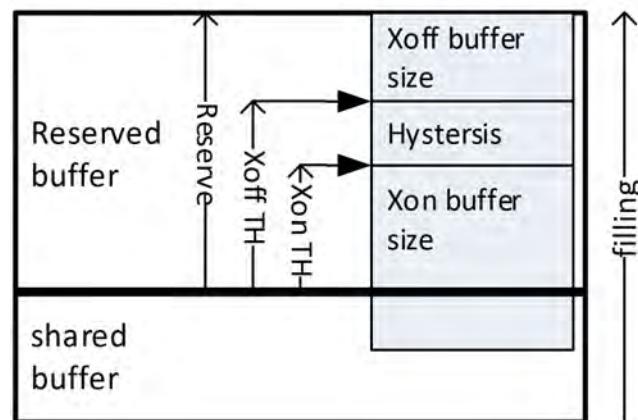
```
switch (config interface ethernet 1/1) # dcb priority-flow-control mode on
```

When working with lossless traffic, the receiving side sends a pause frame (Xoff) to the transmitting side before the buffer is filled. When the buffer empties, the receiving side sends an un-pause frame (Xon) to the transmitting side.

### 5.14.1 Flow Control Threshold Configuration for Spectrum

The user has to set the buffer usage Xoff and Xon thresholds. The thresholds depend on network parameters (bandwidth, link latency, MTU) and the allocated size for the region.

**Figure 25: Xon/Xoff Configuration**



When working with global flow control mode only, a single PG shall be used and Xoff and Xon shall be set on this PG. When working with priority flow control, Xoff and Xon shall be set on each lossless PG.



See Section 5.16, “Shared Buffers,” on page 975 for more information on flow control.

## 5.14.2 Commands

### dcb priority-flow-control enable

```
dcb priority-flow-control enable [force]
no dcb priority-flow-control enable [force]
```

Enables PFC globally on the switch.

The no form of the command globally disables PFC on the switch.

<b>Syntax Description</b>	force	Forces operation
<b>Default</b>	PFC is disabled.	
<b>Configuration Mode</b>	Config	
<b>History</b>	3.1.0000	
	3.3.0000	Updated Example
<b>Role</b>	admin	
<b>Example</b>	<pre>switch (config)# dcb priority-flow-control enable This action might cause traffic loss while shutting down a port with priority-flow-control mode on Type 'yes' to confirm enable pfc globally: yes switch (config)# show dcb priority-flow-control  PFC enabled Priority Enabled List      : Priority Disabled List    : 0 1 2 3 4 5 6 7  TC      Lossless ---  ----- 0          N 1          Y 2          Y 3          N  Interface      PFC admin      PFC oper -----  ----- 1/1          Disabled        Disabled 1/2          Disabled        Disabled 1/3          Disabled        Disabled 1/4          Disabled        Disabled ... switch (config) #</pre>	
<b>Related Commands</b>	show dcb priority-flow-control	
<b>Note</b>	This command asks the user to approve traffic loss because some interfaces with DCB mode activated might get shut down.	

## dcb priority-flow-control priority

**dcb priority-flow-control priority <prio> enable**  
**no dcb priority-flow-control priority <prio> enable**

Enables PFC per priority on the switch.

The no form of the command disables PFC per priority on the switch.

<b>Syntax Description</b>	prio	0-7.
<b>Default</b>	PFC is disabled for all priorities.	
<b>Configuration Mode</b>	Config	
<b>History</b>	3.1.0000	
<b>Role</b>	admin	
<b>Example</b>	<pre>switch (config)# dcb priority-flow-control priority 0 enable switch (config)# show dcb priority-flow-control  PFC enabled Priority Enabled List      : 0 Priority Disabled List     : 1 2 3 4 5 6 7  TC      Lossless ---  ----- 0        N 1        Y 2        Y 3        N  Interface      PFC admin      PFC oper -----  -----  ----- 1/1            Disabled       Disabled 1/2            Disabled       Disabled 1/3            Disabled       Disabled 1/4            Disabled       Disabled ... switch (config) #</pre>	
<b>Related Commands</b>	show dcb priority-flow-control	
<b>Note</b>		

## **dcb priority-flow-control mode on**

**dcb priority-flow-control mode on [force]**  
**no dcb priority-flow-control mode**

Enables PFC per interface.

The no form of the command disables PFC per interface.

<b>Syntax Description</b>	force	Force command implementation.																		
<b>Default</b>	PFC is disabled for all interfaces.																			
<b>Configuration Mode</b>	Config Interface Ethernet Config Interface Port Channel Config Interface MLAG Port Channel																			
<b>History</b>	3.1.0000																			
	3.3.4500	Added MLAG port-channel configuration mode																		
<b>Role</b>	admin																			
<b>Example</b>	<pre>switch (config interface ethernet 1/1) # dcb priority-flow-control mode on switch (config interface ethernet 1/1) # show dcb priority-flow-control  PFC enabled Priority Enabled List      : 0 Priority Disabled List     : 1 2 3 4 5 6 7  TC      Lossless ---  ----- 0       N 1       Y 2       Y 3       N</pre> <table border="1"> <thead> <tr> <th>Interface</th> <th>PFC admin</th> <th>PFC oper</th> </tr> </thead> <tbody> <tr> <td>1/1</td> <td>On</td> <td>Enabled</td> </tr> <tr> <td>1/2</td> <td>Disabled</td> <td>Disabled</td> </tr> <tr> <td>1/3</td> <td>Disabled</td> <td>Disabled</td> </tr> <tr> <td>1/4</td> <td>Disabled</td> <td>Disabled</td> </tr> <tr> <td>...</td> <td></td> <td></td> </tr> </tbody> </table>		Interface	PFC admin	PFC oper	1/1	On	Enabled	1/2	Disabled	Disabled	1/3	Disabled	Disabled	1/4	Disabled	Disabled	...		
Interface	PFC admin	PFC oper																		
1/1	On	Enabled																		
1/2	Disabled	Disabled																		
1/3	Disabled	Disabled																		
1/4	Disabled	Disabled																		
...																				
<b>Related Commands</b>	show dcb priority-flow-control																			
<b>Note</b>																				

## show dcb priority-flow-control

**show dcb priority-flow-control [interface <type> <inf>] [detail]**

Displays DCB priority flow control configuration and status.

<b>Syntax Description</b>	type	<ul style="list-style-type: none"> <li>• ethernet</li> <li>• port-channel</li> </ul>
	inf	The interface number.
	detail	Adds details information to the show output.
<b>Default</b>	N/A	
<b>Configuration Mode</b>	Any Command Mode	
<b>History</b>	3.1.0000	
<b>Role</b>	admin	
<b>Example</b>	<pre>switch (config interface ethernet 1/1) # show dcb priority-flow-control  PFC enabled Priority Enabled List      : 0 Priority Disabled List     : 1 2 3 4 5 6 7  TC      Lossless ---  ----- 0          N 1          Y 2          Y 3          N  Interface    PFC admin    PFC oper -----  -----  ----- 1/1        On           Enabled 1/2        Disabled     Disabled 1/3        Disabled     Disabled 1/4        Disabled     Disabled ... switch (config) #</pre>	

### Related Commands

### Note

## 5.15 Quality of Service (QoS)

### 5.15.1 QoS Classification

QoS classification assigns a QoS class to the packet. The QoS class of the packet is indicated internally in the switch using the switch-priority parameter (8 possible values).

Switch-priority affects the packet buffering and transmission scheduling. There are 8 possible values for switch-priority. The classification is based on the PCP and DEI fields in the VLAN tag, the DSCP field in the IP header. In addition, the default value can be configured for the incoming port. And the switch-priority of the packet also can be reconfigured by the ACL.

The switch-priority of the packet is used for priority fields re-marking at the egress.

#### 5.15.1.1 Trust Levels

QoS classification depends on the port configuration for QoS trust level which determines which packet header fields derive the switch-priority. The following trust states are supported:

- Trust port
  - Based on port default settings
- Trust L2 (PCP,DEI)
  - Based on packet PCP,DEI fields for VLAN tagged packets
  - Else, based on the port default setting for VLAN un-tagged packets
- Trust L3 (DSCP)
  - Else, based on packet DSCP field for IP packet
  - Else, based on port default setting for non-IP
- Trust both
  - Else, based on packet DSCP for IP packet
  - Else, based on packet PCP,DEI for VLAN tagged packets
  - Else, based on the port default setting

Table 56 and figure summarize the classification rules.

**Table 56 - Packet Classification Rules**

Packet Type		QoS Classification Config (per Interface)			
IP/MPLS	VLAN	Trust Both	Trust L3	Trust L2	Trust Port
IP/MPLS	Tagged	DSCP	DSCP	PCP,DEI	Port Default
IP/MPLS	Untagged	DSCP	DSCP	Port Default	Port Default
non-IP/MPLS	Tagged	PCP,DEI	Port Default	PCP,DEI	Port Default
non-IP/MPLS	Untagged	Port Default	Port Default	Port Default	Port Default

Default switch-priority is configured as trust L2.

### 5.15.1.2 Switch Priority to IEEE Priority Mapping

IEEE defines priority value for a packet which is used in the switch for the pause flow control. The device maps the switch-priority into IEEE priority value using device global switch priority to IEEE priority table.

### 5.15.1.3 Default QoS Configuration

*Table 57 - Default QoS Configuration*

Parameter	Range	Configuration
Trust level	All ports	Trust L2
DSCP to switch-priority	0-7	0
DSCP to switch-priority	8-15	1
DSCP to switch-priority	16-23	2
DSCP to switch-priority	24-31	3
DSCP to switch-priority	32-39	4
DSCP to switch-priority	40-47	5
DSCP to switch-priority	48-55	6
DSCP to switch-priority	56-63	7
PCP to switch-priority	0	0
PCP to switch-priority	1	1
PCP to switch-priority	2	2
PCP to switch-priority	3	3
PCP to switch-priority	4	4
PCP to switch-priority	5	5
PCP to switch-priority	6	6
PCP to switch-priority	7	7
Port PCP,DEI default	All ports	0
Port switch-priority when “trust port” is enabled	All ports	0
Switch-priority to IEEE priority	0	0
Switch-priority to IEEE priority	1	1
Switch-priority to IEEE priority	2	2
Switch-priority to IEEE priority	3	3
Switch-priority to IEEE priority	4	4
Switch-priority to IEEE priority	5	5
Switch-priority to IEEE priority	6	6
Switch-priority to IEEE priority	7	7

## 5.15.2 QoS Rewrite

Spectrum™ based switch systems enables rewriting QoS identifier values (DSCP, PCP, DEI) of incoming packets.

The configuration for preserving the values or rewriting them is set per ingress port. The configuration of the new values is set per egress port and is based on the mapping from the switch-priority.

In addition, the packets that pass the router module in the switch can be configured to change the “rewrite enable” configuration as well as the switch-priority.

### 5.15.2.1 Switch-priority to PCP,DEI Re-marking Mapping

Packet PCP and DEI fields can be updated by the switch based on switch-priority to PCP,DEI mapping tables. The mapping can be configured per egress port.

The reason for the mapping is to enable changing interpretation between two administrative domains in the network, or when a source of data is not fully trusted, and the default values are not desired. This mapping takes effect after deriving switch-priority from the PCP,DEI fields.

### 5.15.2.2 Switch-priority to DSCP Re-marking Mapping

Packet DSCP field can be updated based on switch-priority to DSCP mapping tables. The mapping can be configured per egress port. MPLS packets are untouched regardless this setting.

The reason for the mapping is to enable changing interpretation between two administrative domains in the network, or when a source of data is not fully trusted. This mapping will take affect after deriving switch-priority from the DSCP field.

### 5.15.2.3 DSCP to Switch-priority in Router

Spectrum™ enables mapping of DSCP to switch-priority in the router using a global mapping table.

This mapping has global configuration for whether to change the “Rewrite/Preserve PCP,DEI” bit. This configuration sets how the DSCP to switch-priority would affect the packet.

### 5.15.2.4 Default Configuration

- By default no ingress rewrite configuration is set
- By default PCP rewrite configuration in router is set
- The default mapping is as following:
  - Switch-priority= $i$  to PCP,DEI= $i,0$ ,  $i=0-7$
  - Switch-priority= $i$  to DSCP= $8i$ ,  $i=0-7$

## 5.15.3 Queuing and Scheduling (ETS) for SwitchX

Enhanced Transmission Selection (ETS) provides a common management framework for assignment of bandwidth to traffic classes, for weighted round robin (WRR) scheduling. If a traffic class does not use all the bandwidth allocated to it, other traffic classes can use that available

bandwidth. This allows optimal utilization of the network capacity while prioritizing and providing the necessary resources.

The ETS feature has the following attributes:

- ETS global admin:
  - Enable (default) – scheduling mode is WRR according to the configured bandwidth-per-traffic class
  - Disable – scheduling mode is Strict Priority (SP)
- Bandwidth percentage for each traffic class: By default each traffic class gets an equal share

The default mapping of priority to traffic classes (per interface) is as follows:

- Priority 0,1 mapped to TC 0
- Priority 2,3 mapped to TC 1
- Priority 4,5 mapped to TC 2
- Priority 6,7 mapped to TC 3



TC0 and TC3 are lossy TCs, while TC1 and TC2 can be lossless as well as lossy. It is possible but not recommended to map PFC enabled priorities (lossless traffic) to those TC0 or TC3.

ETS is enabled by default (scheduling is WRR).

➤ **To set the scheduling mode to Strict Priority:**

**Step 1.** Run the command `dcb ets disable`.

```
switch (config) # no dcb ets enable
```

➤ **To configure the WRR bandwidth percentage:**

**Step 1.** Make sure ETS feature is enabled. Run:

```
switch (config) # dcb ets enable
```

**Step 2.** Choose the WRR bandwidth rate and distribution.

By default the WRR distribution function is equal 25% per TC. Changing the WRR bandwidth will cause a change in the distribution function, for example if you wish to

schedule more traffic on TC-0, TC-1, TC-2 while reducing the amount of traffic sent on TC-3, run the command `dcb ets tc bandwidth`.

```
switch (config) # dcb ets tc bandwidth 30 30 30 10
# show dcb ets
```

ETS enabled

TC	Bandwidth
0	30%
1	30%
2	30%
3	10%

Number of Traffic Class: 4

```
switch (config) #
```



Traffic class priorities are <0-3>, where 0 is the lowest and 3 is the highest.



The sum of all traffic class bandwidth value (in percentage) should be 100, otherwise the command fails.

**Step 3.** Run the command `show dcb ets` to verify the configuration.

```
switch (config) # show dcb ets
ETS enabled
```

TC	Bandwidth
0	30%
1	30%
2	10%
3	30%

Number of Traffic Class: 4

```
switch (config) #
```

#### 5.15.4 Queuing and Scheduling (ETS) for Spectrum

After the output port of the packet is determined and the packet is buffered, it is queued for transmission. Each egress port is combined from the multi-level queuing structure. The scheduling of transmission from the queues relies on various configurations such as ETS weight, flow control, rate shaping etc.

#### 5.15.4.1 Traffic Class

The switch-priority of the packet assigns it to a specific traffic class (TClass). The TClass of the packet determines the packet path in the queuing structure. There are 8 TCs supported by the system.

#### 5.15.4.2 Traffic Shapers

##### Maximum Shapers

TCs can be configured for rate shaping as described in the following:

- TClass queues: shaper per TClass queue
- Port: shaper per port (bytes only)

Shapers support the following configurations:

- Committed Incoming Rate (CIR) [bits/packets per second]
- Committed Burst Size (CBS) [bytes/packets]

Each shaper has granularity rate of 1Mb/s, 10Mb/s, 100Mb/s and 1Gb/s (or 128K, 1280K, 12M, 128M pps). The maximum CBS is 3GB or 384M packets.

##### Minimum Shapers

TC queues can be configured for minimal rate shaping. The minimum shaper configuration overrides all other scheduling configurations. So that if ETS or WRR scheduling allocates to a TC queue lower rate than the configured minimum, that queue receives strictly higher priority over the others. If several queues receive a rate below the configured minimum, the arbitration between them can be configured as a WRR, or as strict according to the queue index.

The configuration of min shaper is identical to the configuration of max shaper.

#### 5.15.4.3 Default Shaper Configuration

*Table 58 - Default Shaper Configuration*

Parameter	Range	Configuration
Switch-priority to TC	0	0
Switch-priority to TC	1	1
Switch-priority to TC	2	2
Switch-priority to TC	3	3
Switch-priority to TC	4	4
Switch-priority to TC	5	5
Switch-priority to TC	6	6
Switch-priority to TC	7	7
Shaping	All ports	No max/min shaping configured

### 5.15.5 RED and ECN



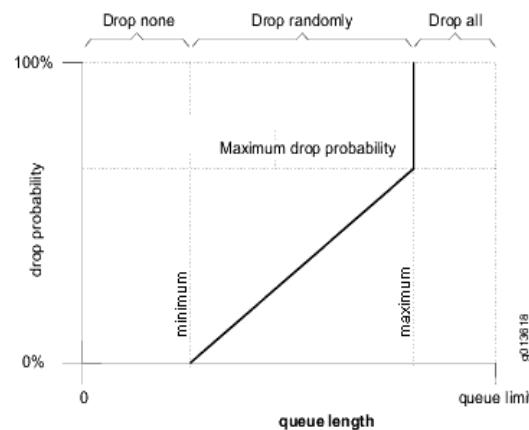
Supported only on Spectrum™ based switch systems.

Random early detection (RED) is a mechanism that randomly drops packets before the switch buffer fills up in case of congestion. Explicit congestion notification (ECN) is used for congestion control protocols (TCP and RoCE CC – DCQCN) to handle congestion before packets are dropped. RED and ECN can be configured separately or concurrently per traffic class.

Spectrum™ based systems support relative RED/ECN on TC queues. This feature allows the thresholds of the drop/mark actions to behave relatively to the dynamic thresholds configured for the shared buffer.

RED/ECN drop profiles are defined according to 2 parameters as shown in Figure 26:

**Figure 26: RED/ECN Drop Profiles**



- Minimum – a threshold that defines the average queue length below which the packets are not dropped/mark
- Maximum – a threshold that defines the average queue length above which the packets are always dropped/mark

It is possible to configure the minimum and maximum thresholds to have the same value which would represent a step function from “drop none” to “drop all”.



Spectrum™ based systems support RED/ECN only for unicast traffic classes.

## 5.15.6 Commands

### 5.15.6.1 QoS Classification

#### vlan default priority

**vlan default priority [<priority>]**  
**no vlan default priority [<priority>]**

Configures default PCP for packets arrived without VLAN tag.  
The no form of the command resets the value to its default.

<b>Syntax Description</b>	priority	Range: 0-7
<b>Default</b>	0	
<b>Configuration Mode</b>	Config Interface Ethernet Config Interface Port Channel Config Interface MLAG Port Channel	
<b>History</b>	3.6.1002	
<b>Role</b>	admin	
<b>Example</b>	switch (config interface ethernet 1/1) # vlan default priority 0	
<b>Related Commands</b>	N/A	
<b>Notes</b>	This command is only supported on Spectrum™ based switch systems	

## vlan default dei

```
vlan default dei [<dei>]  
no vlan default dei [<dei>]
```

Configures default DEI for packets arrived without VLAN tag.  
The no form of the command resets the value to its default.

<b>Syntax Description</b>	N/A
<b>Default</b>	0
<b>Configuration Mode</b>	Config Interface Ethernet Config Interface Port Channel Config Interface MLAG Port Channel
<b>History</b>	3.6.1002
<b>Role</b>	admin
<b>Example</b>	switch (config interface ethernet 1/1) # vlan default dei 0
<b>Related Commands</b>	N/A
<b>Notes</b>	This command is only supported on Spectrum™ based switch systems

## qos trust

```
qos trust [port | L2 | L3 | both]  
no qos trust [port | L2 | L3 | both]
```

Configures QoS trust mode for the interface.  
The no form of the command resets the value to its default.

<b>Syntax Description</b>	N/A
<b>Default</b>	L2
<b>Configuration Mode</b>	Config Interface Ethernet Config Interface Port Channel Config Interface MLAG Port Channel
<b>History</b>	3.6.1002
<b>Role</b>	admin
<b>Example</b>	switch (config interface ethernet 1/1) # qos trust L2
<b>Related Commands</b>	N/A
<b>Notes</b>	This command is only supported on Spectrum™ based switch systems

## **qos default switch-priority**

```
qos default switch-priority [<switch-priority>]  
no qos default switch-priority [<switch-priority>]
```

Configures default switch-priority for interface when “port” trust mode is active, or for non-IP and untagged packets in other trust modes.  
The no form of the command resets the value to its default.

<b>Syntax Description</b>	switch-priority	Range: 0-7
<b>Default</b>	0	
<b>Configuration Mode</b>	Config Interface Ethernet Config Interface Port Channel Config Interface MLAG Port Channel	
<b>History</b>	3.6.1002	
<b>Role</b>	admin	
<b>Example</b>	switch (config interface ethernet 1/1) # qos default switch-priority 0	
<b>Related Commands</b>	qos trust	
<b>Notes</b>	This command is only supported on Spectrum™ based switch systems	

## **qos map pcp dei**

**qos map pcp <pcp> dei <dei> [to switch-priority <switch-priority>]  
no qos map pcp <pcp> dei <dei> [to switch-priority <switch-priority>]**

Configures interface PCP,DEI to switch-priority mapping for IP/MPLS and non-IP/MPLS tagged packets in “L2” trust mode and for non-IP/MPLS tagged packets in “both” trust mode.

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

<b>Syntax Description</b>	N/A
<b>Default</b>	PCP to switch-priority mapping: 0 → 0 1 → 1 2 → 2 3 → 3 4 → 4 5 → 5 6 → 6 7 → 7
<b>Configuration Mode</b>	Config Interface Ethernet Config Interface Port Channel Config Interface MLAG Port Channel
<b>History</b>	3.6.1002
<b>Role</b>	admin
<b>Example</b>	switch (config interface ethernet 1/1) # qos map pcp 5 dei 5
<b>Related Commands</b>	qos trust
<b>Notes</b>	This command is only supported on Spectrum™ based switch systems

## **qos map dscp**

**qos map dscp <dscp> [to switch-priority <switch-priority>]  
no qos map dscp <dscp> [to switch-priority <switch-priority>]**

Configures interface DSCP to switch-priority mapping in “L3” or “both” trust mode.  
The no form of the command resets the value to its default.

<b>Syntax Description</b>	switch-priority	Range: 0-7
	dscp	Range: 0-63
<b>Default</b>	DSCP to switch-priority mapping:	0-7 → 0 8-15 → 1 16-23 → 2 24-31 → 3 32-39 → 4 40-47 → 5 48-55 → 6 56-63 → 7
<b>Configuration Mode</b>	Config Interface Ethernet Config Interface Port Channel Config Interface MLAG Port Channel	
<b>History</b>	3.6.1002	
<b>Role</b>	admin	
<b>Example</b>	switch (config interface ethernet 1/1) # qos map dscp 45	
<b>Related Commands</b>	qos trust	
<b>Notes</b>	This command is only supported on Spectrum™ based switch systems	

## show qos

**show qos [interface <type> <number>]**

Displays QoS information.

<b>Syntax Description</b>	N/A	
<b>Default</b>	DSCP to switch-priority mapping:	0-7 → 0 8-15 → 1 16-23 → 2 24-31 → 3 32-39 → 4 40-47 → 5 48-55 → 6 56-63 → 7
<b>Configuration Mode</b>	Any Command Mode	
<b>History</b>	3.6.1002	
<b>Role</b>	admin	

**Example**

```
switch (config) # show qos interface ethernet 1/1
Eth1/1
Trust mode: L2
Default switch-priority: 0
Default PCP: 0
Default DEI: 0
PCP,DEI rewrite: disabled
IP PCP,DEI rewrite: preserve (router is disabled)
DSCP rewrite: disabled

PCP,DEI to switch-priority mapping:
PCP,DEI  switch-priority
-----
0,0      0
1,0      1
2,0      2
...
6,1      6
7,1      7

DSCP to switch-priority mapping:
DSCP  switch-priority
-----
0      0
1      0
2      0
...
62     7
63     7

PCP,DEI rewrite mapping (switch-priority to PCP,DEI):
switch-priority  PCP,DEI
-----
0              0,0
1              1,0
2              2,0
...

DSCP rewrite mapping (switch-priority to DSCP):
switch-priority  DSCP
-----
0              0
1              8
2              16
...
```

**Related Commands**

N/A

**Notes**

This command is only supported on Spectrum™ based switch systems

## show interfaces ethernet counters tc

**show interfaces ethernet <slot/port> counters tc <priority>**

Displays traffic group counters for the specified interface and priority.

<b>Syntax Description</b>	slot/port	Number of Ethernet interface in form of slot/port
	priority	Valid priority values: 0-7 or all
<b>Default</b>	N/A	
<b>Configuration Mode</b>	Any Command Mode	
<b>History</b>	3.6.3004	
<b>Role</b>	admin	
<b>Example</b>	<pre>switch (config) # show interfaces ethernet 1/1 counters tc 3</pre> <pre>TC 3  0          packets  0          bytes  0          queue depth  0          unicast no buffer discard  0          WRED discard</pre>	
<b>Related Commands</b>		
<b>Note</b>	This command is only supported on Spectrum™ based switch systems	

## show interfaces ethernet counters pg

**show interfaces ethernet <slot/port> counters pg <priority>**

Displays port group counters for the specified interface and priority.

<b>Syntax Description</b>	slot/port	Number of Ethernet interface in form of slot/port
	priority	Valid priority values: 0-7 or all
<b>Default</b>	N/A	
<b>Configuration Mode</b>	Any Command Mode	
<b>History</b>	3.6.3004	
<b>Role</b>	admin	
<b>Example</b>	<pre>switch (config) # show interfaces ethernet 1/1 counters pg 4</pre> <pre>PG 4  0          packets  0          bytes  0          queue depth  0          no buffer discard  0          shared buffer discard</pre>	
<b>Related Commands</b>		
<b>Note</b>	This command is only supported on Spectrum™ based switch systems	

## show interfaces ethernet counters pfc prio

**show interfaces ethernet <slot/port> counters pfc prio <priority>**

Displays priority flow control counters for the specified interface and priority.

<b>Syntax Description</b>	slot/port	Number of Ethernet interface in form of slot/port
	priority	Valid priority values: 0-7 or all
<b>Default</b>	N/A	
<b>Configuration Mode</b>	Any Command Mode	
<b>History</b>	3.6.3004	
<b>Role</b>	admin	
<b>Example</b>	<pre>switch (config) # show interfaces ethernet 1/1 counters pfc prio 1  PFC 1  Rx   0          pause packets   0          pause duration  Tx   0          pause packets   0          pause duration</pre>	
<b>Related Commands</b>		
<b>Note</b>	This command is only supported on Spectrum™ based switch systems	

## show qos interface

**show qos interface <type> <port-id>**

Display QoS information.

<b>Syntax Description</b>	type	Ethernet, port-channel, or mlag-port-channel
<b>Default</b>	N/A	
<b>Configuration Mode</b>	Any Command Mode	
<b>History</b>	3.6.5000	
<b>Role</b>	admin	
<b>Example</b>	<pre>switch (config)# show qos interface ethernet 1/5 Eth1/5 Trust mode: L2 Default switch-priority: 0 Default PCP: 0 Default DEI: 0 PCP,DEI rewrite: disabled IP PCP;DEI rewrite: enabled DSCP rewrite: disabled  PCP(DEI); DSCP to switch-priority mapping: ----- PCP(DEI)          DSCP          switch-priority ----- 0(0) 0(1)          0 1 2 3 4 5 6 7          0 1(0) 1(1)          8 9 10 11 12 13 14 15         1 2(0) 2(1)          16 17 18 19 20 21 22 23        2 3(0) 3(1)          24 25 26 27 28 29 30 31        3 4(0) 4(1)          32 33 34 35 36 37 38 39        4 5(0) 5(1)          40 41 42 43 44 45 46 47        5 6(0) 6(1)          48 49 50 51 52 53 54 55        6 7(0) 7(1)          56 57 58 59 60 61 62 63        7  PCP(DEI); DSCP rewrite mapping (switch-priority to PCP(DEI); DSCP; traffic-class): ----- switch-priority    PCP(DEI)    DSCP    TC ----- 0                  0(0)      0       0 1                  1(0)      8       1 2                  2(0)      16      2 3                  3(0)      24      3 4                  4(0)      32      4 5                  5(0)      40      5 6                  6(0)      48      6 7                  7(0)      56      7</pre>	

### Related Commands

### Note

## show qos interface l2-mapping

**show qos interface <type> <port-id> l2-mapping**

Displays the PCP, DEI to switch priority table.

<b>Syntax Description</b>	type	Ethernet, port-channel, or mlag-port-channel
<b>Default</b>	N/A	
<b>Configuration Mode</b>	Any Command Mode	
<b>History</b>	3.6.5000	
<b>Role</b>	admin	
<b>Example</b>	<pre>switch (config)# show qos interface ethernet 1/9 l2-mapping  PCP,DEI to switch-priority mapping: ----- PCP(DEI)          switch-priority ----- 0(0) 0(1)          0 1(0) 1(1)          1 2(0) 2(1)          2 3(0) 3(1)          3 4(0) 4(1)          4 5(0) 5(1)          5 6(0) 6(1)          6 7(0) 7(1)          7</pre>	
<b>Related Commands</b>		
<b>Note</b>		

## show qos interface l3-mapping

**show qos interface <type> <port-id> l3-mapping**

Displays the DSCP to switch priority table.

<b>Syntax Description</b>	type	Ethernet, port-channel, or mlag-port-channel
<b>Default</b>	N/A	
<b>Configuration Mode</b>	Any Command Mode	
<b>History</b>	3.6.5000	
<b>Role</b>	admin	
<b>Example</b>	<pre>switch (config)# show qos interface ethernet 1/9 l3-mapping  IP PCP,DEI rewrite: enabled DSCP to switch-priority mapping: ----- DSCP                      switch-priority ----- 0 1 2 3 4 5 6 7              0 8 9 10 11 12 13 14 15        1 16 17 18 19 20 21 22 23      2 24 25 26 27 28 29 30 31      3 32 33 34 35 36 37 38 39      4 40 41 42 43 44 45 46 47      5 48 49 50 51 52 53 54 55      6 56 57 58 59 60 61 62 63      7</pre>	

---

### Related Commands

---

### Note

---

## show qos interface rewrite-mapping

**show qos interface <type> <port-id> rewrite-mapping**

Displays the rewrite mapping of switch priority to PCP, DEI and DSCP table.

<b>Syntax Description</b>	type	Ethernet, port-channel, or mlag-port-channel
<b>Default</b>	N/A	
<b>Configuration Mode</b>	Any Command Mode	
<b>History</b>	3.6.5000	
<b>Role</b>	admin	
<b>Example</b>	<pre>switch (config)# show qos interface ethernet 1/9 rewrite-mapping  PCP,DEI rewrite: disabled IP PCP,DEI rewrite: enabled DSCP rewrite: disabled  Rewrite mapping (switch-priority to PCP,DEI,DSCP):  Egress Interface: Eth1/9 ----- switch-priority    PCP(DEI)    DSCP      TC ----- 0                  0(0)       0         0 1                  1(0)       8         1 2                  2(0)       16        2 3                  3(0)       24        3 4                  4(0)       32        4 5                  5(0)       40        5 6                  6(0)       48        6 7                  7(0)       56        7</pre>	

---

### Related Commands

---

### Note

## show qos interface tc-mapping

**show qos interface <type> <port-id> tc-mapping**

Displays mapping from switch priority to traffic class.

<b>Syntax Description</b>	type	Ethernet, port-channel, or mlag-port-channel		
<b>Default</b>	N/A			
<b>Configuration Mode</b>	Any Command Mode			
<b>History</b>	3.6.5000			
<b>Role</b>	admin			
<b>Example</b>	<pre>switch (config)# show qos interface ethernet 1/9 tc-mapping Switch Priority to TC mapping: ----- Switch Priority    TC ----- 0                  0 1                  1 2                  2 3                  3 4                  4 5                  5 6                  6 7                  7</pre>			
<hr/>				
<b>Related Commands</b>				
<hr/>				
<b>Note</b>				
<hr/>				

## show qos mapping ingress interface egress interface

```
show qos mapping ingress interface <type> <port-id> egress interface <type>
<port-id>
```

Displays end to end mapping configuration: ingress to egress.

<b>Syntax Description</b>	type	Ethernet, port-channel, or mlag-port-channel																																																																
<b>Default</b>	N/A																																																																	
<b>Configuration Mode</b>	Any Command Mode																																																																	
<b>History</b>	3.6.5000																																																																	
<b>Role</b>	admin																																																																	
<b>Example</b>	<pre>switch (config)# show qos mapping ingress interface ethernet 1/8 egress interface ethernet 1/9  Ingress Interface: Eth1/8 Trust mode: L2 Default Switch Priority: 0 Rewrite PCP,DEI: disabled Rewrite DSCP : disabled  Global Rewrite mode: enabled  PCP,DEI and DSCP to switch-priority mapping:</pre> <hr/> <table> <thead> <tr> <th>PCP,DEI</th> <th>DSCP</th> <th>switch-priority</th> </tr> </thead> <tbody> <tr><td>0(0) 0(1)</td><td>0 1 2 3 4 5 6 7</td><td>0</td></tr> <tr><td>1(0) 1(1)</td><td>8 9 10 11 12 13 14 15</td><td>1</td></tr> <tr><td>2(0) 2(1)</td><td>16 17 18 19 20 21 22 23</td><td>2</td></tr> <tr><td>3(0) 3(1)</td><td>24 25 26 27 28 29 30 31</td><td>3</td></tr> <tr><td>4(0) 4(1)</td><td>32 33 34 35 36 37 38 39</td><td>4</td></tr> <tr><td>5(0) 5(1)</td><td>40 41 42 43 44 45 46 47</td><td>5</td></tr> <tr><td>6(0) 6(1)</td><td>48 49 50 51 52 53 54 55</td><td>6</td></tr> <tr><td>7(0) 7(1)</td><td>56 57 58 59 60 61 62 63</td><td>7</td></tr> </tbody> </table> <hr/> <table> <thead> <tr> <th>switch-priority</th> <th>PCP(DEI)</th> <th>DSCP</th> <th>TC</th> </tr> </thead> <tbody> <tr><td>0</td><td>0(0)</td><td>0</td><td>0</td></tr> <tr><td>1</td><td>1(0)</td><td>8</td><td>1</td></tr> <tr><td>2</td><td>2(0)</td><td>16</td><td>2</td></tr> <tr><td>3</td><td>3(0)</td><td>24</td><td>3</td></tr> <tr><td>4</td><td>4(0)</td><td>32</td><td>4</td></tr> <tr><td>5</td><td>5(0)</td><td>40</td><td>5</td></tr> <tr><td>6</td><td>6(0)</td><td>48</td><td>6</td></tr> <tr><td>7</td><td>7(0)</td><td>56</td><td>7</td></tr> </tbody> </table>			PCP,DEI	DSCP	switch-priority	0(0) 0(1)	0 1 2 3 4 5 6 7	0	1(0) 1(1)	8 9 10 11 12 13 14 15	1	2(0) 2(1)	16 17 18 19 20 21 22 23	2	3(0) 3(1)	24 25 26 27 28 29 30 31	3	4(0) 4(1)	32 33 34 35 36 37 38 39	4	5(0) 5(1)	40 41 42 43 44 45 46 47	5	6(0) 6(1)	48 49 50 51 52 53 54 55	6	7(0) 7(1)	56 57 58 59 60 61 62 63	7	switch-priority	PCP(DEI)	DSCP	TC	0	0(0)	0	0	1	1(0)	8	1	2	2(0)	16	2	3	3(0)	24	3	4	4(0)	32	4	5	5(0)	40	5	6	6(0)	48	6	7	7(0)	56	7
PCP,DEI	DSCP	switch-priority																																																																
0(0) 0(1)	0 1 2 3 4 5 6 7	0																																																																
1(0) 1(1)	8 9 10 11 12 13 14 15	1																																																																
2(0) 2(1)	16 17 18 19 20 21 22 23	2																																																																
3(0) 3(1)	24 25 26 27 28 29 30 31	3																																																																
4(0) 4(1)	32 33 34 35 36 37 38 39	4																																																																
5(0) 5(1)	40 41 42 43 44 45 46 47	5																																																																
6(0) 6(1)	48 49 50 51 52 53 54 55	6																																																																
7(0) 7(1)	56 57 58 59 60 61 62 63	7																																																																
switch-priority	PCP(DEI)	DSCP	TC																																																															
0	0(0)	0	0																																																															
1	1(0)	8	1																																																															
2	2(0)	16	2																																																															
3	3(0)	24	3																																																															
4	4(0)	32	4																																																															
5	5(0)	40	5																																																															
6	6(0)	48	6																																																															
7	7(0)	56	7																																																															

### Related Commands

#### Note

## 5.15.6.2 QoS Rewrite

### **qos rewrite pcp**

**qos rewrite pcp-enable**  
**qos rewrite pcp-disable**

Enables or disables PCP,DEI rewrite on the interface.

<b>Syntax Description</b>	N/A
<b>Default</b>	Disabled
<b>Configuration Mode</b>	Config Interface Ethernet Config Interface Port Channel Config Interface MLAG Port Channel
<b>History</b>	3.6.1002
<b>Role</b>	admin
<b>Example</b>	switch (config interface ethernet 1/1) # qos rewrite pcp-enable
<b>Related Commands</b>	
<b>Notes</b>	This command is only supported on Spectrum™ based switch systems

## **qos rewrite dscp**

**qos rewrite dscp-enable**  
**qos rewrite dscp-disable**

Enables or disables DSCP rewrite on the interface.

<b>Syntax Description</b>	N/A
<b>Default</b>	Disabled
<b>Configuration Mode</b>	Config Interface Ethernet Config Interface Port Channel Config Interface MLAG Port Channel
<b>History</b>	3.6.1002
<b>Role</b>	admin
<b>Example</b>	switch (config interface ethernet 1/1) # qos rewrite dscp-enable
<b>Related Commands</b>	
<b>Notes</b>	This command is only supported on Spectrum™ based switch systems

## **qos rewrite map switch-priority pcp dei**

**qos rewrite map switch-priority <switch-priority> pcp <pcp> dei <dei>**  
**no qos rewrite map switch-priority <switch-priority> pcp <pcp> dei <dei>**

Configures switch-priority to PCP,DEI mapping on the interface.  
The no form of the command resets the value to their defaults.

<b>Syntax Description</b>	switch-priority pcp dei	Range: 0-7 Range: 0-7 Value: 0
<b>Default</b>	Switch priority to PCP,DEI mapping:	Switch priority → PCP,DEI: 0 → 0,0 1 → 1,0 2 → 2,0 3 → 3,0 4 → 4,0 5 → 5,0 6 → 6,0 7 → 7,0
<b>Configuration Mode</b>	Config Interface Ethernet Config Interface Port Channel Config Interface MLAG Port Channel	
<b>History</b>	3.6.1002	
<b>Role</b>	admin	
<b>Example</b>	switch (config interface ethernet 1/1) # qos rewrite map switch-priority 11 pcp 7 dei 0	
<b>Related Commands</b>	N/A	
<b>Notes</b>	This command is only supported on Spectrum™ based switch systems	

## **qos rewrite map switch-priority dscp**

```
qos rewrite map switch-priority <switch-priority> dscp <dscp>
no qos rewrite map switch-priority <switch-priority> dscp <dscp>
```

Configures switch-priority to DSCP mapping on the interface.  
The no form of the command resets the value to their defaults.

<b>Syntax Description</b>	N/A
<b>Default</b>	Switch priority to DSCP mapping: 0 → 0 1 → 8 2 → 16 3 → 24 4 → 32 5 → 40 6 → 48 7 → 54
<b>Configuration Mode</b>	Config Interface Ethernet Config Interface Port Channel Config Interface MLAG Port Channel
<b>History</b>	3.6.1002
<b>Role</b>	admin
<b>Example</b>	<pre>switch (config interface ethernet 1/1) # qos rewrite map switch -priority 5 dscp 40</pre>
<b>Related Commands</b>	N/A
<b>Notes</b>	This command is only supported on Spectrum™ based switch systems

## **qos ip rewrite pcp**

```
qos ip rewrite pcp [disable | enable | preserve]
no qos ip rewrite pcp [disable | enable | preserve]
```

Enables or preserves the rewrite of PCP, DEI of routed packets in egress interface.  
The no form of the command resets the value to their defaults.

<b>Syntax Description</b>	disable	No rewrite occurs
	enable	PCP,DEI are rewritten based on the mapping configured on the egress port
	preserve	Ingress interface configuration determines action
<b>Default</b>	Default is “preserve” when router is disabled Default is “enable” when router is enabled (Router can be enabled/disabled using the “ip routing” command)	
<b>Configuration Mode</b>	Config	
<b>History</b>	3.6.1002	
<b>Role</b>	admin	
<b>Example</b>	switch (config) # qos ip rewrite pcp enable	
<b>Related Commands</b>	N/A	
<b>Notes</b>	The parameter “preserve” is only supported on Spectrum based switch systems	

### 5.15.6.3 Queuing and Scheduling (ETS)

#### **dcb ets enable**

**dcb ets enable**  
**no dcb ets enable**

Sets the switch egress scheduling mode to be weighted round robin.  
The no form of the command sets the switch egress scheduling mode to be strict priority.

<b>Syntax Description</b>	N/A	
<b>Default</b>	ETS is enabled	
<b>Configuration Mode</b>	Config	
<b>History</b>	3.1.0000	
	3.6.1002	Updated Note
<b>Role</b>	admin	
<b>Example</b>	switch (config)# dcb ets enable	
<b>Related Commands</b>	show dcb ets	
<b>Note</b>		

## dcb ets tc bandwidth

**dcb ets tc bandwidth <tc-0> <tc-1> <tc-2> <tc-3>**  
**no dcb ets tc bandwidth**

Configures the bandwidth limit of the traffic class.

The no form of the command sets the bandwidths per traffic class back to its default.

<b>Syntax Description</b>	tc-i	0-100.
<b>Default</b>	25% per traffic class	
<b>Configuration Mode</b>	Config	
<b>History</b>	3.1.0000	
	3.6.1002	Updated Note
<b>Role</b>	admin	
<b>Example</b>	switch (config)# dcb ets tc bandwidth 20 20 30 30	
<b>Related Commands</b>	show dcb ets	
<b>Note</b>	<ul style="list-style-type: none"><li>• The sum of all traffic class bandwidth must be equal to 100</li><li>• This command is only supported on SwitchX® based switch systems</li></ul>	

## vlan map-priority

```
vlan map priority <priority> traffic-class <tc>
no vlan map priority <priority>
```

Maps an VLAN user priority to a traffic class.  
The no form of the command sets the mapping back to default.

<b>Syntax Description</b>	N/A	
<b>Default</b>	Priority 0,1 mapped to tc 0 Priority 2,3 mapped to tc 1 Priority 4,5 mapped to tc 2 Priority 6,7 mapped to tc 3	
<b>Configuration Mode</b>	Config Interface Ethernet	
<b>History</b>	3.1.0000 3.6.1002                          Updated Note	
<b>Role</b>	admin	
<b>Example</b>	switch (config interface ethernet 1/1) # vlan map-priority 1 traffic-class 2	
<b>Related Commands</b>	show dcb ets interface	
<b>Note</b>	This command is only supported on SwitchX® based switch systems	

## show dcb ets (SwitchX)

**show dcb ets**

Displays ETS configuration and operational data.

**Syntax Description** N/A

**Default** ETS is enabled.

**Configuration Mode** Any Command Mode

**History** 3.1.0000

3.6.1002 Updated Note

**Role** admin

**Example**

```
switch (config)# show dcb ets

ETS enabled

TC      Bandwidth
-----
0       25%
1       25%
2       25%
3       25%

Number of Traffic Class: 4
```

**Related Commands**

**Note** The show command output is from a SwitchX® based switch system

## bind switch-priority

**bind switch-priority [<priority\_1> [<priority\_2> .. <priority\_n>]]**  
**no bind switch-priority [<priority>]**

Configures binding of switch-priority to traffic class.

The no form of the command:

- When run in the interface configuration mode: Resets to default the binding of all switch-priorities from all traffic classes
- When run in the interface's traffic class: Negates the binding of a specific switch-priority from a specific traffic class

<b>Syntax Description</b>	N/A
<b>Default</b>	Switch priority to traffic class mapping: 0 → 0 1 → 1 2 → 2 3 → 3 4 → 4 5 → 5 6 → 6 7 → 7
<b>Configuration Mode</b>	Config Interface Ethernet Config Interface Ethernet Traffic Class Config Interface Port Channel Config Interface Port Channel Traffic Class Config Interface MLAG Port Channel Config Interface MLAG Port Channel Traffic Class
<b>History</b>	3.6.1002
<b>Role</b>	admin
<b>Example</b>	<pre>switch (config interface ethernet 1/1 traffic-class 0) # bind switch- property 1</pre>
<b>Related Commands</b>	N/A
<b>Notes</b>	<ul style="list-style-type: none"> <li>• Context is egress interface traffic class</li> <li>• This command is only supported on Spectrum™ based switch systems</li> </ul>

## bandwidth guaranteed

**bandwidth guaranteed [<rate>]**  
**no bandwidth guaranteed [<rate>]**

Configures the minimum bandwidth for outbound traffic.

<b>Syntax Description</b>	rate	Rate in GbE Range: 0 - max speed supported
<b>Default</b>	0	
<b>Configuration Mode</b>	Config Interface Ethernet Traffic Class Config Interface Port Channel Traffic Class Config Interface MLAG Port Channel Traffic Class	
<b>History</b>	3.6.1002	
<b>Role</b>	admin	
<b>Example</b>	switch (config interface ethernet 1/1 traffic-class 0) # bandwidth guaranteed 0.4G	
<b>Related Commands</b>	N/A	
<b>Notes</b>	<ul style="list-style-type: none"><li>Context is egress interface traffic class</li><li>Bandwidth guaranteed rate determines the bandwidth guaranteed by the switch for outbound traffic assigned to this traffic class on this interface</li><li>Bandwidth is in granularity of 0.2G</li><li>This command is only supported on Spectrum™ based switch systems</li></ul>	

## bandwidth shape

**bandwidth shape [<rate>]**  
**no bandwidth shape [<rate>]**

Configures the bandwidth shaper for outbound traffic.

<b>Syntax Description</b>	rate Range: 0 - max speed supported	Rate in GbE
<b>Default</b>	Maximum port rate (100GbE on Spectrum™ based switches)	
<b>Configuration Mode</b>	Config Interface Ethernet Traffic Class Config Interface Port Channel Traffic Class Config Interface MLAG Port Channel Traffic Class	
<b>History</b>	3.6.1002	
<b>Role</b>	admin	
<b>Example</b>	switch (config interface ethernet 1/1 traffic-class 7) # bandwidth shape 0.4G	
<b>Related Commands</b>	N/A	
<b>Notes</b>	<ul style="list-style-type: none"> <li>Context is egress interface traffic class and/or port</li> <li>Bandwidth shape rate determines the bandwidth of the shaper for outbound traffic assigned to this traffic class on this interface</li> <li>Bandwidth is in granularity of 0.2G</li> <li>This command is only supported on Spectrum™ based switch systems</li> </ul>	

## dcb ets

```
dcb ets [strict | wrr <weight>]  
no dcb ets [strict | wrr <weight>]
```

Configures ETS mode to strict or WRR.

<b>Syntax Description</b>	weight
<b>Default</b>	Default is WRR with the following default weights.  Traffic class to weight mapping: 0 → 12 1 → 13 2 → 12 3 → 13 4 → 12 5 → 13 6 → 12 7 → 13
<b>Configuration Mode</b>	Config Interface Ethernet Traffic Class Config Interface Port Channel Traffic Class Config Interface MLAG Port Channel Traffic Class
<b>History</b>	3.6.1002
<b>Role</b>	admin
<b>Example</b>	switch (config interface ethernet 1/1 traffic-class 1) # dcb ets wrr 50
<b>Related Commands</b>	N/A
<b>Notes</b>	<ul style="list-style-type: none"><li>• Context is egress interface traffic class</li><li>• This command is only supported on Spectrum™ based switch systems</li></ul>

## show dcb ets (Spectrum)

**show dcb ets [interface {ethernet | mlag-port-channel | port-channel} <number>]**

Displays ETS information.

<b>Syntax Description</b>	N/A
<b>Default</b>	N/A
<b>Configuration Mode</b>	Any Command Mode
<b>History</b>	3.6.1002
	3.6.5000 Updated example output
<b>Role</b>	admin
<b>Example</b>	<pre>switch (config)# show dcb ets interface ethernet 1/1 Eth1/1: Interface Bandwidth Shape [Mbps]: N/A Multicast unaware mapping: disabled  Flags:   S.Mode: Scheduling Mode [Strict/WRR]   D: -   W: Weight   Bw.Sh: Bandwidth Shaper   Bw.Gr: Bandwidth Guaranteed  ETS per TC: ----- TC  S.Mode      W     W(%)   BW Sh.(Mbps)  BW Gr.(Mbps) ----- 0   WRR         12    12     N/A          0 1   WRR         13    13     N/A          0 2   WRR         12    12     N/A          0 3   WRR         13    13     N/A          0 4   WRR         12    12     N/A          0 5   WRR         13    13     N/A          0 6   WRR         12    12     N/A          0 7   WRR         13    13     N/A          0</pre>
<b>Related Commands</b>	N/A
<b>Notes</b>	The show command output is from a Spectrum™ based switch systems

## 5.15.6.4 RED & ECN

### traffic-class congestion-control

```
traffic-class <tc> congestion-control [red | ecn | both] [minimum- absolute
<min> maximum-absolute <max> | minimum-relative <min> maximum-relative
<max>]
no traffic-class <tc> congestion-control
```

Enables RED/ECN marking for traffic class queue.

The no form of the command disables RED/ECN marking for traffic class queue.

<b>Syntax Description</b>	tc	Traffic class. Range: 0-7.
	red	Enables random early detection for traffic class queue
	ecn	Enables explicit congestion notification for traffic class queue
	both	Enables both RED and ECN marking for traffic class queue
	minimum-absolute	Set minimum-absolute value (in KBs) for marking traffic-class queue
	maximum-absolute	Set minimum-absolute value (in KBs) for marking traffic-class queue
	minimum-relative	Set minimum-relative value (in percentage) for marking traffic-class queue
	maximum-relative	Set maximum-relative value (in percentage) for marking traffic-class queue
<b>Default</b>	Disabled	
<b>Configuration Mode</b>	Config Interface Ethernet	
<b>History</b>	3.5.1000	
<b>Role</b>	admin	
<b>Example</b>	<pre>switch (config interfaces ethernet 1/1)# traffic-class 0 congestion- control both minimum-relative 50 maximum-relative 80</pre>	
<b>Related Commands</b>		
<b>Note</b>		

## show interfaces ethernet congestion-control

**show interfaces ethernet congestion-control**

Displays specific interface congestion control information.

<b>Syntax Description</b>	N/A
<b>Default</b>	N/A
<b>Configuration Mode</b>	Any Command Mode
<b>History</b>	3.5.1000
<b>Role</b>	admin
<b>Example</b>	<pre>switch (config)# show interfaces ethernet 1/1 congestion-control Interface ethernet: 1/1  ECN marked packets: 0 TC-0     Mode: ECN     Threshold mode: absolute     Minimum threshold: 0 KB     Maximum threshold: 200 KB     RED dropped packets: 0 TC-1     Mode: RED     Threshold mode: relative     Minimum threshold: 0%     Maximum threshold: 100%     RED dropped packets: 0 TC-2     Mode: none TC-3     Mode: none TC-4     Mode: ECN     Threshold mode: relative     Minimum threshold: 25%     Maximum threshold: 80%     RED dropped packets: 0 TC-5     Mode: none TC-6     Mode: both     Threshold mode: absolute     Minimum threshold: 100 KB     Maximum threshold: 200 KB     RED dropped packets: 0 TC-7     Mode: none  switch (config) #</pre>

---

**Related Commands**

---

**Note**

---

## bind switch-priority

**bind switch-priority [<priority\_1> [<priority\_2> .. <priority\_n>]]**  
**no bind switch-priority [<priority>]**

Configures binding of switch-priority to traffic class.

The no form of the command:

- When run in the interface configuration mode: Resets to default the binding of all switch-priorities from all traffic classes
- When run in the interface's traffic class: Negates the binding of a specific switch-priority from a specific traffic class

<b>Syntax Description</b>	N/A
<b>Default</b>	Switch priority to traffic class mapping: 0 → 0 1 → 1 2 → 2 3 → 3 4 → 4 5 → 5 6 → 6 7 → 7
<b>Configuration Mode</b>	Config Interface Ethernet Config Interface Ethernet Traffic Class Config Interface Port Channel Config Interface Port Channel Traffic Class Config Interface MLAG Port Channel Config Interface MLAG Port Channel Traffic Class
<b>History</b>	3.6.1002
<b>Role</b>	admin
<b>Example</b>	<pre>switch (config interface ethernet 1/1 traffic-class 0) # bind switch- property 1</pre>
<b>Related Commands</b>	N/A
<b>Notes</b>	<ul style="list-style-type: none"> <li>• Context is egress interface traffic class</li> <li>• This command is only supported on Spectrum™ based switch systems</li> </ul>

## bandwidth guaranteed

**bandwidth guaranteed [<rate>]**  
**no bandwidth guaranteed [<rate>]**

Configures the minimum bandwidth for outbound traffic.

<b>Syntax Description</b>	rate	Rate in GbE Range: 0 - max speed supported
<b>Default</b>	0	
<b>Configuration Mode</b>	Config Interface Ethernet Traffic Class Config Interface Port Channel Traffic Class Config Interface MLAG Port Channel Traffic Class	
<b>History</b>	3.6.1002	
<b>Role</b>	admin	
<b>Example</b>	switch (config interface ethernet 1/1 traffic-class 0) # bandwidth guaranteed 0.4G	
<b>Related Commands</b>	N/A	
<b>Notes</b>	<ul style="list-style-type: none"><li>Context is egress interface traffic class</li><li>Bandwidth guaranteed rate determines the bandwidth guaranteed by the switch for outbound traffic assigned to this traffic class on this interface</li><li>Bandwidth is in granularity of 0.2G</li><li>This command is only supported on Spectrum™ based switch systems</li></ul>	

## bandwidth shape

**bandwidth shape [<rate>]**  
**no bandwidth shape [<rate>]**

Configures the bandwidth shaper for outbound traffic.

<b>Syntax Description</b>	rate Range: 0 - max speed supported	Rate in GbE
<b>Default</b>	Maximum port rate (100GbE on Spectrum™ based switches)	
<b>Configuration Mode</b>	Config Interface Ethernet Traffic Class Config Interface Port Channel Traffic Class Config Interface MLAG Port Channel Traffic Class	
<b>History</b>	3.6.1002	
<b>Role</b>	admin	
<b>Example</b>	switch (config interface ethernet 1/1 traffic-class 7) # bandwidth shape 0.4G	
<b>Related Commands</b>	N/A	
<b>Notes</b>	<ul style="list-style-type: none"> <li>Context is egress interface traffic class and/or port</li> <li>Bandwidth shape rate determines the bandwidth of the shaper for outbound traffic assigned to this traffic class on this interface</li> <li>Bandwidth is in granularity of 0.2G</li> <li>This command is only supported on Spectrum™ based switch systems</li> </ul>	

## dcb ets

```
dcb ets [strict | wrr <weight>]  
no dcb ets [strict | wrr <weight>]
```

Configures ETS mode to strict or WRR.

<b>Syntax Description</b>	weight
<b>Default</b>	Default is WRR with the following default weights.  Traffic class to weight mapping: 0 → 12 1 → 13 2 → 12 3 → 13 4 → 12 5 → 13 6 → 12 7 → 13
<b>Configuration Mode</b>	Config Interface Ethernet Traffic Class Config Interface Port Channel Traffic Class Config Interface MLAG Port Channel Traffic Class
<b>History</b>	3.6.1002
<b>Role</b>	admin
<b>Example</b>	switch (config interface ethernet 1/1 traffic-class 1) # dcb ets wrr 50
<b>Related Commands</b>	N/A
<b>Notes</b>	<ul style="list-style-type: none"><li>• Context is egress interface traffic class</li><li>• This command is only supported on Spectrum™ based switch systems</li></ul>

## show dcb ets (Spectrum)

**show dcb ets [interface {ethernet | mlag-port-channel | port-channel} <number>]**

Displays ETS information.

<b>Syntax Description</b>	N/A
<b>Default</b>	N/A
<b>Configuration Mode</b>	Any Command Mode
<b>History</b>	3.6.1002
	3.6.5000 Updated example output
<b>Role</b>	admin
<b>Example</b>	<pre>switch (config)# show dcb ets interface ethernet 1/1 Eth1/1: Interface Bandwidth Shape [Mbps]: N/A Multicast unaware mapping: disabled  Flags:   S.Mode: Scheduling Mode [Strict/WRR]   D: -   W: Weight   Bw.Sh: Bandwidth Shaper   Bw.Gr: Bandwidth Guaranteed  ETS per TC: ----- TC  S.Mode      W     W(%)    BW Sh.(Mbps)  BW Gr.(Mbps) ----- 0   WRR         12    12      N/A          0 1   WRR         13    13      N/A          0 2   WRR         12    12      N/A          0 3   WRR         13    13      N/A          0 4   WRR         12    12      N/A          0 5   WRR         13    13      N/A          0 6   WRR         12    12      N/A          0 7   WRR         13    13      N/A          0</pre>
<b>Related Commands</b>	N/A
<b>Notes</b>	The show command output is from a Spectrum™ based switch systems

## 5.15.6.5 RED & ECN

### **traffic-class congestion-control**

```
traffic-class <tc> congestion-control [red | ecn | both] [minimum- absolute
<min> maximum-absolute <max> | minimum-relative <min> maximum-relative
<max>]
no traffic-class <tc> congestion-control
```

Enables RED/ECN marking for traffic class queue.

The no form of the command disables RED/ECN marking for traffic class queue.

<b>Syntax Description</b>	tc	Traffic class. Range: 0-7.
	red	Enables random early detection for traffic class queue
	ecn	Enables explicit congestion notification for traffic class queue
	both	Enables both RED and ECN marking for traffic class queue
	minimum-absolute	Set minimum-absolute value (in KBs) for marking traffic-class queue
	maximum-absolute	Set minimum-absolute value (in KBs) for marking traffic-class queue
	minimum-relative	Set minimum-relative value (in percentage) for marking traffic-class queue
	maximum-relative	Set maximum-relative value (in percentage) for marking traffic-class queue
<b>Default</b>	Disabled	
<b>Configuration Mode</b>	Config Interface Ethernet	
<b>History</b>	3.5.1000	
<b>Role</b>	admin	
<b>Example</b>	switch (config interfaces ethernet 1/1)# traffic-class 0 congestion-control both minimum-relative 50 maximum-relative 80	
<b>Related Commands</b>		
<b>Note</b>		

## show interfaces ethernet congestion-control

### show interfaces ethernet congestion-control

Displays specific interface congestion control information.

<b>Syntax Description</b>	N/A
<b>Default</b>	N/A
<b>Configuration Mode</b>	Any Command Mode
<b>History</b>	3.5.1000
<b>Role</b>	admin
<b>Example</b>	<pre>switch (config)# show interfaces ethernet 1/1 congestion-control Interface ethernet: 1/1  ECN marked packets: 0 TC-0     Mode: ECN     Threshold mode: absolute     Minimum threshold: 0 KB     Maximum threshold: 200 KB     RED dropped packets: 0 TC-1     Mode: RED     Threshold mode: relative     Minimum threshold: 0%     Maximum threshold: 100%     RED dropped packets: 0 TC-2     Mode: none TC-3     Mode: none TC-4     Mode: ECN     Threshold mode: relative     Minimum threshold: 25%     Maximum threshold: 80%     RED dropped packets: 0 TC-5     Mode: none TC-6     Mode: both     Threshold mode: absolute     Minimum threshold: 100 KB     Maximum threshold: 200 KB     RED dropped packets: 0 TC-7     Mode: none  switch (config) #</pre>

---

**Related Commands**

---

**Note**

---

## 5.16 Shared Buffers



This section is relevant only for Mellanox Spectrum™ based switch systems.

All successfully received packets by a switch are stored on internal memory from the time they are received until the time they are transmitted. The packet buffer is fully shared between all physical ports and is hence called a shared buffer. Buffer configuration is applied in order to provide lossless services and to ensure fairness between the ports and priorities.

The buffer mechanism allows defining reserved memory allocation and limiting the usage of memory based on incoming/outgoing ports and priority of the packet. In addition, the buffer can be divided into static pools, each for a specific set of priorities. Buffer configuration mechanism allows fair enforcement from both ingress and egress sides.

The standard configuration mode allows a simple and concise configuration manner by hiding direct buffer access from user, and collecting all the required configuration settings into “traffic pools”. Users that wish to gain full control of entire buffers set can do so by enabling advanced buffer configuration.

### 5.16.1 Traffic Pool Configuration

The set of configurations which will obtain the optimal shared buffer behavior according to user requirements can be applied by dividing priorities into “traffic pools”. A traffic pool is a logical representation of a traffic profile instance which is supposed to handle all buffer related allocation on the ingress and egress sides to allow fluent flow of the traffic.

Available traffic pool types are as follows:

- Lossy – for standard lossy traffic. This is the default type for all traffic.
- Lossless – for traffic which cannot suffer any loss. Using this type enables a flow control mechanism for the mapped priority as well as setting headroom and Xon/Xoff parameters for the relevant ingress PG buffer.
- Lossy-MC – for layer 2 multicast traffic which requires special care due to stream duplication on the egress side over several ports.

There is no restriction for priority mapping to traffic pools. User can map all priorities to a single traffic pool or create a separate traffic pool for each priority. By default, all memory will be equally divided between all active traffic pools. User can set a memory percentage for a traffic pool out of the entire shared buffer. A state of over-subscription (where sum of percentage is bigger than 100%) is admissible although not advised.

A traffic pool will become functional if at least one priority is mapped to it. Each functional traffic pool will be matched by an iPool, ePool and iPort.PG buffer on each interface. For further detail see Section 5.16.3, “Advanced Buffer Configuration,” on page 976.

## 5.16.2 Lossless Traffic

In order to allow lossless traffic flow, the relevant switch-priority (see Packet Classification) needs to be mapped to the traffic pool type “Lossless”. This could be done in one of the following ways:

- Creating a new custom lossless traffic pool, and mapping a switch-priority to it. In this case PFC configuration takes place automatically.
- Enabling DCB PFC over the said switch-priority along with enabling DCB PFC globally. This will result in mapping of the priority to the lossless-default traffic pool which is reserved merely for this purpose. In addition it is required to enable DCB PFC for the relevant interfaces as well.

When setting lossless traffic configuration, it is strongly recommended to stick with one of the upper modes rather than a combination of them.

## 5.16.3 Advanced Buffer Configuration

### 5.16.3.1 Packet Buffering Classification

When a packet arrives to the switch it is classified according to its ingress port, egress port, and layer 2 and layer 3 header fields. The following terms are used to handle packet classification within the switch:

- Port
  - Ingress port (iPort) – the port which the packet is received on
  - Egress port (ePort) – the port which the packet is transmitted on
- Pool
  - Ingress pool (iPool) – the memory pool on which the packet is counted on the ingress side
  - Egress pool (ePool) – the memory pool on which the packet is counted on the egress side
- Priority
  - Switch priority (SP) – internal identifier of the packet priority which is used as a key for several internal switch functions and decisions, including buffering. The SP of the packet is assigned according to a port’s trust level configuration and packet QoS identifiers in the header (PCP, DEI, DSCP).
  - Priority group (PG) – PG is combined of a group of SPs. It is used for grouping packets of several switch priorities into a single ingress buffer space. PG range is from 0-7, while PG 9 is reserved for control traffic.
  - Traffic class (TC) – TC is combined of a group of SPs. It is used for grouping packets of several switch priorities into a single egress queue and buffer space. TC range is from 0-15, while TC 8-15 is reserved for multicast traffic and TC 16 is reserved for control traffic.

Buffer configuration mechanism provides a way to allocate buffer space for specific traffic types by configuring buffers of the following types.

- iPort.PG – traffic which arrives on a specific port and is mapped to a specific PG
- iPort (iPort.pool) – traffic which arrives on a specific port and is counted on a specific iPool. This sums all iPort.PG mapped to the said iPool.

- ePort.TC – traffic which is transmitted on a specific port and mapped to a specific TC
- ePort (ePort.pool) – traffic which is transmitted on a specific port and counted on a specific ePool. It should sum up all ePort.TCs mapped to the said ePool.

Since multicast packets are duplicated among egress ports, to allow consistent packet counting on ingress and egress sides, the following buffers types are used:

- MC.SP – multicast traffic which is classified per specific switch-priority. Counting occurs on egress side prior to packet duplication.
- ePort.mc – multicast traffic which is going to be transmitted on a specific port

### 5.16.3.2 Buffer Allocation

For the aforementioned classification parameters, a buffering region can be allocated. The buffering region is defined as a set of one of the following: {iPort}, {iPort.pg}, {ePort}, {ePort.TC}, {MC} or {MC.SP}.

For buffer regions, reserved and shared buffering quotas are allocated based on the following configuration parameters:

- Reserved allocation (size) – guaranteed buffering quota for the region which is not shared with other regions
- Shared allocation (shared) – best-effort buffering quota for the region which can be shared with other regions and allocated dynamically. Region usage cannot overflow this quota. Shared allocation can be set using static or dynamic threshold.
- Shared pool – static bound from which the shared space is dynamically allocated

The iPort.PG buffer can be configured to work in one of two modes:

- Lossy – for lossy traffic
- Lossless – for lossless traffic. In this mode, the user must define the flow control thresholds (Xoff, Xon). Reaching Xoff threshold in a PG buffer occupancy will generate “pause” frames to the sender. Reaching Xon threshold ceases “pause” frames transmission. The reserved allocation for this buffer should be at least the value of Xoff to allow sufficient ingress packet buffering for applying Xon/Xoff thresholds.

After initial admittance to headroom buffer—in which its egress port, TC, and ingress PG are defined—a packet is evaluated for eligibility for being stored in the buffer space until it is forwarded. Buffer eligibility is defined based on the following conditions:

1. If current usage is below allocation thresholds for all four shared:
  - iPort.PG && iPort && ePort.TC && ePort
2. If there is available quota within at least one of the four reserved allocation regions:
  - For lossy traffic: iPort.PG || iPort || ePort.TC || ePort
  - For lossless traffic: ePort.TC || ePort. Ingress check is not performed since all the ingress reserved space is allocated for headroom.

If a packet is not eligible for buffering:

- For lossy traffic: Packet is dropped
- For lossless traffic: Packet stays in headroom on which Xon/Xoff thresholds are applied

### 5.16.3.3 Pools

Shared buffer space can be statically divided among multiple pools on the ingress side (iPools) and the egress side (ePools). Each buffer is a region that is mapped to a specific pool.

Each pool has the following parameters:

- Size – the total size which is shared among the regions allocated to that pool. The pool's size binds the amount of cumulative shared usage of the regions that are mapped to the pool. The size can be set to infinite value, in which case occupancy of this pool will not be taken into consideration upon admittance of the packet.



Note: The pool size does not include the reserved sizes of regions.

- Mode – working mode
  - Static – each region has a static maximum threshold defined in bytes. The user sets the maximum shared quota for this buffer from a specific pool by providing a percentage out of the bounded pool size. If the size is set to infinite, shared quota for mapped buffers gets set in bytes.
  - Dynamic – each region has a dynamic maximal threshold defined as alpha ( $\alpha$ ) which is the ratio between the current region usage and the pool's free space (equal to the pool usage subtracted from pool size):
    - $\alpha$  accepts the following values 0, 1/128, 1/64, ...1/2,1,2,...,64, infinity
    - Buffer acceptance condition is:  $\text{region\_usage} < \alpha * \text{free pool space}$

The port region is counted against the pool to which the PG/TC region of the packet is mapped.

### 5.16.3.4 Usage Counting

A packet is counted once on the ingress side and on the egress side.

**Table 59 - Single Packet Usage Counting**

Direction	Traffic Type	Counting Buffers
Ingress		iPort.PG, iPort
Egress	Unicast	ePort.TC, ePort
	Multicast	MC.SP, ePort.mc

### 5.16.3.5 Control Traffic Buffering

Control packets are buffered in dedicated pools: iPoolCtrl, ePoolCtrl. Furthermore, each port has a set of buffers which are dedicated to control:

- iPort: iPort.iPoolCtrl
- iPort.PG: iPort.pg9
- ePort: ePort.ePoolCtrl

- ePort.TC: iPort.tc16

All control buffers are mapped to control pools and are not configurable.

### 5.16.3.6 Default Configuration

The default, out-of-box configuration provides the following settings:

Pools:

- iPool0, ePool0 – default pools for all data traffic. Set to dynamic mode with size of the entire shared buffer each.
- iPoolCtrl, ePoolCtrl – dynamic pools dedicated for control with size of 256KB each
- ePool15 – multicast pool with static mode and infinite size

Buffers:

- All buffer configuration (apart from MC.SP) is similar for all ports
- All switch-priorities are mapped to PG0
- Each switch-priority is mapped to a corresponding TC buffer (i-to-i)

Buffer	Reserved	Shared [%/a/Byte]	Pool	Comment
iPort.iPool0	10KB	alpha 8	iPool0 (fixed)	
iPort.iPoolCtrl	0	alpha 8	iPoolCtrl	iPort control buffer
iPort.pg0	0 (20KB headroom)	alpha 8	iPool0	
iPort.pg9	10KB	alpha 8	iPoolCtrl	iPort.pg control buffer
ePort.ePool0	10KB	alpha 8	ePool0 (fixed)	
ePort.ePoolCtrl	0	alpha 8	ePoolCtrl	ePort control buffer
ePort.mc	10KB	90KB	ePool15 (fixed)	Multicast
ePort.tc0-7	1KB	alpha 8	ePool0	
ePort.tc16	1KB	alpha 8	ePoolCtrl	ePort.tc control buffer
MC.SP0-7	0	alpha ¼	ePool0	Global multicast

### 5.16.3.7 Configuration Example

The following example exhibits how to divide the buffer among traffic priorities in advanced buffer management mode. Assuming that over an out-of-box lossy default configuration is set, the user here configures buffering for lossless traffic classified to switch-priority 1, over Ethernet interfaces 1/1 and 1/5.

The changes on the default configuration are as follows:

- Advanced buffer management is enabled
- Ingress:
  - iPool1 is assigned a size of 13MB
  - Switch-priority is bound to PG1 to allow separate configuration settings

- PG1 is mapped to selected pool iPool1, classified as lossless and set sufficient headroom (reserved size) of 85KB. Xon/Xoff thresholds are set to 20KB. The shared alpha coefficient is set to 1.
- iPort.pool1 buffer receives reserved size of 10k and shared coefficient of alpha 1.
- Egress:
  - ePool1 is assigned an infinite size according to recommended lossless traffic settings
  - TC1 (to which switch-priority is mapped by default) is mapped to the selected pool ePool1, and receives reserved size 0 and an infinite shared threshold
  - ePort.mc buffer receives reserved size 0 and an infinite shared threshold
  - ePort.pool1 buffer receives reserved size 0 and an infinite shared threshold
  - MC.SP1 buffer is mapped to egress pool ePool1, and gets reserved size 0 and an infinite shared threshold
- Finally, priority-flow-control is enabled over switch-priority 1, and over the selected ports.

**Example:**

```
switch (config) # advanced buffer management force
# Pool configuration
switch (config) # pool iPool1 size 13680063 type dynamic
switch (config) # pool ePool1 size inf type static
# Ingress buffer configuration
switch (config) # interface ethernet 1/1 ingress-buffer iPort
  pool iPool1 reserved 10k shared alpha 1
switch (config) # interface ethernet 1/1 ingress-buffer iPort.pgl
  bind switch-priority 1
switch (config) # interface ethernet 1/1 ingress-buffer iPort.pgl
  map pool iPool1 type lossless reserved 85k xoff 20k xon 20k shared alpha 1
switch (config) # interface ethernet 1/1 egress-buffer ePort
  pool ePool1 reserved 0 shared size inf
switch (config) # interface ethernet 1/1 egress-buffer ePort.tc1
  map pool ePool1 reserved 0 shared size inf
switch (config) # interface ethernet 1/1 egress-buffer ePort.mc
  reserved 0 shared size inf
# Egress buffer configuration
switch (config) # interface ethernet 1/5 ingress-buffer iPort
  pool iPool1 reserved 10k shared alpha 1
switch (config) # interface ethernet 1/5 ingress-buffer iPort.pgl
  bind switch-priority 1
switch (config) # interface ethernet 1/5 ingress-buffer iPort.pgl
  map pool iPool1 type lossless reserved 85k xoff 20k xon 20k shared alpha 1
switch (config) # interface ethernet 1/5 egress-buffer ePort pool
  ePool1 reserved 0 shared size inf
switch (config) # interface ethernet 1/5 egress-buffer ePort.tc1
  map pool ePool1 reserved 0 shared size inf
switch (config) # interface ethernet 1/5 egress-buffer ePort.mc
  reserved 0 shared size inf
# MC buffer configuration
switch (config) # pool ePool1 mc-buffer mc.spl reserved 0 shared size inf
# PFC configuration
switch (config) # dcb priority-flow-control enable force
switch (config) # dcb priority-flow-control priority 1 enable
switch (config) # interface ethernet 1/1 dcb priority-flow-control mode on
switch (config) # interface ethernet 1/5 dcb priority-flow-control mode on
```

## 5.16.4 Commands

### traffic pool

```
traffic pool <name> [force]
no traffic pool <name> [force]
```

Creates a traffic pool and enters the traffic pool context on prefix mode enabled.  
The no form of the command deletes a traffic pool.

<b>Syntax Description</b>	name	String up to 20 characters
	force	Enforces configuration
<b>Default</b>	N/A	
<b>Configuration Mode</b>	Config	
<b>History</b>	3.6.5000	
<b>Role</b>	admin	
<b>Example</b>	<pre>switch (config)# traffic pool name switch (config pool name)#+</pre>	
<b>Related Commands</b>		
<b>Note</b>		

## type

```
type <type>
no type <type>
```

Configures the traffic pool type.  
The no form of the command resets a traffic pool.

<b>Syntax Description</b>	type	<ul style="list-style-type: none"><li>• lossless</li><li>• lossy</li><li>• lossy-mc</li></ul>
<b>Default</b>	Lossy	
<b>Configuration Mode</b>	Config Pool	
<b>History</b>	3.6.5000	
<b>Role</b>	admin	
<b>Example</b>	switch (config pool name)# type lossless	
<b>Related Commands</b>		
<b>Note</b>	When using “traffic pool <name> type <type>”, if the traffic pool does not exist then it is created.	

## map switch-priority

```
map switch-priority <priority>
no map switch-priority
```

Maps switch-priorities to the traffic pool.  
The no form of the command unmaps switch-priorities.

Syntax Description	priority	Range: 0-7
<b>Default</b>	N/A	
<b>Configuration Mode</b>	Config Pool	
<b>History</b>	3.6.5000	
<b>Role</b>	admin	
<b>Example</b>	switch (config pool name)# map switch-priority 2 3 1 7	
<b>Related Commands</b>		
<b>Note</b>	When using “traffic pool <name> map switch-priority <priority>”, if the traffic pool does not exist then it is created.	

## type map switch-priority

```
type {lossless | lossy | lossy-mc} map switch-priority <priority>
no type {lossless | lossy | lossy-mc} map switch-priority
```

Configures type of traffic pool and maps switch-priorities to it.  
The no form of the command unmaps switch-priorities.

<b>Syntax Description</b>	type	<ul style="list-style-type: none"><li>• lossless</li><li>• lossy</li><li>• lossy-mc</li></ul>
	priority	Range: 0-7
<b>Default</b>	Type: Lossy	
<b>Configuration Mode</b>	Config Pool	
<b>History</b>	3.6.5000	
<b>Role</b>	admin	
<b>Example</b>	switch (config pool name)# type lossy-mc map switch-priority 2 3 1 7	
<b>Related Commands</b>		
<b>Note</b>	When using “traffic pool <name> type <type> map switch-priority <priority>”, if the traffic pool does not exist the it is created.	

## memory percent

```
memory percent [<percent>]  
no memory percent [<percent>]
```

Sets traffic pool size in percentage out of entire shared buffer memory.  
The no form of the command resets this parameter to its default.

<b>Syntax Description</b>	percent	Range: 0.00-100.00 or “auto”
<b>Default</b>	Auto	
<b>Configuration Mode</b>	Config Pool	
<b>History</b>	3.6.5000	
<b>Role</b>	admin	
<b>Example</b>	switch (config pool name)# memory percent 50.03	
<b>Related Commands</b>		
<b>Note</b>	<ul style="list-style-type: none"><li>Setting “auto” value ensures fair memory division between all traffic pools with “auto” size</li><li>Over-subscription of more than 100% is allowed but not recommended, and will cause display of an exception in the “Exceptions list” in “show traffic pool” command</li></ul>	

## advanced buffer management

**advanced buffer management [force]**  
**no advanced buffer management [force]**

Enable the advanced mode shared buffer configuration.

The no form of the command disables the advanced mode shared buffer configuration.

<b>Syntax Description</b>	force	Run command skipping confirmation prompt
<b>Default</b>	Disabled	
<b>Configuration Mode</b>	Config	
<b>History</b>	3.6.5000	
<b>Role</b>	admin	
<b>Example</b>	switch (config)# advanced buffer management force This will reset all configuration to default. Type 'yes' to confirm: yes	
<b>Related Commands</b>		
<b>Note</b>	When moving advanced buffer management from disable to enable or vice versa, buffer/PFC configuration returns all shared buffer configuration to default.	

## ingress-buffer

```
ingress-buffer <buffer-name>
no ingress-buffer <buffer-name>
```

Creates and enters the ingress buffer context.  
The no form of the command deletes an existing buffer.

<b>Syntax Description</b>	buffer-name	Name of ingress buffer
<b>Default</b>	N/A	
<b>Configuration Mode</b>	Config Interface Ethernet	
<b>History</b>	3.6.1002	
<b>Role</b>	admin	
<b>Example</b>	<pre>switch (config interface ethernet 1/1)# ingress-buffer iPort.pg1 switch (config interface ethernet 1/1 ingress-buffer iPort.pg1)#+</pre>	
<b>Related Commands</b>		
<b>Note</b>	iPort.pg9 is reserved for control traffic and hence cannot be edited	

## egress-buffer

```
egress-buffer <buffer-name>
no egress-buffer <buffer-name>
```

Creates and enters the buffer context.

The no form of the command deletes an existing buffer.

Syntax Description	buffer-name	Name of egress buffer
<b>Default</b>	N/A	
<b>Configuration Mode</b>	Config Interface Ethernet	
<b>History</b>	3.6.1002	
<b>Role</b>	admin	
<b>Example</b>	switch (config interface ethernet 1/1)# egress-buffer ePort.tc4 switch (config interface ethernet 1/1 egress-buffer ePort.tc4)#	
<b>Related Commands</b>		
<b>Note</b>	ePort.tc16 is reserved for control traffic and hence cannot be edited	

## reserved shared size

**reserved <value> shared size <size>**  
**no reserved <value>**

Configures the ePort.mc multicast-buffer.  
The no form of the command resets buffer to default configuration.

<b>Syntax Description</b>	buffer-name                          Name of egress buffer
	value                                Amount of reserved memory for buffer in bytes
	shared size                        Shared memory in bytes or “infinite”
<b>Default</b>	According to system default OOB configuration
<b>Configuration Mode</b>	Config Interface Ethernet Egress Buffer Config Interface Ethernet Ingress Buffer
<b>History</b>	3.6.5000
<b>Role</b>	admin
<b>Example</b>	<pre>switch (config interface ethernet 1/1 egress-buffer ePort.mc)# reserved 5k shared alpha 1/128</pre>
<b>Related Commands</b>	
<b>Note</b>	<ul style="list-style-type: none"><li>• ePort.tc16 is reserved for control traffic and hence cannot be edited</li><li>• It is possible to use “K” and “M” to define shared size</li></ul>

## pool size type

```
pool <pool-name> size <value> type {static | dynamic}  
no pool <pool-name> size <value> type {static | dynamic}
```

Creates pool.

The no form of the command deletes pool.

<b>Syntax Description</b>	pool-name	Possible values: • ePool0 ... ePool6 • iPool0 ... iPool6
	size	Size of pool in bytes, or “inf” for infinite
<b>Default</b>	According to system default OOB configuration	
<b>Configuration Mode</b>	Config	
<b>History</b>	3.6.5000	
<b>Role</b>	admin	
<b>Example</b>	<pre>switch (config)# pool iPool2 size 2M type dynamic switch (config)# pool iPool2 size static type static</pre>	
<b>Related Commands</b>		
<b>Note</b>	It is possible to use “K” for kilobytes and “M” for megabytes to define pool size.	

## pool reserved shared

```
pool <pool-name> reserved <reserved> shared <shared units> <shared>
no pool <pool-name>
```

Configures the buffer.

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

<b>Syntax Description</b>	<table border="0"> <tr> <td>pool-name</td><td>Possible values: iPool0-iPool7</td></tr> <tr> <td>reserved</td><td>Amount of reserved memory for the buffer in bytes</td></tr> <tr> <td>shared units</td><td> The amount of shared memory for this buffer  Possible values: alpha, max, size <ul style="list-style-type: none"> <li>• In alpha mode, alpha can have the following values: 0, 1/128, 1/64 ... 1, 2, 4, ... 64, inf</li> <li>• In max mode, the shared size is defined as a percentage of the pool size</li> <li>• In size mode, the shared size is defined in bytes or infinite</li> </ul> </td></tr> </table>	pool-name	Possible values: iPool0-iPool7	reserved	Amount of reserved memory for the buffer in bytes	shared units	The amount of shared memory for this buffer Possible values: alpha, max, size <ul style="list-style-type: none"> <li>• In alpha mode, alpha can have the following values: 0, 1/128, 1/64 ... 1, 2, 4, ... 64, inf</li> <li>• In max mode, the shared size is defined as a percentage of the pool size</li> <li>• In size mode, the shared size is defined in bytes or infinite</li> </ul>
pool-name	Possible values: iPool0-iPool7						
reserved	Amount of reserved memory for the buffer in bytes						
shared units	The amount of shared memory for this buffer Possible values: alpha, max, size <ul style="list-style-type: none"> <li>• In alpha mode, alpha can have the following values: 0, 1/128, 1/64 ... 1, 2, 4, ... 64, inf</li> <li>• In max mode, the shared size is defined as a percentage of the pool size</li> <li>• In size mode, the shared size is defined in bytes or infinite</li> </ul>						
<b>Default</b>	According to system default OOB configuration						
<b>Configuration Mode</b>	Config Interface Ethernet Egress Buffer Config Interface Ethernet Ingress Buffer						
<b>History</b>	3.6.1002						
<b>Role</b>	admin						
<b>Example</b>	<pre>switch (config interface ethernet 1/1 ingress-buffer iPort)# pool iPool0 reserved 90K shared alpha 1/8</pre>						
<b>Related Commands</b>							
<b>Note</b>							

## map pool type reserved

```
map [pool <pool name> type <type> [xoff <xoff-value> xon <xon value>] reserved <reserved size> shared <shared units> <shared size>]
```

Maps iPort.pg buffer to a given pool and sets its reserved and shared sizes.  
The no form of the command resets buffer to default pool mapping and configuration.

<b>Syntax Description</b>	pool-name	Possible values: iPool0 ... iPool7
	type	Possible values: lossy, lossless
	reserved size	Amount of reserved memory for the buffer in bytes
	shared units	Possible values: size, alpha, max
	shared size	<p>The amount of shared memory for this buffer</p> <ul style="list-style-type: none"> <li>• In alpha mode, alpha can have the following values: 0, 1/128, 1/64 ... 1, 2, 4, ... 64, inf</li> <li>• In max mode, the shared size is defined as a percentage of the pool size</li> <li>• In size mode, the shared size is defined in bytes or infinite</li> </ul> <p>Shared size depends on type and size of the given pool:</p> <ul style="list-style-type: none"> <li>• For static pool shared size is in packets</li> <li>• For dynamic pool shared size is in alpha units</li> <li>• For static pool with infinite size only alpha infinite is supported</li> </ul>
	xoff	Relevant only on lossless type, Xoff threshold in bytes
	xon	Relevant only on lossless type, Xon threshold in bytes
<b>Default</b>	According to system default OOB configuration	
<b>Configuration Mode</b>	Config Interface Ethernet Ingress Buffer	
<b>History</b>	3.6.1002	
	3.6.5000	Updated command syntax
<b>Role</b>	admin	
<b>Example</b>	<pre>switch (config interface ethernet 1/9 ingress-buffer iPort.pg5)# map pool iPool6 type lossy reserved 3k shared alpha 2 switch (config interface ethernet 1/9 ingress-buffer iPort.pg5)# map pool iPool4 type lossless reserved 7k xoff 2k xon 1k shared max 20</pre>	
<b>Related Commands</b>		
<b>Note</b>	<ul style="list-style-type: none"> <li>• Xon and Xoff values are in KB and valid only for “lossless” type</li> <li>• It is possible to use “K” and “M” quantifiers to set reserved size</li> </ul>	

## bind switch-priority

**bind switch-priority <list-of-switch-priorities>**

Bind a switch priority (SP) to an ingress buffer.

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

<b>Syntax Description</b>	list-of-switch-priorities	Possible values: 0-7		
<b>Default</b>	According to system default OOB configuration			
<b>Configuration Mode</b>	Config Interface Ethernet Ingress Buffer			
<b>History</b>	3.6.1002			
<b>Role</b>	admin			
<b>Example</b>	switch (config interface ethernet 1/1 ingress-buffer iPort.pg1)# bind switch-priority 0 1			
<b>Related Commands</b>				
<b>Note</b>				

## description

### description <description>

Configures buffer description.

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

<b>Syntax Description</b>	description	Text string
<b>Default</b>	""	
<b>Configuration Mode</b>	Config Interface Ethernet Egress Buffer Config Interface Ethernet Ingress Buffer	
<b>History</b>	3.6.1002	
<b>Role</b>	admin	
<b>Example</b>	switch (config interface ethernet 1/1 ingress-buffer iPort.pg1)# description example	
<b>Related Commands</b>		
<b>Note</b>		

## pool mc-buffer

```
pool <pool-name> mc-buffer <buffer> reserved <reserved> shared <shared
units> <shared-size>
no pool <pool-name> mc-buffer
```

Maps MC-buffer to specified egress pool and sets its reserved and shared sizes.  
The no form of the command resets the values to their default.

<b>Syntax Description</b>	mc-buffer reserved shared	Buffer can have the values mc.sp0, mc.sp1...mc.sp7 The amount of shared memory for this buffer The amount of shared memory for this buffer <ul style="list-style-type: none"><li>• In alpha mode, alpha can have the following values: 0, 1/128, 1/64 ... 1, 2, 4, ... 64, inf</li><li>• In max mode, the shared size is defined as a percentage of the pool size</li><li>• In size mode, the shared size is defined in bytes or infinite</li></ul>
<b>Default</b>	N/A	
<b>Configuration Mode</b>	Config Config Interface Ethernet Egress Buffer	
<b>History</b>	3.6.1002 3.6.5000	Added “size” parameter and note
<b>Role</b>	admin	
<b>Example</b>	switch (config)# pool ePool4 mc-buffer mc.sp6 reserved 3k shared size 2K	
<b>Related Commands</b>		
<b>Note</b>	<ul style="list-style-type: none"> <li>• The qualifiers “K” and “M” may be used to set reserved and shared size</li> <li>• The units alpha, max, size is presented to the user according to the pool type “static”, “dynamic” and “size”: <ul style="list-style-type: none"> <li>• Alpha when pool type is dynamic and size is defined in bytes</li> <li>• Max when pool type is static and size is defined in bytes</li> <li>• Size when pool type is static and size is infinite</li> </ul> </li> </ul>	

## pool description

```
pool <pool-name> description <description>
no pool <pool-name> description
```

Configures the buffer description of a specific pool-name.  
The no form of the command resets the values to their default.

<b>Syntax Description</b>	pool-name	Possible values: <ul style="list-style-type: none"><li>• ePool0 ... ePool7</li><li>• iPool0 ... iPool7</li></ul>
	description	String text (20 character max)
<b>Default</b>	""	
<b>Configuration Mode</b>	Config	
<b>History</b>	3.6.1002	
	3.6.5000	
<b>Role</b>	admin	
<b>Example</b>	switch (config)# pool iPool6 description mapped-to-pg3	
<b>Related Commands</b>		
<b>Note</b>		

## cable-length

**cable-length [<meters>]**

Configures the cable length in meters for the given port.

<b>Syntax Description</b>	meters	Cable length in meters Range: 5-100,000
<b>Default</b>	N/A	
<b>Configuration Mode</b>	Config Interface Ethernet	
<b>History</b>	3.6.5000	
<b>Role</b>	admin	
<b>Example</b>	switch (config interface ethernet 1/4)# cable-length 10	
<b>Related Commands</b>		
<b>Note</b>	<ul style="list-style-type: none"><li>The user may use the quantifier “K” to indicate kilometers (e.g. “cable-length 5K”)</li><li>This command is used to calculate the required buffer to sustain the delay caused by the cable length</li></ul>	

## show buffers mode

### show buffers mode

Displays current mode for shared buffers.

<b>Syntax Description</b>	N/A
<b>Default</b>	N/A
<b>Configuration Mode</b>	Any Command Mode
<b>History</b>	3.6.5000
<b>Role</b>	admin
<b>Example</b>	<pre>switch (config)# show buffers mode Current mode: user mode</pre>
<b>Related Commands</b>	
<b>Note</b>	

## show buffers status

**show buffers status [interfaces ethernet <slot>/<port>]**

Displays buffer usage status.

<b>Syntax Description</b>	<slot>/<port>	Ethernet interface
<b>Default</b>	N/A	
<b>Configuration Mode</b>	Any Command Mode	
<b>History</b>	3.6.1002	
	3.6.5000	Updated example output
<b>Role</b>	admin	

**Example**

```
switch (config)# show buffers status interfaces ethernet 1/9
```

Interface	Buffer	Pool	Resv [Byte]	Shared [%/a/Byte]	Usage [Byte]	MaxUsage [Byte]
Eth1/9	iPort.iPool0	iPool0	10.0K	alpha 8	0	0
	iPort.iPool1	iPool1	0	alpha 0	0	0
	iPort.iPool2	iPool2	0	alpha 0	0	0
	iPort.iPool3	iPool3	0	alpha 0	0	0
	iPort.iPool4	iPool4	0	alpha 0	0	0
	iPort.iPool5	iPool5	0	alpha 0	0	0
	iPort.iPool6	iPool6	0	alpha 0	0	0
	iPort.iPool7	iPool7	0	alpha 0	0	0
	iPort.iPoolCtrl	iPoolCtrl	0	alpha 8	0	0
	iPort.pg0	iPool0	0	alpha 8	0	0
	iPort.pg1	iPool0	0	alpha 8	0	0
	iPort.pg2	iPool0	0	alpha 8	0	0
	iPort.pg3	iPool0	0	alpha 8	0	0
	iPort.pg4	iPool0	0	alpha 8	0	0
	iPort.pg5	iPool0	0	alpha 8	0	0
	iPort.pg6	iPool0	0	alpha 8	0	0
	iPort.pg7	iPool0	0	alpha 8	0	0
	iPort.pg9	iPoolCtrl	10.0K	alpha 8	0	0
	ePort.ePool0	ePool0	5.0K	alpha 8	0	0
	ePort.ePool1	ePool1	0	alpha 0	0	0
	ePort.ePool2	ePool2	0	alpha 0	0	0
	ePort.ePool3	ePool3	0	alpha 0	0	0
	ePort.ePool4	ePool4	0	alpha 0	0	0
	ePort.ePool5	ePool5	0	alpha 0	0	0
	ePort.ePool6	ePool6	0	alpha 0	0	0
	ePort.ePool7	ePool7	0	alpha 0	0	0
	ePort.mc	ePool15	5.0K	90.0K	0	0
	ePort.ePoolCtrl	ePoolCtrl	0	alpha 8	0	0
	ePort.tc0	ePool0	1.0K	alpha 8	0	0
	ePort.tc1	ePool0	1.0K	alpha 8	0	0
	ePort.tc2	ePool0	1.0K	alpha 8	0	0
	ePort.tc3	ePool0	1.0K	alpha 8	0	0
	ePort.tc4	ePool0	1.0K	alpha 8	0	0
	ePort.tc5	ePool0	1.0K	alpha 8	0	0
	ePort.tc6	ePool0	1.0K	alpha 8	0	0
	ePort.tc7	ePool0	1.0K	alpha 8	0	0

**Related Commands**
**Note**

## show buffers details

**show buffers details [interface ethernet <id>]**

Displays buffer status in details.

<b>Syntax Description</b>	<slot>/<port>	Ethernet interface
<b>Default</b>	N/A	
<b>Configuration Mode</b>	Any Command Mode	
<b>History</b>	3.6.1002	
	3.6.5000	Updated example output
<b>Role</b>	admin	

**Example**

```
switch (config)# show buffers details interfaces ethernet 1/9
Flags: Y - Lossy, L - Lossless
      S - Static, D - Dynamic
Shared size is in percent/Bytes for static pool and in alphas for dynamic
pool.
```

Interface: Eth1/9

Buffer	Resv [Byte]	Xoff [Byte]	Xon [Byte]	Shared [%/a/Byte]	Pool	Description
iPort.iPool0(Y)	10.0K	-	-	alpha 8	iPool0(D)	
iPort.iPool1(Y)	0	-	-	alpha 0	iPool1(D)	
iPort.iPool2(Y)	0	-	-	alpha 0	iPool2(D)	
iPort.iPool3(Y)	0	-	-	alpha 0	iPool3(D)	
iPort.iPool4(Y)	0	-	-	alpha 0	iPool4(D)	
iPort.iPool5(Y)	0	-	-	alpha 0	iPool5(D)	
iPort.iPool6(Y)	0	-	-	alpha 0	iPool6(D)	
iPort.iPool7(Y)	0	-	-	alpha 0	iPool7(D)	
iPort.iPoolCtrl(Y)	0	-	-	alpha 8	iPoolCtrl(D)	
iPort.pg0(Y)	0	-	-	alpha 8	iPool0(D)	
iPort.pg1(Y)	0	-	-	alpha 8	iPool0(D)	
iPort.pg2(Y)	0	-	-	alpha 8	iPool0(D)	
iPort.pg3(Y)	0	-	-	alpha 8	iPool0(D)	
iPort.pg4(Y)	0	-	-	alpha 8	iPool0(D)	
iPort.pg5(Y)	0	-	-	alpha 8	iPool0(D)	
iPort.pg6(Y)	0	-	-	alpha 8	iPool0(D)	
iPort.pg7(Y)	0	-	-	alpha 8	iPool0(D)	
iPort.pg9(Y)	10.0K	-	-	alpha 8	iPoolCtrl(D)	
ePort.ePool0	5.0K	-	-	alpha 8	ePool0(D)	
ePort.ePool1	0	-	-	alpha 0	ePool1(D)	
ePort.ePool2	0	-	-	alpha 0	ePool2(D)	
ePort.ePool3	0	-	-	alpha 0	ePool3(D)	
ePort.ePool4	0	-	-	alpha 0	ePool4(D)	
ePort.ePool5	0	-	-	alpha 0	ePool5(D)	
ePort.ePool6	0	-	-	alpha 0	ePool6(D)	
ePort.ePool7	0	-	-	alpha 0	ePool7(D)	
ePort.mmc	5.0K	-	-	90.0K	ePool15(S)	
ePort.ePoolCtrl	0	-	-	alpha 8	ePoolCtrl(D)	
ePort.tc0	1.0K	-	-	alpha 8	ePool0(D)	
ePort.tc1	1.0K	-	-	alpha 8	ePool0(D)	
ePort.tc2	1.0K	-	-	alpha 8	ePool0(D)	
ePort.tc3	1.0K	-	-	alpha 8	ePool0(D)	
ePort.tc4	1.0K	-	-	alpha 8	ePool0(D)	
ePort.tc5	1.0K	-	-	alpha 8	ePool0(D)	
ePort.tc6	1.0K	-	-	alpha 8	ePool0(D)	
ePort.tc7	1.0K	-	-	alpha 8	ePool0(D)	

switch-priority to Buffers mapping:

Switch-priority	Buffer
0	iPort.pgo
1	iPort.pgo
2	iPort.pgo
3	iPort.pgo
4	iPort.pgo
5	iPort.pgo
6	iPort.pgo
7	iPort.pgo

---

**Related Commands**

---

**Note**

---

## show buffers pools

**show buffers pools [pool-name]**

Displays buffer pool statistics.

<b>Syntax Description</b>	pool-name	• iPool0-iPool7 • ePool0-ePool7
<b>Default</b>	N/A	
<b>Configuration Mode</b>	Any Command Mode	
<b>History</b>	3.6.1002	
	3.6.5000	Updated example output
<b>Role</b>	admin	
<b>Example</b>	<pre>switch (config)# show buffers pools Flags: S - Static, D - Dynamic  ----- Pool      Direction    Size      Usage     MaxUsage   Description           [Byte]       [Byte]     [Byte] ----- iPool0    ingress(D)  13.2M    0         576        Lossy-default iPool1    ingress(D)  0         0         0 iPool2    ingress(D)  0         0         0 iPool3    ingress(D)  0         0         0 iPool4    ingress(D)  0         0         0 iPool5    ingress(D)  0         0         0 iPool6    ingress(D)  0         0         0 iPool7    ingress(D)  0         0         0 iPoolCtrl ingress(D)  256.0K   0         0          Control ePool0    egress(D)   13.2M    0         0          Default ePool1    egress(D)   0         0         0 ePool2    egress(D)   0         0         0 ePool3    egress(D)   10.0K    0         0 ePool4    egress(D)   0         0         0 ePool5    egress(D)   0         0         0 ePool6    egress(D)   0         0         0 ePool7    egress(D)   0         0         0 ePool15   egress(S)   inf      0         0          Multicast ePoolCtrl egress(D)  256.0K   0         0          Control</pre>	
<b>Related Commands</b>		
<b>Note</b>	When advanced buffer management is disabled, the “Description” field specifies the e/iPool’s relevant traffic pool name.	

## show buffers pools mc-buffers

**show buffers pools [<pool-name>] mc-buffers**

Displays global multicast buffers usage status.

<b>Syntax Description</b>	pool-name	Possible values: ePool0 ... ePool7
<b>Default</b>	N/A	
<b>Configuration Mode</b>	Any Command Mode	
<b>History</b>	3.6.5000	
<b>Role</b>	admin	
<b>Example</b>	<pre>switch (config)# show buffers pools ePool0 mc-buffers ----- MC-Buffer      Pool      Resv      Shared      Usage      MaxUsage               [Byte]    [%/a/Byte]  [Byte]    [Byte] ----- mc.sp0        ePool0     0         alpha 1/4   0          0 mc.sp1        ePool0     0         alpha 1/4   0          0 mc.sp2        ePool0     0         alpha 1/4   0          0 mc.sp3        ePool0     0         alpha 1/4   0          0 mc.sp4        ePool0     0         alpha 1/4   0          0 mc.sp5        ePool0     0         alpha 1/4   0          0 mc.sp6        ePool0     0         alpha 1/4   0          0 mc.sp7        ePool0     0         alpha 1/4   0          0</pre>	

### Related Commands

### Note

## show traffic pool

**show traffic pool [<name>]**

Displays state and configuration information for a given traffic pool.

**Syntax Description** N/A

**Default** N/A

**Configuration Mode** Any Command Mode

**History** 3.6.5000

**Role** admin

**Example**

```
switch (config)# show traffic pool
```

Traffic Pool	Type	Memory [%]	Switch Priorities	Memory actual [Bytes]	Usage [KB]	Max Usage [Bytes]
lossless-default (RO)	lossless	auto		0	0	0
lossy-default	lossy	auto	0, 1, 2, 3, 4, 5, 6, 7	13.7M	0	0

Exception list:

N/A

### Related Commands

**Note**

- Omission of traffic pool name displays information about all existing traffic pools
- The “Exception list” section displays messages to indicate any unrecommended configuration

## show traffic pool interface ethernet

**show traffic pool <name> interface ethernet <device/port>**

Displays state and configuration information for the buffers on a given port related to a given traffic pool.

<b>Syntax Description</b>	<device/port>	Ethernet interface
<b>Default</b>	N/A	
<b>Configuration Mode</b>	Any Command Mode	
<b>History</b>	3.6.5000	
<b>Role</b>	admin	
<b>Example</b>	<pre>switch (config)# show traffic pool lossy-default interface ethernet 1/1  ----- Switch-priority    Ingress buffer    Egress buffer ----- 0                  iPort.pgo          ePort.tc0 1                  iPort.pgo          ePort.tc1 2                  iPort.pgo          ePort.tc2 3                  iPort.pgo          ePort.tc3 4                  iPort.pgo          ePort.tc4 5                  iPort.pgo          ePort.tc5 6                  iPort.pgo          ePort.tc6 7                  iPort.pgo          ePort.tc7  ----- Name              Memory percent    Size (bytes)    Usage (bytes) ----- lossy-default      auto            13.7M          0  ----- Ingress buffer    Headroom size (bytes)  Xon (bytes)   Xoff (bytes) ----- iPort.pgo          N/A             N/A           N/A  ----- Direction         Pool Usage (bytes)  Pool Max Usage (bytes) ----- Ingress           0               0 Egress            0               0  Exception list: N/A</pre>	

### Related Commands

### Note

## 5.17 Storm Control



This section is relevant only for Spectrum™ systems.

Storm Control is a feature which can be enabled on L2 Ethernet ports and LAGs to monitor inbound traffic to prevent disruptions caused by a broadcast, multicast, or unicast traffic storm on the physical interfaces.

Storm Control utilizes a bandwidth-based method to measure traffic where packets exceeding the percentage level specified by the user are dropped.

Users are able to monitor broadcast, unknown unicast, and unregistered multicast traffic while supporting differing thresholds for each type or monitor a summary of all the previously mentioned traffic with one threshold.

## 5.17.1 Commands

### storm-control level

[no] **storm-control {broadcast|unreg-multicast|unknown-unicast|all}** level <level> [force]

The command enables Storm Control on selected interface.

The no form of the command disables Storm Control on selected interface.

<b>Syntax Description</b>	{broadcast unreg-multi-cast unknown-unicast all}	<ul style="list-style-type: none"> <li>Each port can support broadcast, unregistered-multicast, unknown-unicast or all configurations</li> <li>All means one threshold level for all traffic types. It is not identical to configuring broadcast, unregistered-multicast and unknown-unicast together</li> </ul>
	<level>	Configuring packet types separately will give individual Storm Control levels per packet type.
<b>Default</b>	no storm control	
<b>Configuration Mode</b>	Config Interface Ethernet Config Interface Port Channel	
<b>History</b>	3.6.4006	
	3.6.4110	Updated command syntax, default and configuration mode
<b>Role</b>	admin	
<b>Example</b>	switch (config)# interface ethernet storm-control broadcast level 3 force	
<b>Related Commands</b>		
<b>Note</b>	<ul style="list-style-type: none"> <li>"all" and other configurations are mutually exclusive.</li> <li>User can use "force" form of command to resolve collisions and apply new configuration.</li> <li>Storm Control can be configured on LAG but cannot be configured on LAG members.</li> <li>Storm Control cannot be configured on router ports.</li> <li>Storm Control cannot be configured on a port which takes part in monitoring sessions as destination port.</li> </ul>	

## show storm-control

### show storm-control

The command displays the configuration levels and dropped packets for each traffic type.

<b>Syntax Description</b>	N/A
<b>Default</b>	N/A
<b>Configuration Mode</b>	Config
<b>History History</b>	3.6.4006 3.6.4110 Updated example output.
<b>Role</b>	admin
<b>Example</b>	<pre>switch (config)# show storm-control interface eth 1/1 Broadcast level: 10% Broadcast packets dropped: 0 Multicast level: 100% Multicast packets dropped: 0 Unicast level: 100% Unicast packets dropped: 0 All traffic types level: 100% All traffic types packets dropped: 0 ...</pre>
<b>Related Commands</b>	
<b>Note</b>	

## 5.18 Head-of-Queue Lifetime Limit

Head-of-queue (HoQ) lifetime limit (HLL) is a mechanism which allows discarding packets attempting to be transmitted after HLL time from the time that they were ready to be transmitted at the head of the scheduling group.

When HLL\_packet2Stall (7 as default) packets encounter HLL drop, the scheduling group enters a stall state. During that state all packets to the sub-group are discarded. The subgroup exits stall state after HLL\_time\*8.

A counter called HoQ discard packets counts the number of discarded packets due to HLL.

## 5.18.1 Commands

### hll

**hll <max-time>**

**no hll**

Configures HLL time on this interface.

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

<b>Syntax Description</b>	max-time	Possible values: <ul style="list-style-type: none"><li>• &lt;4   16   32   64   128   256   512&gt;ms</li><li>• &lt;1   2&gt;sec</li><li>• “inf” to disable HLL</li></ul>
<b>Default</b>	512ms	
<b>Configuration Mode</b>	Config Interface Ethernet Config Interface Port Channel Config Interface MLAG Port Channel	
<b>History</b>	3.6.5000	
<b>Role</b>	admin	
<b>Example</b>	switch (config interface ethernet 1/10)# hll 512ms	
<b>Related Commands</b>		
<b>Note</b>		

## 5.19 User Defined Keys



This feature is supported only for Mellanox Spectrum™ based switch systems.

User defined keys (UDKs) allow defining custom byte keys—that is, groups of bytes that can be matched to a predefined point in the packet (an extraction point, e.g. the start of a MAC header, or an IP header)—which is useful when wanting to make a match with a part of the packet which does not have a dedicated key.



The maximum number of UDKs is 4.

An extraction point may be defined for each packet type in a UDK. For each extraction point, an offset (from the beginning of the extraction) is defined.

To be able to modify a UDK after attaching it to an ACL rule, it is first necessary to un-match the UDK from the ACL. 2, change the match mode of the UDK to none using the command “no udk match mode”.



Defining a UDK affects the throughput for packets equal or smaller than 128 bytes.

## 5.19.1 Commands

### udk

**udk <udk-name>**  
**no udk <udk-name>**

Creates user defined key.  
The no form of the command deletes user defined key.

<b>Syntax Description</b>	udk-name	String
<b>Default</b>	N/A	
<b>Configuration Mode</b>	Config	
<b>History</b>	3.6.5000	
<b>Role</b>	admin	
<b>Example</b>	switch (config)# udk udk_name switch (config udk udk_name) #	
<b>Related Commands</b>		
<b>Note</b>	Defining UDK affects the throughput for packets equal or smaller than 128 bytes.	

## match mode

**match mode <match-mode>**  
**no match mode**

Configures user defined key match mode.  
The no form of the command resets this parameter to its default.

<b>Syntax Description</b>	match-mode	Possible values: • acl • all
<b>Default</b>	None	
<b>Configuration Mode</b>	Config UDK	
<b>History</b>	3.6.5000	
<b>Role</b>	admin	
<b>Example</b>	switch (config udk udk_name)#	match mode all
<b>Related Commands</b>	udk <udk-name>	
<b>Note</b>		

## extraction point

**extraction point mode <mode> [packet type <type> [extraction point <point> [offset <offset>]]]**

Configures user-defined key extraction point mode.

<b>Syntax Description</b>	mode	Possible values: <ul style="list-style-type: none"> <li>• 12</li> <li>• 13</li> <li>• 14</li> </ul>
	packet type	Sets user defined key packet type. Possible values: <ul style="list-style-type: none"> <li>• For L2: l2</li> <li>• For L3: arp; ipv4; ipv6</li> <li>• For L4: udp</li> </ul>
	extraction point	Sets user defined key extraction point. Possible values for: <ul style="list-style-type: none"> <li>• l2: l2-ether-type; start-of-header</li> <li>• arp: start-of-header</li> <li>• ipv4; ipv6: start-of-header; start-of-payload</li> <li>• udp: start-of-payload</li> </ul>
	offset	Sets user defined key extraction point offset Range: 0-126 (even values)
<b>Default</b>	<ul style="list-style-type: none"> <li>• Mode: l3</li> <li>• Default extraction point per packet type: <ul style="list-style-type: none"> <li>• L2: start-of-header</li> <li>• ARP; IPv4; IPv6: start-of-header</li> <li>• UDP: start-of-payload</li> </ul> </li> <li>• Offset: 0</li> </ul>	
<b>Configuration Mode</b>	Config UDK	
<b>History</b>	3.6.5000	
<b>Role</b>	admin	
<b>Example</b>	<pre>switch (config udk udk_name)# extraction point mode 13 packet type ipv4 extraction point start-of-header offset 2</pre>	
<b>Related Commands</b>	udk <udk-name>	
<b>Note</b>		

## len

**len <length>**

Configures user-defined key length.

<b>Syntax Description</b>	length	Range: 1-4
<b>Default</b>	4	
<b>Configuration Mode</b>	Config UDK	
<b>History</b>	3.6.5000	
<b>Role</b>	admin	
<b>Example</b>	switch (config udk udk_name)# len 4	
<b>Related Commands</b>	udk <udk-name>	
<b>Note</b>		

## show udk

**show udk [<udk-name>]**

Displays summary for user-defined keys.

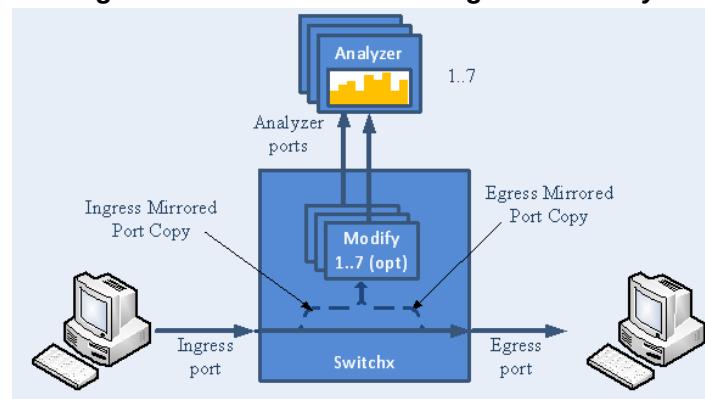
<b>Syntax Description</b>	udk-name	Displays information about specific UDK
<b>Default</b>	N/A	
<b>Configuration Mode</b>	Any Command Mode	
<b>History</b>	3.6.5000	
<b>Role</b>	admin	
<b>Example</b>	<pre>switch (config)# show udk  UDK name: udk_name Match mode: none Length: 4 Extraction mode: 13 IPv4 extraction point: start-of-header IPv4 offset: 22 IPv6 extraction point: start-of-header IPv6 offset: 0 ARP extraction point: start-of-header ARP offset: 0</pre>	
<b>Related Commands</b>	<a href="#">udk &lt;udk-name&gt;</a>	
<b>Note</b>		

## 5.20 Port Mirroring

Port mirroring enables data plane monitoring functionality which allows the user to send an entire traffic stream for testing. Port mirroring sends a copy of packets of a port's traffic stream, called "mirrored port", into an analyzer port. Port mirroring is used for network monitoring. It can be used for intrusion detection, security breaches, latency analysis, capacity and performance matters, and protocol analysis.

Figure 27 provides an overview of the mirroring functionality.

**Figure 27: Overview of Mirroring Functionality**

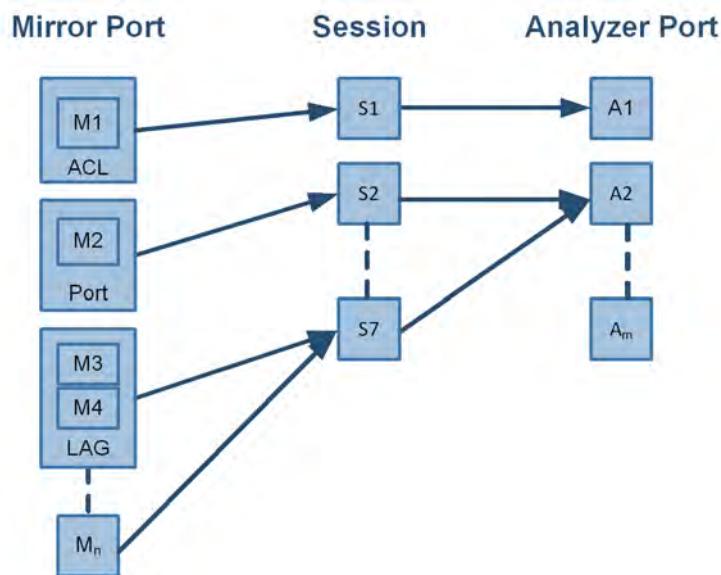


There is no limitation on the number of mirroring sources and more than a single source can be mapped to a single analyzer destination.

### 5.20.1 Mirroring Sessions

Port mirroring is performed by configuring mirroring sessions. A session is an association of a mirror port (or more) and an analyzer port.

**Figure 28: Mirror to Analyzer Mapping**



A mirroring session is a monitoring configuration mode that has the following parameters:

**Table 60 - Mirroring Parameters**

Parameter	Description	Access
Source interface(s)	List of source interfaces to be mirrored.	RW
Destination interface	A single analyzer port through which all mirrored traffic egress.	RW
Header format	The format and encapsulation of the mirrored traffic when sent to analyzer.	RW
Truncation	Enabling truncation segments each mirrored packet to 64 bytes.	RW
Congestion control	Controls the behavior of the source port when destination port is congested.	RW
Admin state	Administrative state of the monitoring session.	RW

### 5.20.1.1 Source Interface

The source interface (mirror port) refers to the interface from which the traffic is monitored. Port mirroring does not affect the switching of the original traffic. The traffic is simply duplicated and sent to the analyzer port. Traffic in any direction (either ingress, egress or both) can be mirrored.

There is no limitation on the number of the source interfaces mapped to a mirroring session.



Ingress and egress traffic flows of a specific source interface can be mapped to two different sessions.

### LAG

The source interface can be a physical interface or a LAG.

Port mirroring can be configured on a LAG interface but not on a LAG member. When a port is added to a mirrored LAG it inherits the LAG's mirror configuration. However, if port mirroring configuration is set on a port, that configuration must be removed prior to adding the port to a LAG interface.

When a port is removed from a LAG, the mirror property is switched off for that port.

### Control Protocols

All control protocols captured on the mirror port are forwarded to the analyzer port in addition to their normal treatment. For example LACP, STP, and LLDP are forwarded to the analyzer port in addition to their normal treatment by the CPU.

Exceptions to the behavior above are the packets that are being handled by the MAC layer, such as pause frames.

### 5.20.1.2 Destination Interface

The destination interface is an analyzer port to which mirrored traffic is directed. The mirrored packets are duplicated, optionally modified, and sent to the analyzer port. SwitchX® platforms support up to 7 analyzer ports, and Spectrum™ platforms support up to 2 only, where any mirror

port can be mapped to any analyzer port and more than a single mirror port can be mapped to a single analyzer port.

Packets can be forwarded to any destination using the command destination interface.

The analyzer port supports status and statistics as any other port.

## LAG

The destination interface cannot be a member of LAG when the header format is local.

## Control Protocols

The destination interface may also operate in part as a standard port, receiving and sending out non-mirrored traffic. When the header format is configured as a local port, ingress control protocol packets that are received by the local analyzer port get discarded.

## Advanced MTU Considerations

The analyzer port, like its counterparts, is subject to MTU configuration. It does not send packets longer than configured.

When the analyzer port sends encapsulated traffic, the analyzer traffic has additional headers and therefore longer frame. The MTU must be configured to support the additional length, otherwise, the packet is truncated to the configured MTU.

The system on the receiving end of the analyzer port must be set to handle the egress traffic. If it is not, it might discard it and indicate this in its statistics (packet too long).

### 5.20.1.3 Header Format

Ingress traffic from the source interface can be manipulated in several ways depending on the network layout using the command header-format.

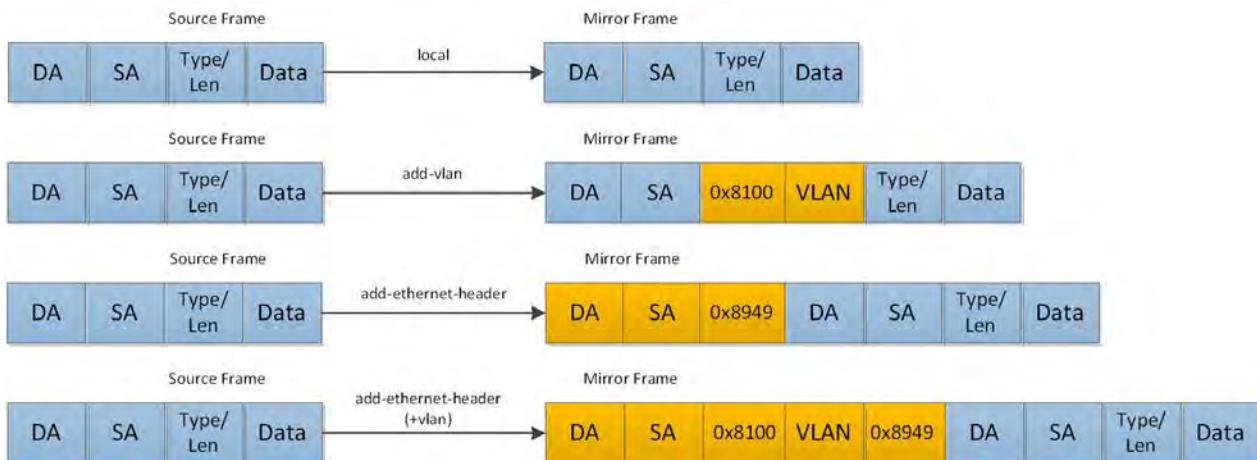
If the analyzer system is directly connected to the destination interface, then the only parameters that can be configured on the port are the MTU, speed and port based flow control. Priority flow control is not supported in this case. However, if the analyzer system is indirectly connected to the destination interface, there are two options for switching the mirrored data to the analyzer system:

- A VLAN tag may be added to the Ethernet header of the mirrored traffic
- An Ethernet header can be added with include a new destination address and VLAN tag



It must be taken into account that adding headers increases packet size.

**Figure 29: Header Format Options**



#### 5.20.1.4 Congestion Control

The destination ports might receive pause frames that lead to congestion in the switch port. In addition, too much traffic directed to the analyzer port (for example 40GbE mirror port is directed into 10GbE analyzer port) might also lead to congestion.

In case of congestion:

- When best effort mode is enabled on the analyzer port, SwitchX drops excessive traffic headed to the analyzer port using tail drop mechanism, however, the regular data (mirrored data heading to its original port) does not suffer from a delay or drops due to the analyzer port congestion.
- When the best effort mode on the analyzer port is disabled, the SwitchX does not drop the excessive traffic. This might lead to buffer exhaustion and data path packet loss.

The default behavior in congestion situations is to drop any excessive frames that may clog the system.



ETS, PFC and FC configurations do not apply to the destination port.

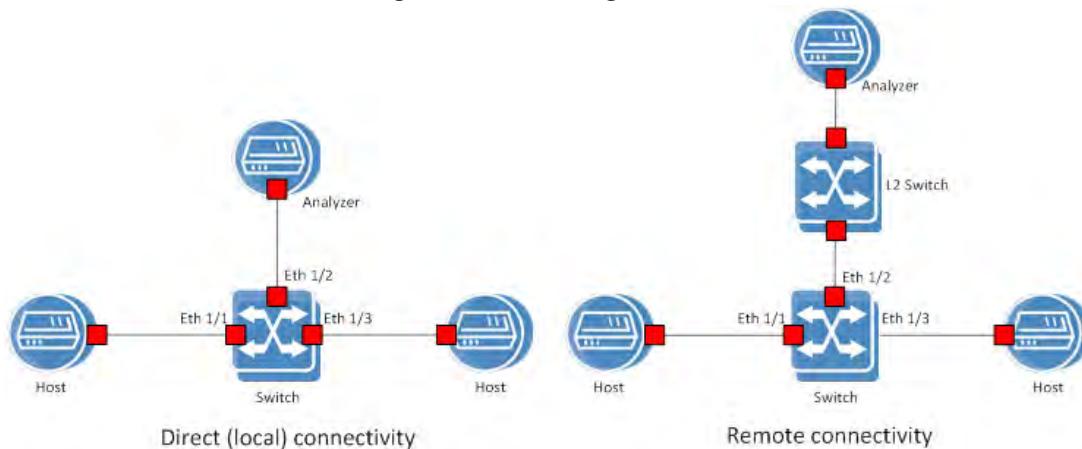
#### 5.20.1.5 Truncation

When enabled, the system can truncate the mirrored packets into smaller 64-byte packets (default) which is enough to capture the packets' L2 and L3 headers.

#### 5.20.2 Configuring Mirroring Sessions

Figure 30 presents two network scenarios with direct and remote connectivity to the analyzer equipment. Direct connectivity is when the analyzer is connected to the analyzer port of the switch. In this case there is no need for adding an L2 header to the mirrored traffic. Remote connectivity is when the analyzer is indirectly connected to the analyzer port of the switch. In this situation, adding an L2 header may be necessary depending on the network's setup.

**Figure 30: Mirroring Session**



➤ **To configure a mirroring session:**

**Step 1.** Create a session. Run:

```
switch (config) # monitor session 1
```



This command enters a monitor session configuration mode. Upon first implementation the command also creates the session.

**Step 2.** Add source interface(s). Run:

```
switch (config monitor session 1) # add source interface ethernet 1/1 direction both
```

**Step 3.** Add destination interface. Run:

```
switch (config monitor session 1) # destination interface ethernet 1/2
```

**Step 4.** (Optional) Set header format. Run:

```
switch (config monitor session 1) # header-format add-ethernet-header destination-mac  
00:0d:ec:f1:a9:c8 add-vlan 10 priority 5 traffic-class 2
```



For remote connectivity use the header formats add-vlan or add-ethernet-header. For local connectivity, use local.

**Step 5.** (Optional) Truncate the mirrored traffic to 64-byte packets. Run:

```
switch (config monitor session 1) # truncate
```

**Step 6.** (Optional) Set congestion control. Run:

```
switch (config monitor session 1) # congestion pause-excessive-frames
```



The default for this command is to drop excessive frames. The pause-excessive-frames option uses flow control to regulate the traffic from the source interfaces.



If the option pause-excessive-frame is selected, make sure that flow control is enabled on **all** source interfaces on the ingress direction of the monitoring session using the command flowcontrol in the interface configuration mode.

#### Step 7. Enable the session. Run:

```
switch (config monitor session 1) # no shutdown
```

### 5.20.3 Verifying Mirroring Sessions

➤ *To verify the attributes of a specific mirroring session:*

```
switch (config) # show monitor session 1
Session 1:
  Admin: Enable
  Status: Up
  Truncate: Enable
  Destination interface: eth1/2
  Congestion type: pause-excessive-frames
  Header format: add-ethernet-header
  -switch priority: 5

  Source interfaces
  -----
  Interface  Direction
  -----
    eth1/1      both
```

➤ *To verify the attributes of running mirroring sessions:*

```
switch (config) # show monitor session summary
Flags: i ingress, e egress, b both

-----
Session Admin     Status Mode      Destination Source
-----
1       Enable     Up      add-eth    eth1/2      eth1/1(b)
2       Disable    Down    add-vlan   eth1/2      eth1/8(i), pol(e)
3       Enable     Up      add-eth    eth1/5      eth1/18(e)
7       Disable    Down    local
```

## 5.20.4 Commands

### 5.20.4.1 Config

#### monitor session

```
monitor session <session-id>
no monitor session <session-id>
```

Creates session and enters monitor session configuration mode upon using this command for the first time.

The no form of the command deletes the session.

<b>Syntax Description</b>	session-id	The monitor session ID. Range is: <ul style="list-style-type: none"><li>• 1-7 for SwitchX®</li><li>• 1-2 for Spectrum™</li></ul>		
<b>Default</b>	N/A			
<b>Configuration Mode</b>	Config			
<b>History</b>	3.3.3500			
<b>Role</b>	admin			
<b>Example</b>	<pre>switch (config)# monitor session 1 switch (config monitor session 1)#+</pre>			
<b>Related Commands</b>				
<b>Note</b>				

## 5.20.4.2 Config Monitor Session

### destination interface

**destination interface <type> <number> [force]**  
**no destination interface**

Sets the egress interface number.

The no form of the command deletes the destination interface.

<b>Syntax Description</b>	interface	Sets the interface type and number (e.g. ethernet 1/2)
	force	Eliminates the need to shutdown the port prior to the operation
<b>Default</b>	no destination interface	
<b>Configuration Mode</b>	Config Monitor Session	
<b>History</b>	3.3.3500	
	3.3.4100	Added force argument
	3.6.4006	Added note
<b>Role</b>	admin	
<b>Example</b>	switch (config monitor session 1) # destination interface ethernet 1/2	
<b>Related Commands</b>		
<b>Note</b>	<ul style="list-style-type: none"> <li>Port cannot be used as destination port in monitor session when storm-control is configured on port.</li> <li>Force command cannot remove storm-control configuration. Error output: Configuration error, storm control is configured on port</li> <li>When removing an interface from a monitor session it gains the default attributes of Ethernet ports</li> </ul>	

## shutdown

**shutdown**  
**no shutdown**

Disables the session.  
The no form of the command enables the session.

<b>Syntax Description</b>	N/A
<b>Default</b>	Disabled
<b>Configuration Mode</b>	Config Monitor Session
<b>History</b>	3.3.3500
<b>Role</b>	admin
<b>Example</b>	<pre>switch (config monitor session 1) # no shutdown switch (config monitor session 1) #</pre>
<b>Related Commands</b>	
<b>Note</b>	

## add source interface

```
add source interface <type> <number> direction <d-type>
no source interface <type> <number>
```

Adds a source interface to the mirrored session.

The no form of the command deletes the source interface.

<b>Syntax Description</b>	interface <type> <number>	Configures interface as “ethernet” or “port-channel”.
	direction <d-type>	Configures the direction of the mirrored traffic. The options are as follows: <ul style="list-style-type: none"> <li>• egress – sets the egress traffic to be monitored</li> <li>• ingress – sets the ingress traffic to be monitored</li> <li>• both – sets egress and ingress traffic to be monitored</li> </ul>
<b>Default</b>	N/A	
<b>Configuration Mode</b>	Config Monitor Session	
<b>History</b>	3.3.3500	
	3.5.1000	Updated
<b>Role</b>	admin	
<b>Example</b>	<pre>switch (config monitor session 1) # add source interface ethernet 1/1 direction ingress</pre>	
<b>Related Commands</b>		
<b>Note</b>	<ul style="list-style-type: none"> <li>• If mirroring is configured in one direction (e.g. ingress) on an interface and then is configured in the other direction (e.g. egress), then the ultimate setting is “both”</li> <li>• Spectrum™ based switch systems only support mirroring ingress traffic</li> </ul>	

## header-format

```
header-format {local [traffic-class <tc>] | add-vlan <vlan-id> [priority <prio>]
[traffic-class <tc>] [switch-priority <sp>] | add-ether-net-header destination-mac
<mac-address> [add-vlan <vlan-id> [priority <prio>]] [traffic-class <tc>]}
```

**no header-format**

Sets the header format of the mirrored traffic.

The no form of the command resets the parameter values back to default.

<b>Syntax Description</b>	local	The mirrored header of the frame is not changed.
	traffic-class <tc>	Changes the egress traffic class of the frame. Range: 0-3.
	switch-priority <sp>	Changes the egress switch priority of the frame. Range: 0-15.
	add-vlan <vlan-id>	An 802.1q VLAN tag is added to the frame.
	priority <prio>	The priority to be added to the Ethernet header. Range: 0-7.
	add-ether-net-header	Adds an Ethernet header to the mirrored frame.
	destination-mac	The destination MAC address of the added Ethernet frame.
<b>Default</b>	no-change vlan 1 priority 0 traffic-class 0	
<b>Configuration Mode</b>	Config Monitor Session	
<b>History</b>	3.3.3500	
	3.5.1000	Added switch-priority parameter
<b>Role</b>	admin	
<b>Example</b>	<pre>switch (config monitor session 1) # header-format add-ether-net-header destination-mac 00:0d:ec:f1:a9:c8 add-vlan 10 priority 5 traffic-class 2</pre>	
<b>Related Commands</b>		
<b>Note</b>	<ul style="list-style-type: none"> <li>If add-ether-net-header is used, the source MAC address is the one attached to the switch</li> <li>The parameter traffic-class is only available on SwitchX® based switch systems</li> <li>The parameter switch-priority is only available on Spectrum™ based switch systems</li> </ul>	

## truncate

**truncate**  
**no truncate**

Truncates the mirrored frames to 64-byte packets.  
The no form of the command disables truncation.

<b>Syntax Description</b>	N/A
<b>Default</b>	no truncate
<b>Configuration Mode</b>	Config Monitor Session
<b>History</b>	3.3.3500
<b>Role</b>	admin
<b>Example</b>	<pre>switch (config monitor session 1) # truncate switch (config monitor session 1) #</pre>
<b>Related Commands</b>	
<b>Note</b>	This command applies for all sessions on the same analyzer port.

## congestion

**congestion [drop-excessive-frames | pause-excessive-frames]  
no congestion**

Sets the system's behavior when congested  
The no form of the command disables truncation.

<b>Syntax Description</b>	drop-excessive-frames	Drops excessive frames.
	pause-excessive-frames	Pauses excessive frames.
<b>Default</b>	drop-excessive-frames	
<b>Configuration Mode</b>	Config Monitor Session	
<b>History</b>	3.3.3500	
	3.3.4000	Added Syntax Description.
<b>Role</b>	admin	
<b>Example</b>	<pre>switch (config monitor session 1) # congestion pause-excessive-frames switch (config monitor session 1) #</pre>	
<b>Related Commands</b>		
<b>Note</b>	This command applies for all sessions on the same analyzer port.	

### 5.20.4.3 Show

#### show monitor session

```
show monitor session <session-id>
```

Displays monitor session configuration and status.

<b>Syntax Description</b>	session-id	The monitor session ID Range: 1-7
<b>Default</b>	N/A	
<b>Configuration Mode</b>	Any Command Mode	
<b>History</b>	3.3.3500	
	3.5.1000	Updated Note section
	3.6.5000	Updated Example
<b>Role</b>	admin	
<b>Example</b>	<pre>switch (config) # show monitor session 1 Session 1:     Admin: Disable     Status: Down     Truncate: Disable     Destination interface: N/A     Congestion type: drop-excessive-frames     Header format: local     -switch priority: 0      Source interfaces     -----     Interface  Direction     -----     eth1/1      both switch (config) #</pre>	
<b>Related Commands</b>		
<b>Note</b>		

## show monitor session summary

### show monitor session summary

Displays monitor session configuration and status summary.

<b>Syntax Description</b>	N/A
<b>Default</b>	N/A
<b>Configuration Mode</b>	Any Command Mode
<b>History</b>	3.3.3500
	3.6.5000 Updated Example
<b>Role</b>	admin
<b>Example</b>	<pre>switch (config) # show monitor session summary Flags: i ingress, e egress, b both  ----- Session Admin      Status Mode      Destination Source ----- 1       Disable     Down   local     N/A          eth1/1(b) 2       Disable     Down   add-vlan  eth1/2        eth1/8(i) switch (config) #</pre>
<b>Related Commands</b>	
<b>Note</b>	

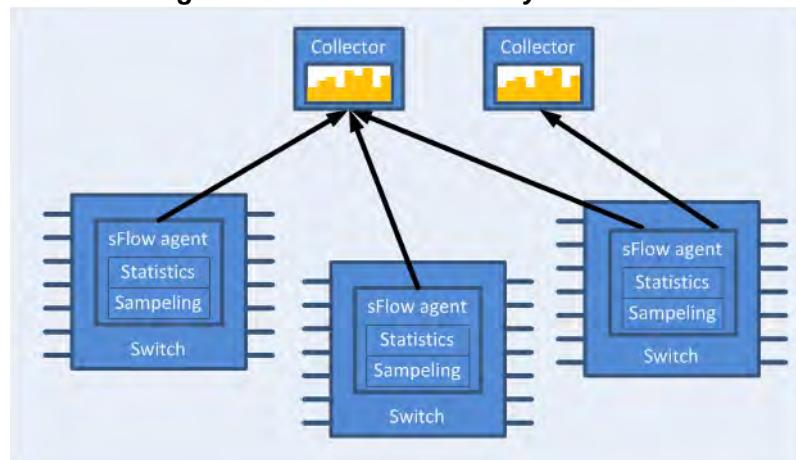
## 5.21 sFlow

sFlow (ver. 5) is a procedure for statistical monitoring of traffic in networks. MLNX-OS supports an sFlow sampling mechanism (agent), which includes collecting traffic samples and data from counters. The sFlow datagrams are then sent to a central collector.

The sampling mechanism must ensure that any packet going into the system has an equal chance of being sampled, irrespective of the flow to which it belongs. The sampling mechanism provides the collector with periodical information on the amount (and load) of traffic per interface by loading the counter samples into sFlow datagrams.

The sFlow packets are encapsulated and sent in UDP over IP. The UDP port number that is used is the standard 6343 by default.

**Figure 31: sFlow Functionality Overview**



### 5.21.1 Flow Samples

The sFlow agent samples the data path based on packets.

Truncation and sampling rate are the two parameters that influence the flow samples. In case of congestion the flow samples can be truncated to a predefined size before it is assigned to the CPU. The truncation can be set to any value between 64 to 256 bytes with the default being 128 bytes.

The sampling rate can be adjusted by setting an average rate. The system assures that a random number of packets is sampled, however, the sample rate on average converges to the configured rate. Valid values range between 4000 to 16777215 packets.

## 5.21.2 Statistical Samples

The sFlow agent samples interface counters time based. Polling interval is configurable to any value between 5-3600 seconds with the default being 20 seconds.

The following statistics are gathered by the CPU:

**Table 61 - List of Statistical Counters**

Counter	Description
Total packets	The number of packets that pass through sFlow-enabled ports.
Number of flow samples	The number of packets that are captured by the sampling mechanism.
Number of statistic samples	The number of statistical samples.
Number of discarded samples	The number of samples that were discarded.
Number of datagrams	The number of datagrams that were sent to the collector.

## 5.21.3 sFlow Datagrams

The sFlow datagrams contain flow samples and statistical samples.

The sFlow mechanism uses IP protocol, therefore if the packet length is more than the interface MTU, it becomes fragmented by the IP stack. The MTU may also be set manually to anything in the range of 200-9216 bytes. The default is 1400 bytes.

## 5.21.4 Sampled Interfaces

sFlow must be enabled on physical or LAG interfaces that require sampling. When adding a port to a LAG, sFlow must be disabled on the port. If a port with enabled sFlow is configured to be added to a LAG, the configuration is rejected. Removing a port from a LAG disables sFlow on the port regardless of the LAG's sFlow status.

## 5.21.5 Configuring sFlow

➤ *To configure the sFlow agent:*

**Step 1.** Unlock the sFlow commands. Run:

```
switch (config) # protocol sflow
```

**Step 2.** Enable sFlow on the system. Run:

```
switch (config) # sflow enable
```

**Step 3.** Enter sFlow configuration mode. Run:

```
switch (config) # sflow
switch (config sflow) #
```

**Step 4.** Set the central collector's IP. Run:

```
switch (config sflow) # collector-ip 10.10.10.10
```

**Step 5.** Set the agent-ip used in the sFlow header. Run:

```
switch (config sflow) # agent-ip 20.20.20.20
```

**Step 6.** (Optional) Set the sampling rate of the mechanism. Run:

```
switch (config sflow) # sampling-rate 16000
```



This means that one every 16000 packet gets collected for sampling.

**Step 7.** (Optional) Set the maximum size of the data path sample. Run:

```
switch (config sflow) # max-sample-size 156
```

**Step 8.** (Optional) Set the frequency in which counters are polled. Run:

```
switch (config sflow) # counter-poll-interval 19
```

**Step 9.** (Optional) Set the maximum size of the datagrams sent to the central collector. Run:

```
switch (config sflow) # max-datatype-size 1500
```

**Step 10.** Enable the sFlow agent on the desired interfaces. Run:

```
switch (config interface ethernet 1/1)# sflow enable  
switch (config interface port-channel 1)# sflow enable
```

## 5.21.6 Verifying sFlow

➤ *To verify the attributes of the sFlow agent:*

```
switch (config)# show sflow

sflow protocol enabled
sflow enabled
sampling-rate 16000
max-sampled-size 156
counter-poll-interval 19
max-datatype-size 1500
collector-ip 10.10.10.10
collector-port 6343
agent-ip 20.20.20.20
ingress ports
Interfaces
Ethernet: eth1/1
Port-channel: pol
Statistics:
Total Samples: 2000
Number of flow samples: 1200
Estimated Number of flow discarded: 0
Number of statistic samples: 800
Number of datagrams: 300
```

## 5.21.7 Commands

### 5.21.7.1 Config

#### protocol sflow

**protocol sflow**  
**no protocol sflow**

Unhides the sFlow commands.

The no form of the command deletes sFlow configuration and hides the sFlow commands.

---

**Syntax Description** N/A

**Default** Disabled

**Configuration Mode** Config

**History** 3.3.3500

**Role** admin

**Example**  
switch (config) # protocol sflow  
switch (config) #

**Related Commands**

---

**Note**

---

## sflow enable (global)

**sflow enable**  
**no sflow enable**

Enables sFlow in the system.

The no form of the command disables sFlow without deleting the configuration.

---

**Syntax Description** N/A

**Default** Disabled

**Configuration Mode** Config

**History** 3.3.3500

**Role** admin

**Example**  
switch (config) # sflow enable  
switch (config) #

---

**Related Commands**

---

**Note**

## sflow

### sflow

Enters sFlow configuration mode.

**Syntax Description** N/A

**Default** N/A

**Configuration Mode** Config

**History** 3.3.3500

**Role** admin

**Example**  
`switch (config) # sflow  
switch (config sflow) #`

**Related Commands**

**Note**

## 5.21.7.2 Config sFlow

### sampling-rate

**sampling-rate <rate>**  
**no sampling-rate**

Sets sFlow sampling ratio.

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

<b>Syntax Description</b>	rate	Sets the number of packets passed before selecting one for sampling. The range is 4000-16777215. Zero disables sampling.
<b>Default</b>	16000	
<b>Configuration Mode</b>	Config sFlow	
<b>History</b>	3.3.3500	
<b>Role</b>	admin	
<b>Example</b>		<pre>switch (config sflow) # sampling-rate 16111 switch (config sflow) #</pre>
<b>Related Commands</b>		
<b>Note</b>		

## max-sample-size

**max-sample-size <packet-size>**  
**no max-sample-size**

Sets the maximum size of sampled packets by sFlow.  
The no form of the command resets the parameter to its default value.

<b>Syntax Description</b>	packet-size	The sampled packet size. The range is 64-256 bytes.
<b>Default</b>	128 bytes	
<b>Configuration Mode</b>	Config sFlow	
<b>History</b>	3.3.3500	
<b>Role</b>	admin	
<b>Example</b>	switch (config sflow) # max-sample-size 165 switch (config sflow) #	
<b>Related Commands</b>		
<b>Note</b>	Sampled payload beyond the configured size is discarded.	

## counter-poll-interval

**counter-poll-interval <seconds>**  
**no counter-poll-interval**

Sets the sFlow statistics polling interval.

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

<b>Syntax Description</b>	seconds	The sFlow statistics polling interval in seconds. Range is 5-3600 seconds. Zero disables the statistic polling.		
<b>Default</b>	20 seconds			
<b>Configuration Mode</b>	Config sFlow			
<b>History</b>	3.3.3500			
<b>Role</b>	admin			
<b>Example</b>	<pre>switch (config sflow) # counter-poll-interval 30 switch (config sflow) #</pre>			
<b>Related Commands</b>				
<b>Note</b>				

## max-datatype-size

**max-datatype-size <packet-size>**  
**no max-datatype-size**

Sets the maximum sFlow packet size to be sent to the collector.  
The no form of the command resets the parameter to its default value.

<b>Syntax Description</b>	packet-size	The packet size of the packet being sent to the collector. The range is 200-9216 bytes.
<b>Default</b>	1400 bytes	
<b>Configuration Mode</b>	Config sFlow	
<b>History</b>	3.3.3500	
<b>Role</b>	admin	
<b>Example</b>	<pre>switch (config sflow) # max-datatype-size 9216 switch (config sflow) #</pre>	
<b>Related Commands</b>		
<b>Note</b>	This packet contains the data sample as well as the statistical counter data.	

## collector-ip

```
collector-ip <ip-address> [udp-port <udp-port-number>]  
no collector-ip [<ip-address> udp-port]
```

Sets the collector's IP.

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

<b>Syntax Description</b>	ip-address	The collector IP address.
	udp-port <udp-port-number>	Sets the collector UDP port number.
<b>Default</b>	ip-address: 0.0.0.0 udf-port-number: 6343	
<b>Configuration Mode</b>	Config sFlow	
<b>History</b>	3.3.3500	
<b>Role</b>	admin	
<b>Example</b>	<pre>switch (config sflow) # collector-ip 10.10.10.10 switch (config sflow) #</pre>	
<b>Related Commands</b>		
<b>Note</b>		

## agent-ip

```
agent-ip {<ip-address> | interface [ethernet <slot/port> | port-channel <channel-group>] | <if-name> | loopback <number> | vlan <id>}
no agent-ip
```

Sets the IP address associated with this agent.

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

<b>Syntax Description</b>	interface	Configures a specific ethernet/port-channel interface's agent IP.
	if-name	Interface name (e.g. mgmt0, mgmt1).
	ip-address	The sFlow agent's IP address (i.e. the source IP of the packet).
	loopback <number>	Loopback interface number. Range: 1-32.
	vlan <id>	Interface VLAN. Range: 1-4094.
<b>Default</b>	ip-address: 0.0.0.0	
<b>Configuration Mode</b>	Config sFlow	
<b>History</b>	3.3.3500	
	3.3.5200	Updated "interface" parameters
<b>Role</b>	admin	
<b>Example</b>	<pre>switch (config sflow) # agent-ip 20.20.20.20 switch (config sflow) #</pre>	
<b>Related Commands</b>		
<b>Note</b>	The IP address here is used in the sFlow header.	

## clear counters

### clear counters

Clears sFlow counters.

---

**Syntax Description** N/A

**Default** N/A

**Configuration Mode** Config sFlow

**History** 3.3.3500

**Role** admin

**Example**  
switch (config sflow) # clear counters  
switch (config sflow) #

---

**Related Commands**

---

**Note**

## **sflow enable (interface)**

**sflow enable**  
**no sflow enable**

Enables sFlow on this interface.

The `no` form of the command disables sFlow on the interface.

### 5.21.7.3 Show

#### show sflow

##### show sflow

Displays sFlow configuration and counters.

<b>Syntax Description</b>	N/A
<b>Default</b>	N/A
<b>Configuration Mode</b>	Any Command Mode
<b>History</b>	3.3.3500
	3.6.3004 Updated output example
<b>Role</b>	admin
<b>Example</b>	<pre>switch (config)# show sflow sflow protocol enabled sflow enabled sampling-rate 16000 max-sampled-size 156 counter-poll-interval 19 max-datatype-size 1500 collector-ip 10.10.10.10 collector-port 6343 agent-ip 20.20.20.20 ingress ports Interfaces Ethernet: eth1/1 Port-channel: po1 Statistics: Total Samples: 2000 Number of flow samples: 1200 Estimated Number of flow discarded: 0 Number of statistic samples: 800 Number of datagrams: 300</pre>

---

#### Related Commands

---

#### Note

---

## 5.22 Transport Applications

### 5.22.1 RDMA over Converged Ethernet (RoCE)

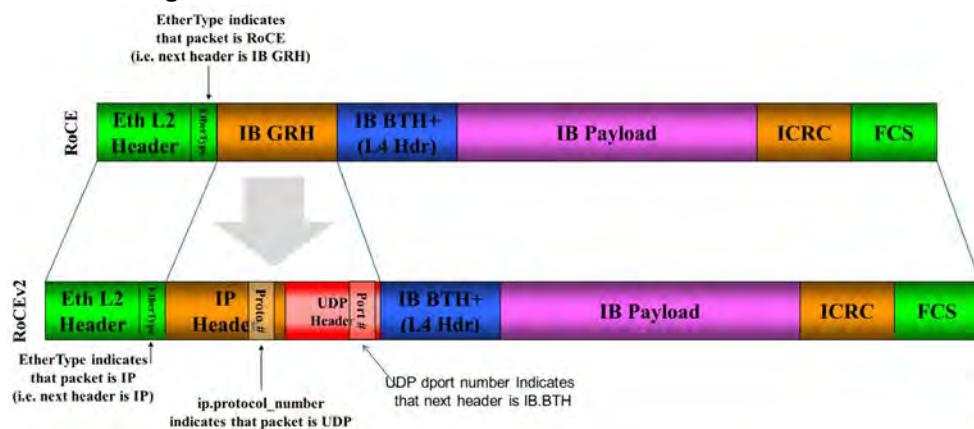
#### 5.22.1.1 RoCE Overview

Remote Direct Memory Access (RDMA) is the remote memory management capability that allows server to server data movement directly between application memory without any CPU involvement. RDMA over Converged Ethernet (RoCE) is a mechanism to provide this efficient data transfer with very low latencies on loss-less Ethernet networks. With advances in data center convergence over reliable Ethernet, ConnectX® EN with RoCE uses the proven and efficient RDMA transport to provide the platform for deploying RDMA technology in mainstream data center application at 10GigE and 40GigE link-speed. ConnectX® EN with its hardware offload support takes advantage of this efficient RDMA transport services over Ethernet to deliver ultra-low latency for performance-critical and transaction intensive applications such as financial, database, storage, and content delivery networks. RoCE encapsulates IB transport and GRH headers in Ethernet packets bearing a dedicated ether type. While the use of GRH is optional within subnets, it is mandatory when using RoCE. Applications written over IB verbs should work seamlessly, but they require provisioning of GRH information when creating address vectors. The library and driver are modified to provide mapping from GID to MAC addresses required by the hardware.

#### 5.22.1.1.1 IP Routable (RoCEv2)

A straightforward extension of the RoCE protocol enables traffic to operate in layer 3 environments. This capability is obtained via a simple modification of the RoCE packet format. Instead of the GRH used in RoCE, routable RoCE packets carry an IP header which allows traversal of IP L3 Routers and a UDP header that serves as a stateless encapsulation layer for the RDMA Transport Protocol Packets over IP.

**Figure 32: RoCEv2 and RoCE Frame Format Differences**

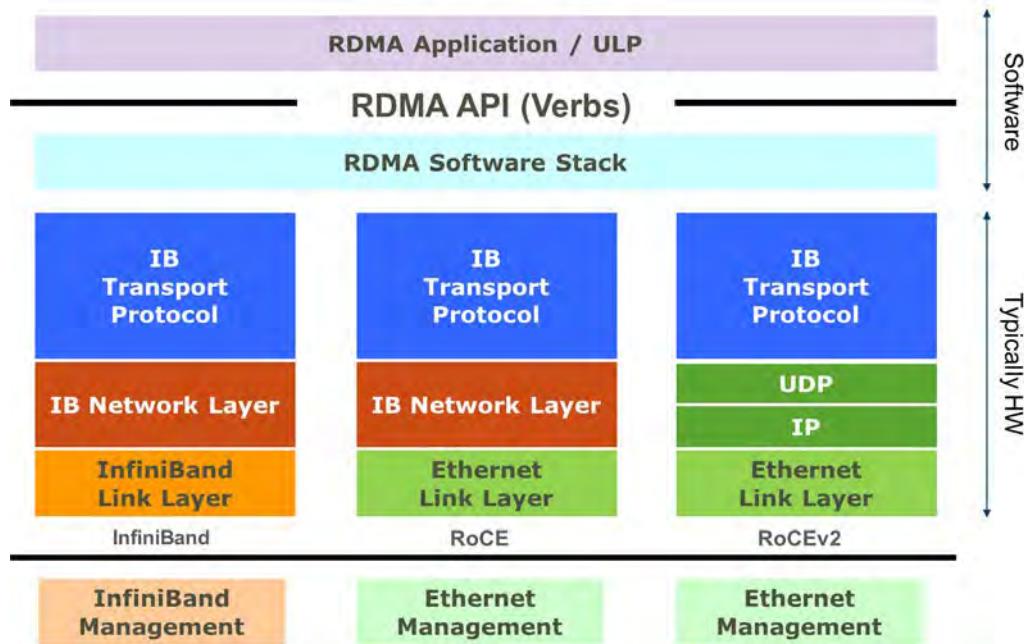


The proposed RoCEv2 packets use a well-known UDP destination port value that unequivocally distinguishes the datagram. Similar to other protocols that use UDP encapsulation, the UDP source port field is used to carry an opaque flow-identifier that allows network devices to imple-

ment packet forwarding optimizations (e.g. ECMP) while staying agnostic to the specifics of the protocol header format.

Furthermore, since this change exclusively affects the packet format on the wire, and due to the fact that with RDMA semantics packets are generated and consumed below the AP applications can seamlessly operate over any form of RDMA service (including the routable version of RoCE as shown in Figure 2), in a completely transparent way<sup>1</sup>.

**Figure 33: RoCEv2 Protocol Stack**



### 5.22.1.2 RoCE Configuration

In order to function reliably, RoCE requires a form of flow control. While it is possible to use global flow control, this is normally undesirable, for performance reasons.

The normal and optimal way to use RoCE is to use Priority Flow Control (PFC). To use PFC, it must be enabled on all endpoints and switches in the flow path.

In the following section we present instructions to configure PFC on Mellanox ConnectX™ cards. There are multiple configuration steps required, all of which may be performed via PowerShell. Therefore, although we present each step individually, you may ultimately choose to write a PowerShell script to do them all in one step. Note that administrator privileges are required for these steps.

For further information, please refer to the following URL:

<http://blogs.technet.com/b/josebda/archive/2012/07/31/deploying-windows-server-2012-with-smb-direct-smb-over-rdma-and-the-mellanox-connectx-3-using-10gbe-40gbe-roce-step-by-step.aspx>

1. Standard RDMA APIs are IP based already for all existing RDMA technologies

### 5.22.1.2.1 Prerequisites

The following are the driver's prerequisites in order to set or configure RoCE:

- ConnectX®-3 and ConnectX®-3 Pro firmware version 2.30.3000 or higher
- Set HCA to use Ethernet protocol:  
Display the Device Manager and expand "System Devices".

### 5.22.1.2.2 Configuring Windows Host



Since PFC is responsible for flow controlling at the granularity of traffic priority, it is necessary to assign different priorities to different types of network traffic.

As per RoCE configuration, all ND/NDK traffic is assigned to one or more chosen priorities, where PFC is enabled on those priorities.

Configuring Windows host requires configuring QoS.

#### 5.22.1.2.2.1 Using Global Pause Flow Control (GFC)

- *To use Global Pause Flow Control (GFC) mode, disable QoS and Priority:*

```
PS $ Disable-NetQosFlowControl  
PS $ Disable-NetAdapterQos
```

### 5.22.1.3 Configuring Switch Systems

- *To enable RoCE, the SwitchX should be configured as follows:*

- Ports facing the host should be configured as access ports, and either use global pause or Port Control Protocol (PCP) for priority flow control
- Ports facing the network should be configured as trunk ports, and use Port Control Protocol (PCP) for priority flow control

### 5.22.1.4 Configuring Router (PFC only)

The router uses L3's DSCP value to mark the egress traffic of L2 PCP. The required mapping, maps the three most significant bits of the DSCP into the PCP. This is the default behavior, and no additional configuration is required.

#### 5.22.1.4.1 Copying Port Control Protocol (PCP) Between Subnets

The captured PCP option from the Ethernet header of the incoming packet can be used to set the PCP bits on the outgoing Ethernet header.

### 5.22.1.5 Configuring the RoCE Mode

Configuring the RoCE mode requires the following:

- RoCE mode is configured per-driver and is enforced on all the devices in the system



The supported RoCE modes depend on the firmware installed. If the firmware does not support the needed mode, the fallback mode would be the maximum supported RoCE mode of the installed NIC.

RoCE mode can be enabled and disabled via PowerShell.

➤ ***To enable RoCE using the PowerShell:***

- Open the PowerShell and run:

```
Set-MlnxDriverCoreSetting -RoceMode 1
```

➤ ***To enable RoCEv2 using the PowerShell:***

- Open the PowerShell and run:

```
Set-MlnxDriverCoreSetting -RoceMode 2
```

➤ ***To disable any version of RoCE using the PowerShell:***

Open the PowerShell and run:

```
Set-MlnxDriverCoreSetting -RoceMode 0
```

➤ ***To check current version of RoCE using the PowerShell:***

**Step 1.** Open the PowerShell and run:

```
Get-MlnxDriverCoreSetting
```

**Step 2.** Example output:

```
Caption : DriverCoreSettingData 'mlx4_bus'  
Description : Mellanox Driver Option Settings  
. .  
RoceMode : 0
```

## 5.23 802.1x Protocol

The 802.1x standard describes a way to authenticate hosts (or supplicants) and to allow connection only to a list of allowed hosts pre-configured on an authentication server. The authentication is performed by the switch (authenticator) which negotiates the authentication with a RADIUS server (authentication server). This allows to block traffic from non-authenticated sources.

The 802.1x protocol defines the following roles:

- Supplicant – the host. It provides the authentication credentials to the authenticator and awaits approval.
- Authenticator – the device that connects the supplicant to the network, and checks the authentication with the authentication server. The authenticator is also in charge of blocking and isolating of new client till authenticated and allowing communication once the client has passed the authentication. Mellanox switch acts as an authenticator.
- Authentication server – a RADIUS server which can authenticate the user.



The 802.1x is available only on access physical ports. It is not available on LAG and MLAG ports.



A local analyzer port cannot support 802.1x protocol.



802.1x cannot be activated on router port interfaces.



802.1x cannot run on a port configured to switchport trunk or hybrid.



Management interfaces cannot be configured as 802.1x port access entity (PAE) authenticators.

### 5.23.1 802.1x Operating Modes

The following operating modes are supported in 802.1x:

- Single host – only one supplicant can communicate through the port.

Once authentication of the supplicant is accepted by the authentication server, the switch allows it access. If the supplicant logs off or the port state is changed, the port becomes unauthenticated. And if a different supplicant tries to access through this port, its bidirectional traffic is discarded (including authentication traffic).



An exception to this is multicast and broadcast traffic which do get transmitted over the interface once authenticated and are exposed to an unauthorized supplicant if it exists.

- Multi-host mode – allows connection of multiple hosts over a single port. Only the first supplicant is authenticated. Subsequent hosts have network access without the need to authenticate.

### 5.23.2 Configuring 802.1x

➤ *To configure 802.1x on the switch*

- Step 1.** Enable 802.1x protocol. Run:

```
switch (config) # protocol dot1x
```

- Step 2.** Enable the system as authenticator. Run:

```
switch (config) # dot1x system-auth-control
```

- Step 3.** Configure RADIUS server parameters. Run:

```
switch (config) # dot1x radius-server host 10.10.10.10 key my4uth3nt1c4t10nk3y retransmit 2 timeout 3
```

- Step 4.** Enter the configuration mode of an Ethernet interface. Run:

```
switch (config) # interface ethernet 1/1
switch (config interface ethernet 1/1) #
```

- Step 5.** Configure the interface as a port access entity authenticator. Run:

```
switch (config interface ethernet 1/1) # dot1x pae authenticator
```

- Step 6.** Configure the interface to perform authentication on ingress traffic. Run:

```
switch (config interface ethernet 1/1) # dot1x port-control auto
```

- Step 7.** Verify 802.1x configuration. Run:

```
switch (config interface ethernet 1/1) # show dot1x interfaces ethernet 1/1
```

Eth1/1	
PAE Status:	Enabled
Configured host mode:	Multi-host
Configured port-control:	Auto
Authentication status:	Unauthorized

```
Re-Authentication:           Disabled
Re-Authentication period (sec): -
Tx wait period (sec):       30
Quiet period (sec):         60
Max request retry:          2
Last EAPOL RX source MAC:   00:00:00:00:00:00
switch (config interface ethernet 1/1)#

```

### 5.23.3 Commands

#### protocol dot1x

**protocol dot1x**  
**no protocol dot1x**

Enables 802.1x EAPOL protocol.

The no form of the command disables 802.1x EAPOL protocol.

<b>Syntax Description</b>	N/A
<b>Default</b>	Disabled
<b>Configuration Mode</b>	Config
<b>History</b>	3.4.2008
<b>Role</b>	admin
<b>Example</b>	switch (config)# protocol dot1x
<b>Related Commands</b>	
<b>Note</b>	

## dot1x clear-statistics

### dot1x clear-statistics

Resets the 802.1x counters on all or a specific port.

<b>Syntax Description</b>	N/A
<b>Default</b>	N/A
<b>Configuration Mode</b>	Config Config Interface Ethernet
<b>History</b>	3.4.2008
<b>Role</b>	admin
<b>Example</b>	switch (config)# dot1x clear-statistics
<b>Related Commands</b>	
<b>Note</b>	

## dot1x pae authenticator

**dot1x pae authenticator**  
**no dot1x pae authenticator**

Configures the port as a 802.1x port access entity (PAE) authenticator.  
The no form of the command disables the port from being a 802.1x PAE authenticator.

<b>Syntax Description</b>	N/A
<b>Default</b>	Disabled
<b>Configuration Mode</b>	Config Interface Ethernet
<b>History</b>	3.4.2008
<b>Role</b>	admin
<b>Example</b>	<pre>switch (config interface ethernet 1/2)# dot1x system-auth-control</pre>
<b>Related Commands</b>	
<b>Note</b>	

## dot1x host-mode

**dot1x host-mode [multi-host | single-host]**  
**no dot1x host-mode**

Configures the authentication mode to either multi-host or single-host.  
The no form of the command resets the parameter to its default.

<b>Syntax Description</b>	multi-host	Sets the interface to operate in a port-based mode
	single-host	Sets the interface to operate in a MAC-based mode with support of a single supplicant per interface
<b>Default</b>	single-host	
<b>Configuration Mode</b>	Config Interface Ethernet	
<b>History</b>	3.4.2008	
	3.4.2300	Added “single-host” option
<b>Role</b>	admin	
<b>Example</b>	switch (config interface ethernet 1/2)# dot1x host-mode single-host	
<b>Related Commands</b>		
<b>Note</b>		

## dot1x port-control

**dot1x port-control [auto | force-authorized | force-unauthorized]  
no dot1x port-control**

Configures 802.1x port access entity (PAE) port-control.  
The no form of the command resets the parameter to its default.

<b>Syntax Description</b>	auto	The authenticator uses PAE authentication services to allow or block the port traffic
	force-authorized	Allows traffic on this port regardless of supplicant authorization
	force-unauthorized	Blocks traffic on this port regardless of supplicant authorization
<b>Default</b>	Force-authorized	
<b>Configuration Mode</b>	Config Interface Ethernet	
<b>History</b>	3.4.2008	
<b>Role</b>	admin	
<b>Example</b>	switch (config interface ethernet 1/2)# dot1x port-control auto	
<b>Related Commands</b>		
<b>Note</b>		

## dot1x radius-server host

```
dot1x radius-server host <IP address> [enable | auth-port <port> | key <password> | prompt-key | retransmit <retries> | timeout <seconds>]  

no dot1x radius-server host <IP address> enable
```

Configure 802.1x RADIUS server IP address.

The no form of the command disables 802.1x RADIUS server.

<b>Syntax Description</b>	auth-port enable key prompt-key retransmit timeout	Sets 802.1x RADIUS port to use with this server. Range: 1-65535. Sets 802.1x RADIUS as administratively enabled Configures 802.1x global RADIUS shared secret for servers. Prompts for key, rather than entering on command line Configure 802.1x global RADIUS retransmit count for servers. The time configured is in seconds. Range: 0-5. Configures 802.1x global RADIUS timeout value for servers. The time configured is in seconds. Range: 1-60.
<b>Default</b>	auth-port: 1812 key: empty string retransmit: 1 timeout: 3	
<b>Configuration Mode</b>	Config	
<b>History</b>	3.4.2008	
<b>Role</b>	admin	
<b>Example</b>	switch (config)# dot1x radius-server host 10.10.10.10 auth-port 65535 prompt-key enable	
<b>Related Commands</b>		
<b>Note</b>	<ul style="list-style-type: none"> <li>The no form of the various parameters resets them to their default values as indicated in the Default section above</li> <li>It is possible to configure up to 5 RADIUS servers</li> <li>It is possible to configure only 1 authentication port per RADIUS server IP</li> </ul>	

## dot1x reauthenticate

**dot1x reauthenticate**  
**no dot1x reauthenticate**

Enables supplicant re-authentication according to the configuration of command “dot1x timeout reauthentication”.

The no form of the command disables supplicant re-authentication.

<b>Syntax Description</b>	N/A
<b>Default</b>	No re-authentication
<b>Configuration Mode</b>	Config Interface Ethernet
<b>History</b>	3.4.2008
<b>Role</b>	admin
<b>Example</b>	switch (config interface ethernet 1/2)# dot1x reauthenticate
<b>Related Commands</b>	
<b>Note</b>	

## dot1x system-auth-control

**dot1x system-auth-control**  
**no dot1x system-auth-control**

Enables the system as authenticator.

The no form of the command disables the system as authenticator.

<b>Syntax Description</b>	N/A
<b>Default</b>	Disabled
<b>Configuration Mode</b>	Config
<b>History</b>	3.4.2008
<b>Role</b>	admin
<b>Example</b>	switch (config)# dot1x system-auth-control
<b>Related Commands</b>	
<b>Note</b>	

## dot1x timeout reauthentication

**dot1x timeout reauthentication <period>**  
**no dot1x timeout reauthentication**

Configures the number of seconds between re-authentication attempts.  
The no form of the command resets the parameter to its default.

<b>Syntax Description</b>	period	Time in second. Range: 1-65535 seconds.		
<b>Default</b>	3600 seconds			
<b>Configuration Mode</b>	Config Interface Ethernet			
<b>History</b>	3.4.2008			
<b>Role</b>	admin			
<b>Example</b>	switch (config interface ethernet 1/2)# dot1x timeout reauthentication 3600			
<b>Related Commands</b>				
<b>Note</b>				

## dot1x timeout quiet-period

```
dot1x timeout quiet-period <period>
no dot1x timeout quiet-period
```

Configures the number of seconds that the authenticator remains quiet following a failed authentication exchange with the supplicant.

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

<b>Syntax Description</b>	period	Time in second. Range: 1-65535 seconds.
<b>Default</b>	60 seconds	
<b>Configuration Mode</b>	Config Interface Ethernet	
<b>History</b>	3.4.2008	
<b>Role</b>	admin	
<b>Example</b>	switch (config interface ethernet 1/2)# dot1x timeout quiet-period 60	
<b>Related Commands</b>		
<b>Note</b>		

## dot1x timeout tx-period

**dot1x timeout tx-period <period>**  
**no dot1x timeout tx-period**

Configures the maximum number of seconds that the authenticator waits for supplicant response of EAP-request/identify frame before retransmitting the request.  
The no form of the command resets the parameter to its default.

<b>Syntax Description</b>	period	Time in second. Range: 1-65535 seconds.
<b>Default</b>	30 seconds	
<b>Configuration Mode</b>	Config Interface Ethernet	
<b>History</b>	3.4.2008	
<b>Role</b>	admin	
<b>Example</b>	switch (config interface ethernet 1/2)# dot1x timeout quiet-period 30	
<b>Related Commands</b>		
<b>Note</b>		

## dot1x max-req

**dot1x max-req <retries>**  
**no dot1x max-req**

Configures the maximum amount of retries for the authenticator to communicate with the supplicant over EAP.

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

<b>Syntax Description</b>	retries	The number of request retries. Range: 1-10.
<b>Default</b>	2	
<b>Configuration Mode</b>	Config Interface Ethernet	
<b>History</b>	3.4.2008	
<b>Role</b>	admin	
<b>Example</b>	switch (config interface ethernet 1/2)# dot1x max-req 2	
<b>Related Commands</b>		
<b>Note</b>		

## show dot1x

### show dot1x

Displays 802.1x information on all interfaces.

<b>Syntax Description</b>	N/A
<b>Default</b>	N/A
<b>Configuration Mode</b>	Any Command Mode
<b>History</b>	3.4.2008
<b>Role</b>	admin
<b>Example</b>	<pre>switch (config)# show dot1x System authentication is enabled ----- Port      Pae     Host-mode   Port-control      Status ----- Eth1/1    Enabled  multi-host  auto            unauthorized Eth1/2    Disabled multi-host  force-authorized down Eth1/3    Disabled multi-host  force-authorized down Eth1/4    Disabled multi-host  force-authorized down Eth1/5    Disabled multi-host  force-authorized down Eth1/6    Disabled multi-host  force-authorized down Eth1/7    Disabled multi-host  force-authorized down Eth1/8    Disabled multi-host  force-authorized down Eth1/9    Disabled multi-host  force-authorized down ... switch (config)# </pre>
<b>Related Commands</b>	
<b>Note</b>	

## show dot1x interfaces ethernet

**show dot1x interfaces ethernet <slot>/<port>**

Displays 802.1x interface information.

<b>Syntax Description</b>	<slot>/<port>	Ethernet interface
<b>Default</b>	N/A	
<b>Configuration Mode</b>	Any Command Mode	
<b>History</b>	3.4.2008	
<b>Role</b>	admin	
<b>Example</b>	<pre>switch (config)# show dot1x interfaces ethernet 1/2  Eth1/2 PAE Status: Enabled Configured host mode: Multi-host Configured port-control: Auto Authentication status: Unauthorized Re-Authentication: Enabled Re-Authentication period (sec): 3600 Tx wait period (sec): 30 Quiet period (sec): 60 Max request retry: 2 Last EAPOL RX source MAC: 00:00:00:00:00:00 switch (config interface ethernet 1/2)# switch (config)</pre>	
<b>Related Commands</b>		
<b>Note</b>		

## show dot1x interfaces ethernet statistics

**show dot1x interfaces ethernet <slot>/<port> statistics**

Displays 802.1x interface information.

<b>Syntax Description</b>	<slot>/<port>	Ethernet interface
<b>Default</b>	N/A	
<b>Configuration Mode</b>	Any Command Mode	
<b>History</b>	3.4.2008	
<b>Role</b>	admin	
<b>Example</b>	<pre>switch (config)# show dot1x interfaces ethernet 1/2 statistics</pre> <pre>Eth1/2   EAPOL frames received: 3   EAPOL frames transmitted: 2   EAPOL Start frames received: 1   EAPOL Logoff frames received: 0   EAP Response-ID frames received: 2   EAP Response frames received: 0   EAP Request-ID frames transmitted: 2   EAP Request frames transmitted: 0   Invalid EAPOL frames received: 0   EAP length error frames received: 0   Last EAPOL frame version: 1   Last EAPOL frame source: 00:1A:A0:02:E9:8E switch (config)# </pre>	
<b>Related Commands</b>		
<b>Note</b>		

## show dot1x radius

### show dot1x radius

Displays 802.1x RADIUS settings.

**Syntax Description** N/A

**Default** N/A

**Configuration Mode** Any Command Mode

**History** 3.4.2008

**Role** admin

**Example**

```
switch (config)# show dot1x radius
802.1x RADIUS defaults:
    Key:          *****
    Timeout:      3
    Retransmit:   1
No 802.1x RADIUS servers configured.
switch (config)#+
```

**Related Commands**

**Note**

## 5.24 Voice VLAN

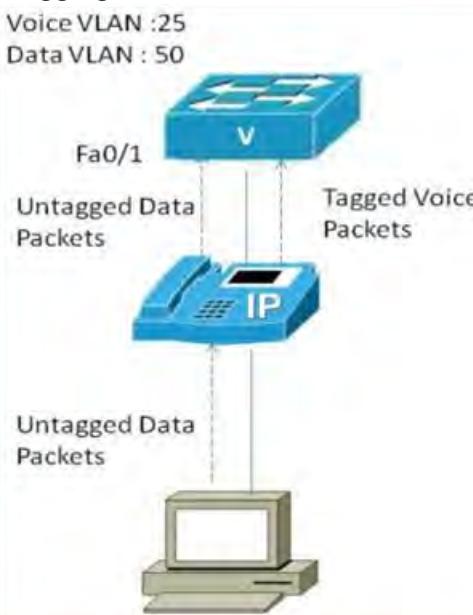
Voice VLAN allows configuring a port to provide QoS to voice and data traffic in a scenario where a terminal is connected to an IP phone which is in turn connected to the port on the switch. The IP phone bridges the data traffic from the terminal into the switch port. Any voice traffic from the IP phone is also sent to the same port with no differentiation. Therefore it is in the administrator's interest to provide different QoS to the voice traffic and the data traffic by placing the voice traffic on a different VLAN from the data traffic.

This can be achieved by configuring a voice VLAN on the desired switch port using LLDP-MED TLVs. Media Endpoint Discovery (MED) TLVs allow the switch to apply certain policies by informing the remote media device to configure itself using different TLV.

In this use-case scenario we employ the use of the network policy TLV, which is defined as per TIA-TR41. The network policy TLV can be used to inform a specific VLAN to use for an application stream.

MLNX-OS® allow the user to configure the VLAN for voice traffic. In Figure 34, the user configures a voice VLAN of 25 and the switch port has a PVID of 50. Therefore all the voice traffic is switched onto VLAN 25 and the untagged packets from the terminal are switched into VLAN 50.

**Figure 34: Tagging Voice Packets with a Different VLAN ID**



### 5.24.1 Configuring Voice VLAN

- *To configure LLDP-MED TLV, run:*

```

switch (config) # interface ethernet 1/4
switch (config interface ethernet 1/4) # lldp med-tlv-select media-capabilities
switch (config interface ethernet 1/4) # lldp med-tlv-select network-policy
switch (config interface ethernet 1/4) # lldp med-tlv-select all

```

- To verify LLDP-MED TLV configuration, run:

```

switch (config) # show lldp interfaces
TLV flags:
PD: port-description, SN: sys-name, SD: sys-description, SC: sys-capabilities, MA: man-
agement-address
ETS-C: ETS-Configuration, ETS-R: ETS-Recommendation, AP: Application Priority, PFC:
Priority Flow Control
CEE: Converged Enhanced Ethernet DCBX version
MED-CAP: Media Capabilities
MED-NWP: MED-Network Policy

Interface Receive   Transmit   TLVs
-----
Eth1/1    Enabled   Enabled   PD, SD
Eth1/2    Enabled   Enabled   PD, SN, SD, SC, MA, PFC, AP, ETS-C, ETS-R
Eth1/3    Disabled  Disabled  PD, SN, SD, SC, MA, PFC, AP, ETS-C, ETS-R, MED-NWP
Eth1/4    Enabled   Enabled   PD, SN, SD, SC, MA, PFC, AP, ETS-C, ETS-R,
                           MED-CAP, MED-NWP
Eth1/5    Enabled   Enabled   PD, SN, SD, SC, MA, PFC, AP, ETS-C, ETS-R
Eth1/6    Enabled   Enabled   PD, SN, SD, SC, MA, PFC, AP, ETS-C, ETS-R
...
.

switch (config) # show lldp interfaces ethernet 1/4
TLV flags:
PD: port-description, SN: sys-name, SD: sys-description, SC: sys-capabilities, MA: man-
agement-address
ETS-C: ETS-Configuration, ETS-R: ETS-Recommendation, AP: Application Priority, PFC:
Priority Flow Control
CEE: Converged Enhanced Ethernet DCBX version
MED-CAP: Media Capabilities
MED-NWP: MED-Network Policy

Interface Receive   Transmit   TLVs
-----
Eth1/4    Enabled   Enabled   PD, SN, SD, SC, MA, PFC, AP, ETS-C, ETS-R,
                           MED-CAP, MED-NWP

switch (config) # show lldp interfaces ethernet 1/4 med-cap
Media Capabilities:
  LLDP-MED Capab   : Yes
  Network Policy   : Yes
  Location Id     : No
  Ext Power MDI-PSE: No
  Ext Power MDI-PD : No

Network Policy:
  Application Type : 1 (Voice)
  VLAN Id         : 11
  L2 Priority     : 0
  DSCP Value      : 0

```

➤ **To configure voice VLAN:**

**Step 1.** Create a VLAN. Run:

```
switch (config) # vlan 200
switch (config vlan 200) # exit
switch (config) #
```

**Step 2.** Set the interface mode to be hybrid. Run:

```
switch (config) # interface ethernet 1/4 switchport mode hybrid
switch (config) # interface ethernet 1/4 switchport hybrid allowed-vlan 200
```

**Step 3.** Assign the VLAN to the interface. Run:

```
switch (config) # interface ethernet 1/4 switchport voice vlan 200
```

**Step 4.** (Optional) Change the PVID of the port so that untagged packets go to a different VLAN than the default. Run:

```
switch (config)# vlan 300
switch (config vlan 300)# exit
switch (config)# interface ethernet 1/4 switchport access vlan 300
```

**Step 5.** Verify the configuration. Run:

```
switch (config)# show interfaces switchport
Interface      Mode       Access vlan      Allowed vlans
-----
Eth1/1         access     1
Eth1/2         access     1
Eth1/3         access     1
Eth1/4         hybrid     300             200
Eth1/5         access     1
...
switch (config)# show lldp interfaces ethernet 1/4
TLV flags:
PD: port-description, SN: sys-name, SD: sys-description, SC: sys-capabilities, MA: management-address
ETS-C: ETS-Configuration, ETS-R: ETS-Recommendation, AP: Application Priority, PFC: Priority Flow Control
CEE: Converged Enhanced Ethernet DCBX version
MED-CAP: Media Capabilities
MED-NWP: MED-Network Policy

Interface Receive   Transmit   TLVs
-----
Eth1/4    Enabled    Enabled    PD, SN, SD, SC, MA, PFC, AP, ETS-C, ETS-R,
          MED-CAP, MED-NWP

switch (config)# show lldp interfaces ethernet 1/4 med-cap
Media Capabilities:
  LLDP-MED Capab  : Yes
  Network Policy  : Yes
  Location Id    : No
  Ext Power MDI-PSE: No
  Ext Power MDI-PD : No
```

```
Network Policy:  
  Application Type : 1 (Voice)  
  VLAN Id         : 200  
  L2 Priority     : 0  
  DSCP Value      : 0
```

➤ **To remove voice VLAN and LLDP-MED TLV:**

- Step 1.** Remove the voice VLAN from the interface. Run:

```
switch (config)# no interface ethernet 1/4 switchport voice vlan
```

- Step 2.** Disable the MED TLV from the interface. Run:

```
switch (config)# interface ethernet 1/4 lldp med-tlv-select none
```

## 5.24.2 Limitations

1. LLDP MED cannot be enabled on a router port interface and vice versa (i.e. a port that has LLDP MED enabled cannot be configured as a router port interface).
2. LLDP MED cannot be enabled on a LAG and vice versa (i.e. a port that has LLDP MED enabled cannot be configured as a LAG).
3. If switchport is in trunk, dot1q-tunnel, or dcbx-access, configuring either the TLV or Voice VLAN gives a warning message.

## 5.25 Store-and-Forward



This section is relevant only for Mellanox Spectrum™ systems.

### 5.25.1 General

Store-and-Forward is used to describe a functionality where a switch receives a complete packet, stores it, and only then forwards it.

since the switch make forwarding decisions based on the destination address which is at the header of the packet, the switch can make the forwarding decision before receiving the complete packet, this process is called cut-through, the switch forwards part of the packet before receiving the complete packet.

Cut-through allows lower latency and saves buffer space, but if an error occurred in the packet while utilizing cut-through, the packet will be forwarded with an error, alternatively, utilizing store-and-forward allows the switch to drop erroneous packets.

The standard implementation of forwarding mode is for the entire switch; either all ports on a switch are in store-and-forward mode or all ports on a switch are in cut-through mode.

MellanoxHPE implements forwarding mode per egress port, which is a more flexible method and vital in cases where a switch is connected to both a storage device and a compute server among other setups.

## 5.25.2 Commands

### switchmode store-and-forward

[no | disable] switchmode store-and-forward

Enables global store-and-forward configuration on the switch.

The no form of the command removes store-and-forward configuration from the switch and reverts it back to the switch's global configuration.

The disable form of the command configures the forwarding mode to cut-through.

<b>Syntax Description</b>	N/A
<b>Default</b>	N/A
<b>Configuration Mode</b>	Config Config Interface Ethernet Config Interface Port Channel
<b>History</b>	3.6.3640
<b>Role</b>	admin
<b>Example</b>	switch (config)# switchmode store-and-forward
<b>Related Commands</b>	
<b>Note</b>	

## 6 IP Routing

### 6.1 General

#### 6.1.1 IP Interfaces

MLNX-OS® supports the following 3 types of IP interfaces:

- VLAN interface
- Loopback interface
- Router port interface



Router port interfaces are not supported on SX10xx-xxxR and SX60xx-xxxR systems.

VLAN interface is a logical IPv4 interface created per subnet over a specific 802.1Q VLAN ID. If two hosts from two different subnets need to communicate (via the IP layer), the network administrator needs to configure two interface VLANs, one for each of the subnets. The user may configure up to 64 VLAN interfaces.

Each interface VLAN has the following attributes:

- Admin state
- Operational state
- MAC address
- IP address and mask
- MTU
- Description
- Set of counters

Loopback interface is a logical software entity where traffic transmitted to this interface is immediately received on the sending end.

Router port interface is a regular switch port configured to operate as an L3 interface. Router port interfaces are assigned an IP address and all L3 commands become applicable to them.

Once configured, router port interfaces no longer partake in the bridging activities of the switch and VLANs configured on them are separate from the pool allocated for the switch ports.

### 6.1.1.1 Configuring a VLAN Interface

- *To configure a VLAN interface:*

**Step 1.** Create a VLAN. Run:

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

**Step 2.** Assign a physical interface to this VLAN. Run:

```
switch (config)# interface ethernet 1/1
switch (config interface ethernet 1/1)# switchport mode access
switch (config interface ethernet 1/1)# exit
```

**Step 3.** There must be at least one interface in the operational state “UP”.

switch (config)# show interface etherent 1/1 status			
Port	Operational state	Speed	Negotiation
---	-----	-----	-----
Eth1/1	Up	40 Gbps	No-Negotiation

**Step 4.** Create a VLAN interface that matches the VLAN. Run:

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

**Step 5.** Configure an IP address and a network mask to the interface. Run:

```
switch (config interface vlan 10)# ip address 10.10.10.10 /24
```

**Step 6.** Verify VLAN interface configuration. Run:

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

Vlan 10
Admin state: Enabled
Operational state: UP
Mac Address: 00:02:c9:5d:e0:f0
Internet Address: 10.10.10.10/24
Broadcast address: 10.10.10.255
MTU: 1500 bytes
Description: my-ip-interface
Counters: disabled
```

### 6.1.1.2 Configuring a Loopback Interface

- *To configure a loopback interface:*

**Step 1.** Create a loopback interface. Run:

```
switch (config)# interface loopback 2
switch (config interface loopback 2)#
```

**Step 2.** Configure an IP address on the loopback interface. Run:

```
switch (config interface loopback 2)# ip address 20.20.20.20 /32
```

**Step 3.** Verify loopback interface configuration. Run:

```
switch (config interface loopback 2)# show interfaces loopback 2

Loopback 2
  Internet Address: 20.20.20.20/32
  Broadcast address: 20.20.20.20
  MTU: 1500 bytes
  Description: my-loopback
switch (config) #
```

#### 6.1.1.3 Configuring a Router Port Interface

**Step 1.** Enter an Ethernet interface's configuration context. Run:

```
switch (config)# interface ethernet 1/10
switch (config interface ethernet 1/10) #
```

**Step 2.** Configure the Ethernet interface to become an router port interface. Run:

```
switch (config interface ethernet 1/10) # no switchport force
```

**Step 3.** Configure an IP address on the router port interface. Run:

```
switch (config interface ethernet 1/10) # ip address 100.100.100.100 /24
```

**Step 4.** Verify router port interface configuration. Run:

```
switch (config interface ethernet 1/10) # show interfaces ethernet 1/10

Eth1/10
  Admin state: Enabled
  Operational state: Down
  Description: N\A
  Mac address: 00:02:c9:96:c6:d8
  MTU: 1500 bytes(Maximum packet size 1522 bytes)
  Flow-control: receive off send off
  Actual speed: 40 Gbps
  Width reduction mode: disabled
  DHCP client: Disabled
  IP Address: 100.100.100.100 /24
  Broadcast address: 100.100.100.255
  Arp timeout: 1500 seconds
  VRF: default
  MAC learning mode: Enabled
  Last clearing of "show interface" counters : 00:00:01
  60 seconds ingress rate: 0 bits/sec, 0 bytes/sec, 0 packets/sec
  60 seconds egress rate: 0 bits/sec, 0 bytes/sec, 0 packets/sec
```

Rx	0 packets
	0 unicast packets
	0 multicast packets
	0 broadcast packets
	0 bytes
	0 error packets
	0 discard packets
Tx	0 packets
	0 unicast packets
	0 multicast packets
	0 broadcast packets
	0 bytes
	0 discard packets

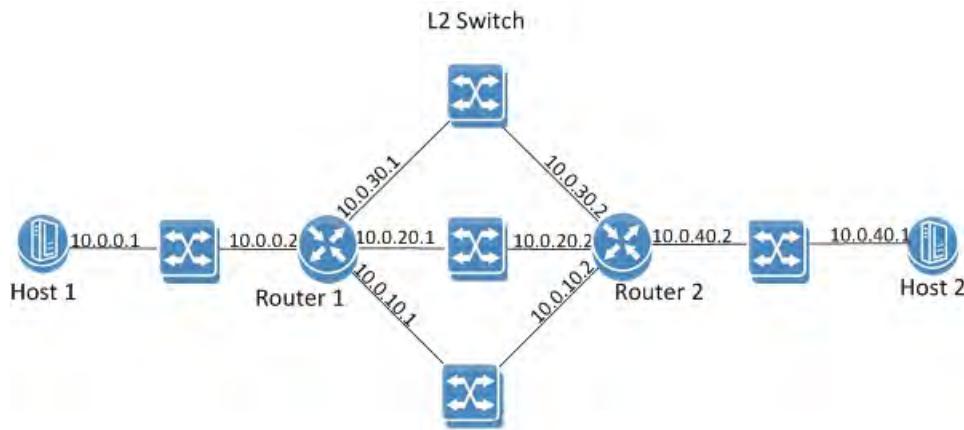
### 6.1.2 Equal Cost Multi-Path Routing (ECMP)

Equal-cost multi-path routing (ECMP) is a routing strategy where next-hop packet forwarding to a single destination can occur over multiple paths.

In Figure 35, routers R1 and R2 can both access each of their router peer networks. Router R1 routing table for 10.0.40/24 will contain the following routes:

- 10.0.10.2
- 10.0.20.2
- 10.0.30.2

**Figure 35: ECMP**



The load balancing function of the ECMP is configured globally on the system.

Hash algorithm can be symmetric or asymmetric. In symmetric hash functions bidirectional flows between routes will follow the same path, while in asymmetric hash functions, bidirectional traffic can follow different paths in both directions.

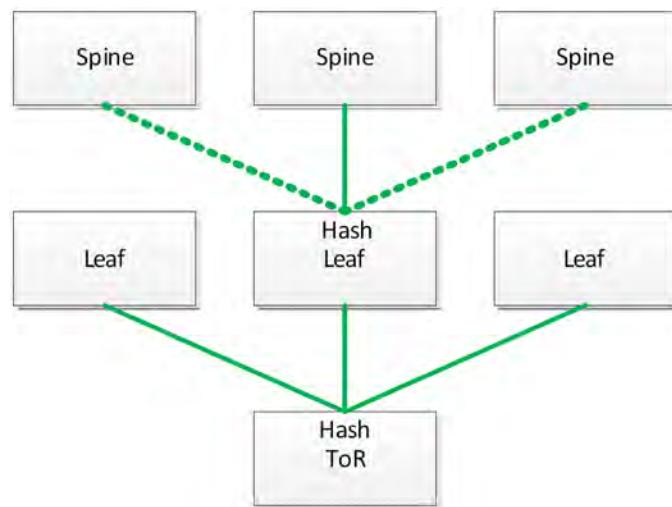
The following load balancing types are supported:

- Source IP & Port – source IP (SIP) and source UDP/TCP port: If the packet is not UDP/TCP, only SIP is used for the hash calculation. This is an asymmetric hash function.
- Destination IP & Port – destination IP (DIP) and destination UDP/TCP port: If the packet is not UDP/TCP, only DIP is used for the hash calculation. This is an asymmetric hash function.
- Source and Destination IP & Port – destination and source IP, as well as destination and source UDP/TCP port: If the packet is not UDP/TCP, only SIP/DIP are used for the hash calculation. This is a symmetric hash function.
- Traffic Class – Load balance based on the traffic class assigned to the packet. This is an asymmetric hash function.
- All (default) – all above fields are part of the hash calculations. This is a symmetric hash function.

#### 6.1.2.1 Hash Functions

It is advised that LAG and ECMP hash function configuration over more than one hop is different. If the same hash function is used over two hops, all the traffic sorted from one hop to following one will arrive already having the same characteristics, which will render the next hash function useless. For example, configure load-balancing on the first hop based on source IP while on the next hop based on destination IP.

**Figure 36: Multiple Hash Functions**



### 6.1.3 Virtual Routing and Forwarding



Only static IPv4 and ECMP are supported with VRF.

Virtual routing and forwarding (VRF) allows multiple routing table instances to coexist within the same router simultaneously. Since the routing instances are independent, IP addresses on each routing table may overlap without conflicting with each other.

VRF can be used for the following purposes:

- Ensure customer privacy and security
- Separate between management and user data
- Support customers with the same address space
- Support VPN

Multiple routing instances defined in the router can have different purposes and can be configured in different manners:

- Different IP interfaces can be attached to different VRFs (only one IP interface can be in a single VRF)
- Routing in VRF can be enabled or disabled
- Each VRF component can run its own routing protocol independently from other instances
- Differently configured IPv4 and IPv6 services

The first VRF in the system is created automatically and it is called “default” VRF. It cannot be deleted or configured.

## 6.1.4 Commands

### 6.1.4.1 General

#### ip l3

**ip l3 [force]**  
**no ip l3 [force]**

Enables IP routing capabilities.

The no form of the command disables IP routing and removes its configuration.

<b>Syntax Description</b>	N/A
<b>Default</b>	If operating with Ethernet system profile: L3
<b>Configuration Mode</b>	Config
<b>History</b>	3.4.1802
<b>Role</b>	admin
<b>Example</b>	<pre>switch (config) # ip l3 force switch (config) #</pre>
<b>Related Commands</b>	N/A
<b>Note</b>	

## vrf definition

**vrf definition <vrf-name>**

Creates the VRF.

<b>Syntax Description</b>	vrf-name	VRF session name
<b>Default</b>	N/A	
<b>Configuration Mode</b>	Config	
<b>History</b>	3.4.2008	
<b>Role</b>	admin	
<b>Example</b>	<pre>switch (config) # vrf definition my-vrf switch (config vrf definition my-vrf) #</pre>	
<b>Related Commands</b>	N/A	
<b>Notes</b>	Only 1 VRF is supported aside from the default VRF	

## routing-context vrf

**routing-context vrf <vrf-name>**

Enters the active-context of the specified session.

<b>Syntax Description</b>	vrf-name	VRF session name
<b>Default</b>	N/A	
<b>Configuration Mode</b>	Config	
<b>History</b>	3.4.2008	
<b>Role</b>	admin	
<b>Example</b>	<pre>switch (config) # routing-context vrf my-vrf switch (config) #</pre>	
<b>Related Commands</b>	N/A	
<b>Notes</b>	<ul style="list-style-type: none"><li>If a routing-context is configured, the user does not have to explicitly specify the VRF name parameter in this or any other VRF command</li><li>If no routing-context is configured and the user does not specify the VRF name, default VRF is used</li></ul>	

## ip routing

**ip routing [vrf <vrf-name>]**

Enables L3 forwarding between high speed interfaces.

<b>Syntax Description</b>	vrf-name	VRF session name
<b>Default</b>	N/A	
<b>Configuration Mode</b>	Config	
<b>History</b>	3.4.1802	
	3.4.2008	Added VRF parameter
<b>Role</b>	admin	
<b>Example</b>	switch (config) # ip routing vrf my-vrf switch (config) #	
<b>Related Commands</b>	N/A	
<b>Notes</b>	<ul style="list-style-type: none"><li>RD must be configured to enable IP routing on the VRF</li><li>If no routing-context is specified, the “routing-context” VRF is automatically configured.</li></ul>	

## description

**description <description>**  
**no description force**

Creates the VRF.

<b>Syntax Description</b>	description	Text string
	force	Forces deletion (no confirmation needed if configuration exists inside the VRF)
<b>Default</b>	N/A	
<b>Configuration Mode</b>	Config VRF Definition	
<b>History</b>	3.4.2008	
<b>Role</b>	admin	
<b>Example</b>	<pre>switch (config vrf definition my-vrf) # description vrf-description switch (config vrf definition my-vrf) #</pre>	
<b>Related Commands</b>	N/A	
<b>Notes</b>		

## rd

**rd [<ip addr>:<0-65,535> | <AS Number>:<0-4,294,967,295> | <AS Number>:<ip addr>]**

Adds a route distinguisher (RD) to the VRF configuration mode.

<b>Syntax Description</b>	ip-addr AS Number	IPv4 address Asynchronous machine number
<b>Default</b>	N/A	
<b>Configuration Mode</b>	Config VRF Definition	
<b>History</b>	3.4.2008	
<b>Role</b>	admin	
<b>Example</b>	<pre>switch (config vrf definition my-vrf) # rd 10.10.10.10:2 switch (config vrf definition my-vrf) #</pre>	
<b>Related Commands</b>	N/A	
<b>Notes</b>	<ul style="list-style-type: none"> <li>RDs internally identify routes belonging to a VRF to distinguish overlapping or duplicate IP address ranges. This allows the creation of distinct routes to the same IP address for different VPNs. The RD is a 64-bit number made up of an AS number or IPv4 address followed by a user-selected ID number. Once an RD has been assigned to a VRF it cannot be changed. To change the RD, remove the VRF then create it again. VRF is not active until an RD is defined.</li> <li>An RD must be defined to enable IP routing on the VRF</li> </ul>	

## vrf forwarding

**vrf forwarding <vrf-name>**

Maps an interface to VRF.

<b>Syntax Description</b>	vrf-name	VRF session name
<b>Default</b>	N/A	
<b>Configuration Mode</b>	Config Interface Ethernet set as router port interface Config Interface VLAN Config Interface Loopback	
<b>History</b>	3.4.2008	
<b>Role</b>	admin	
<b>Example</b>	switch (config interface ethernet 1/2) # vrf forwarding my-vrf switch (config interface ethernet 1/2) #	
<b>Related Commands</b>	N/A	
<b>Notes</b>		

## show ip routing

**show ip routing [vrf <vrf-name> | all]**

Displays IP routing information per VRF.

<b>Syntax Description</b>	vrf	Displays information for specific VRF
	all	Displays information on all VRFs
<b>Default</b>	N/A	
<b>Configuration Mode</b>	Any Command Mode	
<b>History</b>	3.2.0230	
	3.4.2008	Added VRF parameter
<b>Role</b>	admin	
<b>Example</b>	<pre>switch (config) # show ip routing vrf all  VRF Name:      my-vrf ----- IP routing: disabled  VRF Name:      default ----- IP routing: enabled switch (config) #</pre>	
<b>Related Commands</b>	N/A	
<b>Notes</b>	If no routing-context is specified, the “routing-context” VRF is automatically displayed.	

## show routing-context vrf

**show routing-context vrf**

Displays VRF active context.

<b>Syntax Description</b>	N/A
<b>Default</b>	N/A
<b>Configuration Mode</b>	Any Command Mode
<b>History</b>	3.4.2008
<b>Role</b>	admin
<b>Example</b>	<pre>switch (config) # show routing-context vrf VRF active context: my-vrf switch (config) #</pre>
<b>Related Commands</b>	N/A
<b>Notes</b>	

## show vrf

**show vrf [<vrf-name> | all]**

Displays VRF information.

<b>Syntax Description</b>	all vrf-name	Displays information for all VRF instances Name of VRF instance
<b>Default</b>	N/A	
<b>Configuration Mode</b>	Any Command Mode	
<b>History</b>	3.4.2008	
<b>Role</b>	admin	
<b>Example</b>	<pre>switch (config) # show vrf my-vrf  VRF Info   Name: my-vrf   RD: 10.10.10.10:2   Description: Test VRF   IP routing state: Enabled    Protocols: IPv4    Interfaces: Eth1/2 switch (config) #</pre>	
<b>Related Commands</b>	N/A	
<b>Notes</b>	If no routing-context is specified, the “routing-context” VRF is automatically displayed.	

### 6.1.4.2 IP Interfaces

#### switchport

**switchport [force]**  
**no switchport [force]**

Configures the Ethernet interface as a regular switchport.  
The no form of the command configures the Ethernet interface as router port interface.

<b>Syntax Description</b>	force	Forces configuration even if the interface's admin state is enabled.
<b>Default</b>	N/A	
<b>Configuration Mode</b>	Config Interface Ethernet Config Interface Port Channel	
<b>History</b>	3.3.5200	
	3.6.4006	Added storm-control support
<b>Role</b>	admin	
<b>Example</b>	<pre>switch (config interface ethernet 1/10)# no switchport force error message is case storm-control is configured on port: % interface * has storm control configuration. Please remove it first</pre>	
<b>Related Commands</b>		
<b>Note</b>	When storm-control is configured on port, an err-msg will appear. Force command deletes all storm-control configuration from port.	

## encapsulation dot1q vlan

```
encapsulation dot1q vlan <vlan-id> [force]
no encapsulation dot1q vlan [force]
```

Enables L2 802.1Q encapsulation of traffic on a specified router port interface in a VLAN.

The no form of the command disables L2 802.1Q encapsulation of traffic on a specified router port interface in a VLAN.

<b>Syntax Description</b>	vlan-id	Enables L2 802.1Q encapsulation of traffic on a router port interface in a VLAN
	force	Forces admin state down
<b>Default</b>	N/A	
<b>Configuration Mode</b>	Config Interface Ethernet	
<b>History</b>	3.3.5200	
<b>Role</b>	admin	
<b>Example</b>	switch (config interface ethernet 1/10)# encapsulation dot1q vlan 10	
<b>Related Commands</b>		
<b>Note</b>		

### 6.1.4.3 Interface VLAN

#### interface vlan

```
interface vlan <vlan-id>
no interface vlan <vlan-id>
```

Creates a VLAN interface and enters the interface VLAN configuration mode.  
The no form of the command deletes the VLAN interface.

<b>Syntax Description</b>	vlan-id	A numeric range of 1-4094
<b>Default</b>	N/A	
<b>Configuration Mode</b>	Config	
<b>History</b>	3.2.0230	
<b>Role</b>	admin	
<b>Example</b>	<pre>switch (config) # interface vlan 10 switch (config interface vlan 10) #</pre>	
<b>Related Commands</b>	<pre>ip routing vlan &lt;vlan-id&gt; switchport mode switchport access show interfaces vlan</pre>	
<b>Note</b>	<ul style="list-style-type: none"><li>• Make sure the VLAN was created, using the command “vlan &lt;vlan-id&gt;” in the global configuration mode</li><li>• The VLAN must be assigned to one of the L2 interfaces. To do so, run the command “switchport ...”</li><li>• At least one interface belong to that VLAN must be in UP state</li></ul>	

## interface vlan <id> no-autostate

[no] interface vlan <id> no-autostate

Disables the VLAN interface autostate such that its operational state remains up as long as its admin state is up, even if no port in the relevant VLAN egress-list is operationally up.

<b>Syntax Description</b>	vlan-id	A numeric range of 1-4094 or a range of VLANs.
<b>Default</b>	N/A	
<b>Configuration Mode</b>	Config	
<b>History</b>	3.6.4006	
<b>Role</b>	admin	
<b>Example</b>	<pre>switch (config) # interface vlan 10 no-autostate switch (config) # interface vlan 10-13 no-autostate</pre>	
<b>Related Commands</b>	show ip interface vlan <id>	
<b>Note</b>		

## ip address

**ip address <ip-address> <mask>**  
**no ip address <ip-address> <mask>**

Enters user-defined description for the interface.

<b>Syntax Description</b>	ip-address	IPv4 address
	mask	There are two possible ways to the mask: • /length (i.e. /24) • Network address (i.e. 255.255.255.0)
<b>Default</b>	0.0.0.0/0	
<b>Configuration Mode</b>	Config Interface VLAN	
<b>History</b>	3.2.0230	
<b>Role</b>	admin	
<b>Example</b>	<pre>switch (config interface vlan 10) # ip address 10.10.10.10 /24 switch (config interface vlan 10) #</pre>	
<b>Related Commands</b>	interface vlan show interfaces vlan	
<b>Note</b>		

## ip address dhcp

**ip address dhcp**  
**no ip address dhcp**

Enables DHCP on this VLAN interface.

<b>Syntax Description</b>	N/A
<b>Default</b>	Disabled
<b>Configuration Mode</b>	Config Interface VLAN
<b>History</b>	3.4.2008
<b>Role</b>	admin
<b>Example</b>	<pre>switch (config interface vlan 10) # ip address dhcp switch (config interface vlan 10) #</pre>
<b>Related Commands</b>	<a href="#">interface vlan</a> <a href="#">show interfaces vlan</a>
<b>Note</b>	

## counters

**counters**  
**no counters**

Enables counters on the IP interface.

The no form of the command disables counters gathering on the IP interface.

<b>Syntax Description</b>	N/A
<b>Default</b>	counters are disabled.
<b>Configuration Mode</b>	Config Interface VLAN
<b>History</b>	3.2.0230
<b>Role</b>	admin
<b>Example</b>	<pre>switch (config interface vlan 10) # counters switch (config interface vlan 10) #</pre>
<b>Related Commands</b>	counters interface vlan show interfaces vlan
<b>Note</b>	<ul style="list-style-type: none"><li>Enabling counters for the router interface adds delay to the traffic stream</li><li>There are maximum of 16 counter sets</li></ul>

## description

**description <string>**  
**no description**

Enters a description for the interface.  
The no form of the command sets the description to default.

<b>Syntax Description</b>	string	User defined string
<b>Default</b>	""	
<b>Configuration Mode</b>	Config Interface VLAN	
<b>History</b>	3.2.0230	
<b>Role</b>	admin	
<b>Example</b>	switch (config interface vlan 10) # description my-ip-interface switch (config interface vlan 10) #	
<b>Related Commands</b>	interface vlan show interfaces vlan	
<b>Note</b>		

## mtu

**mtu <size> [force]**  
**no mtu**

Sets the MTU for the interface.  
The no form of the command sets the MTU to default.

<b>Syntax Description</b>	size force	1500-9216. Forces command implementation.
<b>Default</b>	1522	
<b>Configuration Mode</b>	Config Interface VLAN	
<b>History</b>	3.2.0230	
<b>Role</b>	admin	
<b>Example</b>	switch (config interface vlan 10)# mtu 9216 switch (config interface vlan 10 #	
<b>Related Commands</b>	interface vlan show interfaces vlan	
<b>Note</b>		

## shutdown

**shutdown**  
**no shutdown**

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

<b>Syntax Description</b>	N/A
<b>Default</b>	The interface is enabled.
<b>Configuration Mode</b>	Config Interface VLAN
<b>History</b>	3.1.0000
<b>Role</b>	admin
<b>Example</b>	<pre>switch (config interface vlan 20) # shutdown switch (config interface vlan 20) #</pre>
<b>Related Commands</b>	interface vlan
<b>Note</b>	

## clear counters

### clear counters

Clears the interface counters.

<b>Syntax Description</b>	N/A
<b>Default</b>	N/A
<b>Configuration Mode</b>	Config Interface VLAN
<b>History</b>	3.2.0230
<b>Role</b>	admin
<b>Example</b>	<pre>switch (config interface vlan 10) # clear counters switch (config interface vlan 10) #</pre>
<b>Related Commands</b>	interface vlan counters
<b>Note</b>	

## ip icmp redirect

```
ip icmp redirect
no ip icmp redirect
```

Enables ICMP redirect.

The no form of the command disables ICMP redirect.

<b>Syntax Description</b>	N/A
<b>Default</b>	Enabled
<b>Configuration Mode</b>	Config Interface VLAN
<b>History</b>	3.4.0010
<b>Role</b>	admin
<b>Example</b>	<pre>switch (config interface vlan 10) # no ip icmp redirect</pre>
<b>Related Commands</b>	<pre>interface vlan counters</pre>
<b>Note</b>	<ul style="list-style-type: none"><li>ICMP redirect transmits messages to hosts alerting them about the existence of more efficient routes to a specific destination</li></ul>

## show ip interface

**show ip interface [vrf <vrf-name> | all] [brief]**

Displays IP interface information.

<b>Syntax Description</b>	vrf	Displays IP interface information per VRF
	all	Displays information on all VRF
	brief	Displays IP interfaces information in a shortened form
<b>Default</b>	N/A	
<b>Configuration Mode</b>	Any Command Mode	
<b>History</b>	3.4.2008	
	3.6.5000	Updated Example
<b>Role</b>	admin	
<b>Example</b>	<pre>switch (config) # show ip interface vrf all brief Interface      Address/Mask      Admin-state   Oper-state    MTU     VRF mgmt0          10.224.22.27/24  Enabled        Up           1500    default mgmt1          0.0.0.0/0        Enabled        Down          1500    default Vlan 20         20.20.20.1/24   Enabled        Down          1500    my-vrf Eth1/1          1.1.1.1/24      Enabled        Down          1500    my-vrf Loopback 10    10.10.10.1/32   Enabled        Up           1500    my-vrf Vlan 30         30.30.30.1/24   Enabled        Down          1500    default Eth1/2          2.2.2.2/24      Enabled        Down          1500    default Loopback 11    11.11.11.1/32   Enabled        Up           1500    default  switch (config) # show ip interface vrf my-vrf brief Interface      Address/Mask      Admin-state   Oper-state    MTU     VRF Vlan 20         20.20.20.1/24   Enabled        Down          1500    my-vrf Eth1/1          1.1.1.1/24      Enabled        Down          1500    my-vrf Loopback 10    10.10.10.1/32   Enabled        Up           1500    my-vrf  switch (config) # show ip interface vrf default brief Interface      Address/Mask      Admin-state   Oper-state    MTU     VRF mgmt0          10.224.22.27/24  Enabled        Up           1500    default mgmt1          0.0.0.0/0        Enabled        Down          1500    default Vlan 30         30.30.30.1/24   Enabled        Down          1500    default Eth1/2          2.2.2.2/24      Enabled        Down          1500    default Loopback 11    11.11.11.1/32   Enabled        Up           1500    default</pre>	

```
switch (config) # show ip interface 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
    Secondary address: 10.10.10.254/24 (alias: 'mgmt0:0')
    IPv6 enabled: yes
    Autoconf enabled: no
    Autoconf route: yes
    Autoconf privacy: no
    DHCPv6 running: no
    IPv6 addresses: 1
    IPv6 address:   fe80::202:c9ff:fe11:alb2/64
    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:
  15139846      bytes
  28452         packets
  0             discards
  0             errors
  0             overruns
  0             carrier
  0             collisions
  1000          queue len
```

---

**Related Commands**

N/A

---

**Notes**

If no routing-context is specified, the “routing-context” VRF is automatically displayed.

---

#### 6.1.4.4 Loopback Interface

##### interface loopback

```
interface loopback <id>
no interface loopback <id>
```

Creates a loopback interface and enters the interface configuration mode.  
The no form of the command deletes the interface.

<b>Syntax Description</b>	id	A numeric range of 0-31
<b>Default</b>	N/A	
<b>Configuration Mode</b>	Config	
<b>History</b>	3.2.3000	
<b>Role</b>	admin	
<b>Example</b>	<pre>switch (config) # interface loopback 10 switch (config interface loopback 10) #</pre>	
<b>Related Commands</b>		
<b>Note</b>	<ul style="list-style-type: none"><li>Up to 32 loopback interfaces can be configured</li><li>Within the loopback configuration mode, you can configure description and ip-address</li><li>MTU cannot be configured on the loopback interface</li></ul>	

## ip address

```
ip address <ip-address> <mask>
no ip address <ip-address> <mask>
```

Enters user-defined description for the interface.

<b>Syntax Description</b>	ip-address	IPv4 address.
	mask	There are two possible ways to the mask: <ul style="list-style-type: none"><li>• /length – only /32 is possible</li><li>• Network address (i.e. 255.255.255.0)</li></ul>
<b>Default</b>	0.0.0.0/0	
<b>Configuration Mode</b>	Config Interface Loopback	
<b>History</b>	3.3.5006	
<b>Role</b>	admin	
<b>Example</b>	switch (config interface loopback 10) # ip address 10.10.10.10 /32	
<b>Related Commands</b>	interface loopback	
<b>Note</b>		

## description

**description <string>**  
**no description**

Enters a description for the interface.  
The no form of the command sets the description to default.

<b>Syntax Description</b>	string	User defined string.
<b>Default</b>	""	
<b>Configuration Mode</b>	Config Interface Loopback	
<b>History</b>	3.3.5006	
<b>Role</b>	admin	
<b>Example</b>	switch (config interface loopback 10) # description my-ip-interface	
<b>Related Commands</b>	interface loopback	
<b>Note</b>		

## show interfaces loopback

**show interface loopback <id>**

Shows the attribute of the interface loopback.

<b>Syntax Description</b>	id	A numeric range of 1-32		
<b>Default</b>	N/A			
<b>Configuration Mode</b>	Config			
<b>History</b>	3.2.3000			
<b>Role</b>	admin			
<b>Example</b>	<pre>switch (config) # show interfaces loopback 2  Loopback 2   Internet Address: 2.2.2.2/32   Broadcast address: 2.2.2.2   MTU: 1500 bytes   Description: my-loopback switch (config) #</pre>			
<hr/>				
<b>Related Commands</b>				
<hr/>				
<b>Note</b>				
<hr/>				

#### 6.1.4.5 Routing and ECMP

##### ip route

```
ip route [vrf <vrf-name>] <ip-prefix> <netmask> {<next-hop-ip-address> |  
ethernet <port> | port-channel <id> | vlan <id> | null0} [<distance>]  
no ip route [vrf <vrf-name>] <ip-prefix> <netmask> [<next-hop-ip-address>]
```

Configures a static route inside VRF.

The no form of the command removes the static route configured.

<b>Syntax Description</b>	vrf-name	VRF session name
	ip-prefix	IP address
	netmask	There are two possible ways to input the mask: <ul style="list-style-type: none"> <li>• /&lt;length&gt; (e.g. /24)</li> <li>• Network address (e.g. 255.255.255.0)</li> </ul>
	distance	Administrative distance assigned to route. Options include: <ul style="list-style-type: none"> <li>• No parameter – route is assigned a default administrative distance of 1</li> <li>• 1-255 – the administrative distance assigned to route</li> </ul>
	next-hop-ip-address	IP address of the next hop
	null0	Sets a static drop-route
<b>Default</b>	N/A	
<b>Configuration Mode</b>	Config	
<b>History</b>	3.1.0000	
	3.4.2008	Added VRF parameter
<b>Role</b>	admin	
<b>Example</b>	switch (config) # ip route vrf my-vrf 80.80.80.0 /24 20.20.20.2	
<b>Related Commands</b>	N/A	
<b>Notes</b>	If no routing-context is specified, the “routing-context” VRF is automatically configured.	

## ip load-sharing

```
ip load-sharing <type>
no ip load-sharing
```

This command sets the ECMP load sharing mode.

The no form of the command sets the load-sharing to default.

<b>Syntax Description</b>	type	<ul style="list-style-type: none"><li>source-ip-port – source ip and TCP/UDP port</li><li>destination-ip-port – destination ip and TCP/UDP port</li><li>source-destination-ip-port – source &amp; destination ip and TCP/UDP port</li><li>traffic-class – traffic class</li><li>flow-label – flow label</li><li>all – all options</li></ul>
<b>Default</b>	all	
<b>Configuration Mode</b>	Config	
<b>History</b>	3.2.0230	
	3.5.1000	Added flow-label parameter and updated Note section
<b>Role</b>	admin	
<b>Example</b>	<pre>switch (config) # ip load-sharing all switch (config) # show ip load-sharing Load sharing: all switch (config)</pre>	
<b>Related Commands</b>	ip route	
<b>Note</b>	The parameter “traffic-class” is available on SwitchX® based systems only	

## show ip route

**show ip route [vrf <vrf-name> | all] [-a | static | summary]**

Displays routing table of VRF instance.

Syntax Description	all	Displays routing tables for all VRF instances
	-a	Displays static routes currently inactive due to the interface being down
	static	Displays static route
	summary	Displays route summary
Default	N/A	
Configuration Mode	Any Command Mode	
History	3.1.0000	
	3.3.3500	Added Distance/Metric column
	3.4.0000	Added -a parameter
	3.4.2008	Added VRF parameter
	3.4.3000	Updated Notes section
	3.6.4070	Added support for BFD and updated notes
	3.6.5000	Updated Example
Role	admin	

**Example**

```

switch (config) # show ip route vrf my-vrf
VRF Name: my-vrf
-----
Destination Mask Gateway Interface Source Distance/Metric
10.10.10.1 255.255.255.255 0.0.0.0 loopback10 direct 0/0
20.20.20.0 255.255.255.0 0.0.0.0 vlan20 direct 0/0
80.80.80.0 255.255.255.0 20.20.20.2 vlan20 static 1/0

switch (config) # show ip route vrf my-vrf static
Flags: F - Failed to install in H/W
VRF Name: default
-----
Flag Destination Mask Gateway Interface Source AD/M
-----
1.1.1.0 255.255.255.0 1.1.1.1 static 1/0

switch (config) # show ip route vrf my-vrf summary
VRF Name: default
-----
Route Source Routes
-----
direct 3
static 0
ospf 0
bgp 0
DHCP 1
Total 4

switch (config) # show ip route vrf my-vrf -a
VRF Name: my-vrf
-----
Destination Mask Gateway Interface Source Distance/Metric
90.90.90.0 255.255.255.0 1.1.1.2 NA static 1/0

```

**Related Commands**
**Notes**

## ip route

- If no routing-context is specified, the “routing-context” VRF is automatically displayed
- If no default route exists, then the message “Route not found” is printed
- route next hop is BFD controlled, status is viewable when <all> is inserted in the command, and it will be shown as follows:
  - If route is removed from routing decision it will be marked as “Active”
  - Protected next hops are marked with “B”
  - BFD protected failed/non active neighbors are marked with “BF”

## show ip route interface

**show ip route interface [vrf <vrf>] {ethernet <slot>/<port> | port-channel <lag> | vlan <vlan>}**

Displays routing table for specific interfaces.

<b>Syntax Description</b>	ethernet port-channel vlan	Displays routing table for Ethernet interfaces Displays routing table for LAG interfaces Displays routing table for VLAN interfaces
<b>Default</b>	N/A	
<b>Configuration Mode</b>	Any Command Mode	
<b>History</b>	3.4.2008 3.6.5000	Added VRF parameter Updated Example
<b>Role</b>	admin	
<b>Example</b>	<pre>switch (config) # show ip route interface vlan 10 VRF Name: default Total number of entries: 1  ----- Address          Type       Hardware Address      Interface ----- 15.0.0.2         Static ETH   DE:DE:BE:EF:DE:AD    vlan 10</pre>	
<b>Related Commands</b>	ip route	
<b>Notes</b>		

## show ip load-sharing

### show ip load-sharing

Displays ECMP hash attribute.

<b>Syntax Description</b>	N/A
<b>Default</b>	N/A
<b>Configuration Mode</b>	Any Command Mode
<b>History</b>	3.2.0230
<b>Role</b>	admin
<b>Example</b>	<pre>switch (config) # show ip load-sharing Load sharing: all switch (config) #</pre>
<b>Related Commands</b>	ip load-sharing
<b>Note</b>	

#### 6.1.4.6 Network to Media Resolution (ARP)

##### ip arp

```
ip arp [vrf <vrf-name>] <ip-address> <mac-address>
no ip arp <ip-address>
```

Configures IP ARP properties of VRF

The no form of the command deletes the static ARP configuration.

<b>Syntax Description</b>	vrf-name	VRF session name
	IP address	IPv4 address
	mac-address	MAC address (format XX:XX:XX:XX:XX:XX)
<b>Default</b>	N/A	
<b>Configuration Mode</b>	Config	
<b>History</b>	3.4.2008	
<b>Role</b>	admin	
<b>Example</b>	switch (config) # ip arp vrf my-vrf 20.20.20.2 aa:bb:cc:dd:ee:ff	
<b>Related Commands</b>	N/A	
<b>Notes</b>	If no routing-context is specified, the “routing-context” VRF is automatically configured.	

## ip arp timeout

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

Sets the dynamic ARP cache timeout.

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

<b>Syntax Description</b>	timeout-value	Time (in seconds) that an entry remains in the ARP cache. Range: 240-28800.
<b>Default</b>	1500 seconds	
<b>Configuration Mode</b>	Config Interface Ethernet Config Interface VLAN Config Interface Port Channel	
<b>History</b>	3.2.0230	
	3.5.1000	Updated Note section
<b>Role</b>	admin	
<b>Example</b>	switch (config) # ip arp timeout 2000	
<b>Related Commands</b>	ip arp show ip arp	
<b>Note</b>	<ul style="list-style-type: none"><li>This configuration may take up to 5 minutes to take effect</li><li>The time interval after which each ARP entry becomes stale may actually vary from 50-150% of the configured value</li></ul>	

## clear ip arp

**clear ip arp [vrf <vrf-name>] [interface <type> | <IP-address>]**

Clears the dynamic ARP cache for the specific VRF session.

<b>Syntax Description</b>	vrf-name	VRF session name
	interface	Clears dynamic ARP entries for a interface
	ip-address	Clears dynamic ARP entries for a specific IP address
<b>Default</b>	N/A	
<b>Configuration Mode</b>	Config	
<b>History</b>	3.2.0230	
<b>History</b>	3.4.2008	Added VRF parameter
<b>Role</b>	admin	
<b>Example</b>	switch (config) # clear ip arp vrf my-vrf	
<b>Related Commands</b>	ip arp show ip arp	
<b>Notes</b>	If no routing-context is specified, the “routing-context” VRF is automatically configured.	

## show ip arp

**show ip arp [vrf <vrf-name> | all] [interface <type> | count]**

Displays all ARP information for VRF instance.

<b>Syntax Description</b>	all	Displays all ARP information for all VRF
	interface	Displays all ARP information for specific interface
	count	Displays number of ARPs for specific VRF
<b>Default</b>	N/A	
<b>Configuration Mode</b>	Any Command Mode	
<b>History</b>	3.3.3000 3.4.2008                          Added VRF parameter 3.6.5000                           Updated example output	
<b>Role</b>	admin	
<b>Example</b>	<pre>switch (config) # show ip arp vrf my-vrf interface vlan 20 VRF Name:           default Total number of entries: 1  ----- Address          Type       Hardware Address      Interface ----- 15.0.0.2         Static ETH   DE:DE:BE:EF:DE:AD    vlan 10</pre>	
<b>Related Commands</b>	ip arp	
<b>Notes</b>	If no routing-context is specified, the “routing-context” VRF is automatically displayed.	

#### **6.1.4.7 IP Diagnostic Tools**

ping

```
ping [vrf <vrf-name>] [-LRUbfqnvVaA] [-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

<b>Syntax Description</b>	Linux Ping options	
vrf	Specifies VRF instance name	
<b>Default</b>	N/A	
<b>Configuration Mode</b>	Config	
<b>History</b>	3.1.0000 3.4.2008                                  Added VRF parameter	
<b>Role</b>	admin	
<b>Example</b>	<pre>switch (config) # ping 172.30.2.2 PING 172.30.2.2 (172.30.2.2) 56(84) bytes of data. 64 bytes from 172.30.2.2: icmp_seq=1 ttl=64 time=0.703 ms 64 bytes from 172.30.2.2: icmp_seq=2 ttl=64 time=0.187 ms 64 bytes from 172.30.2.2: icmp_seq=3 ttl=64 time=0.166 ms 64 bytes from 172.30.2.2: icmp_seq=4 ttl=64 time=0.161 ms 64 bytes from 172.30.2.2: icmp_seq=5 ttl=64 time=0.153 ms 64 bytes from 172.30.2.2: icmp_seq=6 ttl=64 time=0.144 ms ^C --- 172.30.2.2 ping statistics --- 6 packets transmitted, 6 received, 0% packet loss, time 5004ms rtt min/avg/max/mdev = 0.144/0.252/0.703/0.202 ms switch (config) #</pre>	
<b>Related Commands</b>	traceroute	
<b>Note</b>	When using -I option use the interface name + interface number, for example “ping -I vlan10”	

## traceroute

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

-l	Uses specified flow_label for IPv6 packets.
-w	Sets the number of seconds to wait for response to a probe (default is 5.0). Non-integer (float point) values allowed too.
-q	Sets the number of probes per each hop. Default is 3.
-s	Uses source src_addr for outgoing packets.
-z	Sets minimal time interval between probes (default is 0). If the value is more than 10, then it specifies a number in milliseconds, else it is a number of seconds (float point values allowed too).

### **Related Commands**

- Note**

  - The following flags are not supported: -6, -l, -A
  - When using -i option use the interface name + interface number, for example “traceroute -i wlan10”

## tcpdump

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

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

<b>Syntax Description</b>	vrf	Specifies VRF instance name
<b>Default</b>	N/A	
<b>Configuration Mode</b>	Config	
<b>History</b>	3.1.0000	
	3.4.2008	Added VRF parameter
<b>Role</b>	admin	
<b>Example</b>	<pre>switch (config) # tcpdump ..... 09:37:38.678812 IP 192.168.10.7.ssh &gt; 192.168.10.1.54155: P 1494624:1494800(176) ack 625 win 90 &lt;nop,nop,timestamp 5842763 858672398&gt; 09:37:38.678860 IP 192.168.10.7.ssh &gt; 192.168.10.1.54155: P 1494800:1495104(304) ack 625 win 90 &lt;nop,nop,timestamp 5842763 858672398&gt; ... 9141 packets captured 9142 packets received by filter 0 packets dropped by kernel switch (config) #</pre>	
<b>Related Commands</b>	N/A	
<b>Note</b>	<ul style="list-style-type: none"> <li>When using -i option use the interface name + interface number, for example “tcpdump -i vlan10”</li> <li>For all flag options of this command refer to the linux ‘man page’ of tcp dump.</li> </ul>	

### 6.1.4.8 QoS

#### **qos map dscp-to-pcp preserve-pcp**

```
qos map dscp-to-pcp preserve-pcp
no qos map dscp-to-pcp preserve-pcp
```

Configures the router to copy PCP bits when transferring data from one subnet to another.

The no form of the command disables this ability.

<b>Syntax Description</b>	N/A
<b>Default</b>	Disabled.
<b>Configuration Mode</b>	Config
<b>History</b>	3.3.4000
<b>Role</b>	admin
<b>Example</b>	<pre>switch (config) # qos map dscp-to-pcp preserve-pcp switch (config) #</pre>
<b>Related Commands</b>	
<b>Note</b>	

## 6.2 IPv6



IPv6 is supported on Mellanox Spectrum™ based switch systems only.

IP version 6 (IPv6) is a routing protocol which succeeds IPv4. With the expansion of the Internet and data bases IPv6 addresses consist of 128 bits whose purpose is to allow networks to include a significantly higher number of nodes by increasing the pool of available unique IP addresses. IPv6 packets alleviate overhead and allow for future customizability.

Textual representations of IPv6 addresses consist of 128 bits made up from eight 16-bit hexadecimal numbers separated by colons. IPv6 addresses may be abbreviated as follows:

- You may omit leading zeros in each 16-bit sequence
- You may replace an entire sequence with a double colon if it equals zero

For example, these addresses represent the same IPv6 address:

- af23:0000:0000:0000:1284:037d:35ce:2401
- af23:0:0:0:1284:37d:35ce:2401
- af23::1284:37d:35ce:2401

IPv6 addresses typically denote a 64-bit network prefix and a 64-bit host address.

### 6.2.1 Neighbor Discovery Protocol

Neighbor Discovery (ND) decides relationships between neighbors and replaces ARP, ICMP, and ICMP redirect in IPv4.

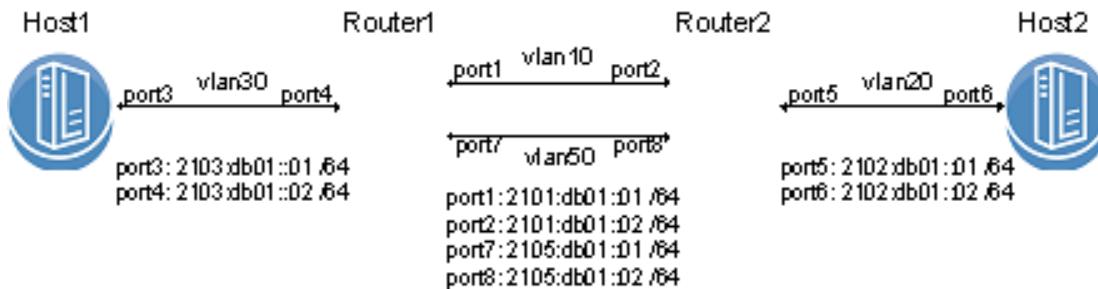
Five kinds of ICMPv6 packets are defined by ND:

- Neighbor advertisement
- Router advertisement
- Neighbor solicitation
- Router solicitation
- Redirect

ND checks whether a neighboring node's address has changed, whether the neighbor is still reachable, and also resolves the address of the neighbor which a packet is being forwarded to. ND is also useful for network nodes for discovering other nodes and performing basic link-layer configuration.

## 6.2.2 Configuring IPv6

**Figure 37: IPv6 Network**



➤ **To configure Router1:**

- Step 1.** Enable IP routing. Run:

```
switch (config)# ip routing
```

- Step 2.** Enable forwarding IPv6 unicast packets. Run:

```
switch (config)# ipv6 routing
```

- Step 3.** Configure the VLAN interfaces. Run:

```
switch (config)# interface vlan 10
switch (config interface vlan 10) # exit
switch (config)# interface vlan 30
switch (config interface vlan 30) # exit
switch (config)# interface vlan 50
switch (config interface vlan 50) # exit
```

- Step 4.** Enable IPv6 on the VLAN interfaces. Run:

```
switch (config)# interface vlan 10 ipv6 enable
switch (config)# interface vlan 30 ipv6 enable
switch (config)# interface vlan 50 ipv6 enable
```

- Step 5.** Configure IPv6 addresses for each one of the VLAN interfaces. Run:

```
switch (config)# interface vlan 10 ipv6 address 2101:db01::1 /64
switch (config)# interface vlan 30 ipv6 address 2103:db01::2 /64
switch (config)# interface vlan 50 ipv6 address 2105:db01::1 /64
```

- Step 6.** Configure IPv6 unicast. Run:

```
switch (config)# ipv6 route 2002:db01:: /64 2101:db01::2
```

- Step 7.** Configure IPv6 unicast. Run:

```
switch (config)# ipv6 route 2002:db01:: /64 2105:db01::2
```

➤ **To configure Router2:**

**Step 1.** Disable prefix mode on the CLI. Run:

```
switch (config)# no cli default prefix-mode enable
```

**Step 2.** Enable the VLANs on the system. Run:

```
switch (config)# vlan 10
switch (config vlan 10) # exit
switch (config)# vlan 20
switch (config vlan 20) # exit
switch (config)# vlan 50
switch (config vlan 50) # exit
```

**Step 3.** Configure the switch ports to accept the VLANs of which they are part only. Run:

```
switch (config)# interface ethernet 1/1 switchport access vlan 10 // port2
switch (config)# interface ethernet 1/2 switchport access vlan 50 // port8
switch (config)# interface ethernet 1/36 switchport access vlan 20 // port5
```

**Step 4.** Disable spanning tree. Run:

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

**Step 5.** Enable forwarding IPv6 unicast packets. Run:

```
switch (config)# ipv6 routing
```

**Step 6.** Configure the VLAN interfaces. Run:

```
switch (config)# interface vlan 10
switch (config interface vlan 10) # exit
switch (config)# interface vlan 20
switch (config interface vlan 20) # exit
switch (config)# interface vlan 50
switch (config interface vlan 50) # exit
```

**Step 7.** Configure IPv6 addresses for each one of the VLAN interfaces. Run:

```
switch (config)# interface vlan 10 ipv6 address 2101:db01::2 /64
switch (config)# interface vlan 20 ipv6 address 2102:db01::1 /64
switch (config)# interface vlan 50 ipv6 address 2105:db01::2 /64
```

**Step 8.** Configure IPv6 unicast. Run:

```
switch (config)# ipv6 route 2103:db01:: /64 2101:db01::1
```

**Step 9.** Configure IPv6 unicast. Run:

```
switch (config)# ipv6 route 2103:db01:: /64 2105:db01::1
```

➤ **Ping neighbor to verify IPv6 configuration:**

```
switch (config)# ping6 2101:db01::2
PING 2101:db01::2(2101:db01::2) 56 data bytes
64 bytes from 2101:db01::2: icmp_seq=1 ttl=64 time=0.371 ms
64 bytes from 2101:db01::2: icmp_seq=2 ttl=64 time=0.620 ms
64 bytes from 2101:db01::2: icmp_seq=3 ttl=64 time=0.192 ms
64 bytes from 2101:db01::2: icmp_seq=4 ttl=64 time=0.277 ms
64 bytes from 2101:db01::2: icmp_seq=5 ttl=64 time=0.231 ms
```

### 6.2.3 Commands

## ipv6 enable

**ipv6 enable**  
**no ipv6 enable**

Assigns automatic link-local IPv6 address to the interface.

The `no form` of the command deassigns that automatic local address and disables IPv6 if no static IPv6 address has been assigned to the interface.

<b>Syntax Description</b>	N/A
<b>Default</b>	Unassigned
<b>Configuration Mode</b>	Config Interface VLAN Config Interface Loopback Config Interface Ethernet configured as a router port interface Config Interface Port Channel configured as a router port interface
<b>History</b>	3.4.1100  3.6.4110 Updated notes and command description.
<b>Role</b>	admin
<b>Example</b>	switch (config vlan 10) # ipv6 enable
<b>Related Commands</b>	
<b>Note</b>	<ul style="list-style-type: none"><li>Assigning an IPv6 address to an interface also enables IPv6 processing on the interface.</li></ul>

## ipv6 address

**ipv6 address <ipv6-address> /<length>**  
**no ipv6 address [<ipv6-address> [/<length>]]**

Enables IPv6 processing and assigns an IPv6 address to the interface.  
The no form of the command removes the specified IPv6 address.

<b>Syntax Description</b>	ipv6-address length	IPv6 address. Mask length for the associated address space. Range: 1-128.
<b>Default</b>	N/A	
<b>Configuration Mode</b>	Config Interface VLAN Config Interface Loopback Config Interface Ethernet configured as a router port interface Config Interface Port Channel configured as a router port interface	
<b>History</b>	3.4.1100 3.6.4110	Updated syntax description and example output.
<b>Role</b>	admin	
<b>Example</b>	switch (config vlan 10) # ipv6 address 2001::1 /120 switch (config vlan 10) # ipv6 address 2001::1/120	
<b>Related Commands</b>		
<b>Note</b>	<ul style="list-style-type: none"> <li>An interface can have up to 16 IPv6 address assignments</li> <li>If the no command does not include a specific address, all address assignments are removed from the interface</li> <li>The mask length may be configured without a space (i.e. &lt;ipv6-address&gt;/&lt;length&gt;)</li> </ul>	

## ipv6 nd managed-config-flag

**ipv6 nd managed-config-flag**  
**no ipv6 nd managed-config-flag**

Sets the managed address configuration flag in IPv6 router advertisements.  
The no form of the command restores the default setting.

<b>Syntax Description</b>	N/A
<b>Default</b>	Managed address configuration flag is not set
<b>Configuration Mode</b>	Config Interface VLAN Config Interface Ethernet configured as a router port interface Config Interface Port Channel configured as a router port interface
<b>History</b>	3.4.1100
	3.6.4110                          Updated configuration mode.
<b>Role</b>	admin
<b>Example</b>	switch (config vlan 10) # ipv6 nd managed-config-flag
<b>Related Commands</b>	
<b>Note</b>	

## ipv6 nd ns-interval

**ipv6 nd ns-interval <period>**  
**no ipv6 nd ns-interval**

Configures the interval between IPv6 neighbor solicitation (NS) transmissions.  
The no form of the command restores the default value.

<b>Syntax Description</b>	period	In milliseconds. Range: 1000-4294967295.		
<b>Default</b>	1000 milliseconds			
<b>Configuration Mode</b>	Config Interface VLAN Config Interface Ethernet configured as a router port interface Config Interface Port Channel configured as a router port interface			
<b>History</b>	3.4.1100			
	3.6.4110	Updated configuration mode.		
<b>Role</b>	admin			
<b>Example</b>	switch (config vlan 10) # ipv6 nd ns-interval 1500			
<b>Related Commands</b>				
<b>Note</b>				

## ipv6 nd other-config-flag

**ipv6 nd other-config-flag**  
**no ipv6 nd other-config-flag**

Indicates that other configuration information is available via DHCPv6.  
The no form of the command removes the other configuration flag.

<b>Syntax Description</b>	N/A
<b>Default</b>	Not set
<b>Configuration Mode</b>	Config Interface VLAN Config Interface Ethernet configured as a router port interface Config Interface Port Channel configured as a router port interface
<b>History</b>	3.4.1100
	3.6.4110                          Updated configuration mode.
<b>Role</b>	admin
<b>Example</b>	switch (config vlan 10) # ipv6 nd other-config-flag
<b>Related Commands</b>	
<b>Note</b>	

## ipv6 nd prefix

```
ipv6 nd prefix <ipv6-address> /<length> [no-autoconfig] [no-onlink] [valid-time {<time> | infinite}] [preferred-time {<time> | infinite}]
ipv6 nd prefix <prefix> no-advertise
no ipv6 nd prefix <prefix>
```

Configures inclusion for router advertisements (RAs) for neighbor.  
The no form of the command removes the corresponding IPv6 nd prefix.

<b>Syntax Description</b>	ipv6-address	IPv6 address.
	length	Prefix length for the associated address space. Range: 1-128.
	no-advertise	Prevents advertising of the specified default prefix.
	valid-time	Time in seconds. Range: 0-4294967295.
	preferred-time	Time in seconds. Range: 0-4294967295.
	no-autoconfig	Indicates that the prefix cannot be used for stateless address configuration.
	no-onlink	Indicates that the prefix cannot be used for on-link determination
<b>Default</b>	valid-time: 2592000 seconds preferred-time: 604800 seconds no-autoconfig: Reset, autoconfig enabled no-onlink: Reset, on-link determination is enabled	
<b>Configuration Mode</b>	Config Interface VLAN Config Interface Ethernet configured as a router port interface Config Interface Port Channel configured as a router port interface	
<b>History</b>	3.4.1100	
	3.6.4110	Updated syntax description, configuration mode and default values.
<b>Role</b>	admin	
<b>Example</b>	switch (config vlan 10) # ipv6 nd prefix 2001::1 /120	
<b>Related Commands</b>		
<b>Note</b>	<ul style="list-style-type: none"> <li>Valid time must be larger than preferred time</li> <li>By default, the router advertises all configured subnets on the interface</li> </ul>	

## ipv6 nd ra dns-servers lifetime

**ipv6 nd ra dns-servers lifetime {<time> | infinite}  
no ipv6 nd ra dns-servers lifetime**

Advertises a lifetime of a Recursive DNS Server (RDNSS).

Using RDNSS and DNSSL options, an IPv6 host can perform IPv6 address network configuration and DNS information simultaneously, without using DHCPv6 for the DNS configuration.

The no form of the command resets the lifetime value to default.

<b>Syntax Description</b>	time  infinite	Possible values: <ul style="list-style-type: none"> <li>• 0 - RDNSS address can no longer be used</li> <li>• 1-4294967295 (sec)</li> </ul> A value of all one bits (0xffffffff) and "infinite" represents infinity.
<b>Default</b>		If no lifetime period is configured on the interface, the default value is 1.5 times the Router Advertisement (RA) interval set by the command "ipv6 nd ra interval".
<b>Configuration Mode</b>		Config Interface VLAN Config Interface Ethernet configured as a router port interface Config Interface Port Channel configured as a router port interface
<b>History</b>	3.4.1100  3.6.4110	
		Updated command and syntax description, configuration mode and default values.
<b>Role</b>	admin	
<b>Example</b>	switch (config vlan 10) # ipv6 nd ra dns-servers lifetime infinite	
<b>Related Commands</b>		
<b>Note</b>	<ul style="list-style-type: none"> <li>• A lifetime value set for an individual RDNSS overrides this value.</li> <li>• The lifetime value is the maximum amount of time after a route advertisement packet is sent that the RDNSS referenced in the packet may be used for name resolution.</li> </ul>	

## ipv6 nd ra dns-server

```
ipv6 nd ra dns-server <ipv6 address> [lifetime [<time> | infinite]]
no ipv6 nd ra dns-server [<ipv6 address>]
```

Configures the IPv6 address of a Recursive DNS Server (RDNSS) to include in the neighbor-discovery router advertisements (RAs).

The no form of the command removes the RDNSS from the configuration.

<b>Syntax Description</b>	ipv6 address	IPv6 address of RDNSS
	lifetime	Maximum lifetime value for the specified RDNSS entry. Possible values: <ul style="list-style-type: none"> <li>• 0 - RDNSS address can no longer be used</li> <li>• 1-4294967295 in seconds</li> </ul>
	infinite	A value of all one bits (0xffffffff) and "infinite" represents infinity.
<b>Default</b>	If no lifetime period is configured on the interface, the default value is 1.5 times the Router Advertisement (RA) interval set by the command “ <code>ipv6 nd ra interval</code> ”.	
<b>Configuration Mode</b>	Config Interface VLAN Config Interface Ethernet configured as a router port interface Config Interface Port Channel configured as a router port interface	
<b>History</b>	3.4.1100	
	3.6.4110	Updated command, example and syntax description, configuration mode and default values.
<b>Role</b>	admin	
<b>Example</b>	<pre>switch (config vlan 10) # ipv6 nd ra dns-server 2001::1 lifetime infinite</pre>	
<b>Related Commands</b>		
<b>Note</b>	<ul style="list-style-type: none"> <li>• Including RDNSS information in RAs provides DNS server configuration for connected IPv6 hosts without requiring DHCPv6</li> <li>• Multiple servers can be configured on the interface by using the command repeatedly</li> <li>• A lifetime value for the RDNSS can optionally be specified with this command, and overrides any default value configured for the interface using the <code>ipv6 nd ra dns-servers lifetime</code> command</li> </ul>	

## ipv6 nd ra dns-suffixes lifetime

**ipv6 nd ra dns-suffixes lifetime {<time> | infinite}**  
**no ipv6 nd ra dns-suffixes lifetime**

Advertises a lifetime of a DNS Search List (DNSSL).

Using RDNSS and DNSSL options, an IPv6 host can perform IPv6 address network configuration and DNS information simultaneously, without using DHCPv6 for the DNS configuration.

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

<b>Syntax Description</b>	time  infinite	Possible values: <ul style="list-style-type: none"> <li>• 0 – RDNSS address can no longer be used</li> <li>• 1-4294967295 – in seconds</li> </ul> A value of all one bits (0xffffffff) and "infinite" represents infinity.
<b>Default</b>		If no lifetime period is configured on the interface, the default value is 1.5 times the Router Advertisement (RA) interval set by the command “ <code>ipv6 nd ra interval</code> ”.
<b>Configuration Mode</b>		Config Interface VLAN Config Interface Ethernet configured as a router port interface Config Interface Port Channel configured as a router port interface
<b>History</b>	3.4.1100  3.6.4110	
		Updated command, example and syntax description, configuration mode and default values.
<b>Role</b>	admin	
<b>Example</b>		<code>switch (config vlan 10) # ipv6 nd ra dns-suffix mellanox.com lifetime infinite</code>
<b>Related Commands</b>		
<b>Note</b>		<ul style="list-style-type: none"> <li>• The DNSSL contains the domain names of DNS suffixes for IPv6 hosts to append to short, unqualified domain names for DNS queries</li> </ul>

## ipv6 nd ra dns-suffix

```
ipv6 nd ra dns-suffix <domain-name> [lifetime {<time> | infinite}]
no ipv6 nd ra dns-suffix [<domain-name>]
```

Creates a DNS search list (DNSSL) to include in the neighbor-discovery Router Advertisements (RAs).

The no form of the command removes the DNSSL from the configuration.

<b>Syntax Description</b>	domain-name	Domain suffix for IPv6 hosts to append to short unqualified domain names for DNS queries. The suffix must contain only alphanumeric characters, “.” (periods), “-” (hyphens), and must begin and end with an alphanumeric character.
	lifetime	Maximum lifetime value for the specified DNSSL entry.
	time	Possible values: • 0 – DNSSL must not be used for name resolution • 1-4294967295 – in seconds
	infinite	A value of all one bits (0xffffffff) and “infinite” represents infinity.
<b>Default</b>		If no lifetime period is configured on the interface, the default value is 1.5 times the Router Advertisement (RA) interval set by the command “ <code>ipv6 nd ra interval</code> ”.
<b>Configuration Mode</b>		Config Interface VLAN Config Interface Ethernet configured as a router port interface Config Interface Port Channel configured as a router port interface
<b>History</b>	3.4.1100	
	3.6.4110	Updated command, example and syntax description, configuration mode and default values.
<b>Role</b>	admin	
<b>Example</b>	<pre>switch (config vlan 10) # ipv6 nd ra dns-suffix mellanox.com lifetime infinite</pre>	
<b>Related Commands</b>		
<b>Note</b>	<ul style="list-style-type: none"> <li>The DNSSL contains the domain names of DNS suffixes for IPv6 hosts to append to short, unqualified domain names for DNS queries</li> <li>Multiple DNS domain names can be added to the DNSSL by reusing the command</li> <li>A lifetime value for the DNSSL can optionally be specified with this command which overrides any default value configured for the interface using the command “<code>ipv6 nd ra dns-suffixes lifetime</code>”</li> </ul>	

## ipv6 nd ra hop-limit

```
ipv6 nd ra hop-limit <limit>
no ipv6 nd ra hop-limit
```

Sets a suggested hop-limit value to be included in route advertisement (RA) packets.  
The no form of the command resets the parameter to its default value.

<b>Syntax Description</b>	limit	The hop-limit value to be included by attached hosts in outgoing packets. <ul style="list-style-type: none"><li>• 0 – unspecified (by this router)</li><li>• 1-255 – number of hops</li></ul>
<b>Default</b>	Limit value is 64	
<b>Configuration Mode</b>	Config Interface VLAN Config Interface Ethernet configured as a router port interface Config Interface Port Channel configured as a router port interface	
<b>History</b>	3.4.1100	
	3.6.4110	Updated configuration modes.
<b>Role</b>	admin	
<b>Example</b>	switch (config vlan 10) # ipv6 nd ra hop-limit 70	
<b>Related Commands</b>		
<b>Note</b>		

## ipv6 nd ra interval max-period

**ipv6 nd ra interval max-period <time> [min-period <time>]  
no ipv6 nd ra interval**

Configures the interval between IPv6 router advertisement (RA) transmissions.  
The no form of the command resets the parameter to its default value.

<b>Syntax Description</b>	time	Maximum interval between successive IPv6 router advertisement transmissions. Range: 4-1800 seconds.
	min-period	minimum interval between successive IPv6 router advertisement transmissions. <ul style="list-style-type: none"> <li>• No parameter: Default is used</li> <li>• 4-1800</li> </ul>
<b>Default</b>	max-period: 600 seconds min-period: See Note	
<b>Configuration Mode</b>	Config Interface VLAN Config Interface Ethernet configured as a router port interface Config Interface Port Channel configured as a router port interface	
<b>History</b>	3.4.1100  3.6.4110	Updated syntax description, configuration modes and notes.
<b>Role</b>	admin	
<b>Example</b>	switch (config vlan 10) # ipv6 nd ra interval max-period 600	
<b>Related Commands</b>		
<b>Note</b>	<ul style="list-style-type: none"> <li>• The min-period must be <math>0.33 * \text{&lt;max-period&gt;}</math> if <math>\text{&lt;max-period&gt;} \geq 9</math> seconds; otherwise, the default is Router Advertisement Interval</li> <li>• The parameter min-period must be no less than 3 seconds and no greater than <math>0.75 * \text{max-period}</math></li> </ul>	

## ipv6 nd ra lifetime

**ipv6 nd ra lifetime <time>**  
**no ipv6 nd ra lifetime**

Router lifetime is associated with a router's usefulness as default route, it does not apply to information contained in other message fields or options. Options that need time limits for their information include their own lifetime fields.

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

<b>Syntax Description</b>	time	The router lifetime specifies the period that the router can be considered as a default router by RA recipients in seconds. <ul style="list-style-type: none"> <li>• 0 – the router should not be considered a default router on this interface</li> <li>• 1-9000 – lifetime period advertised in RAs should not be less than the max router advertisement interval</li> </ul>
<b>Default</b>	3*<router advertisement interval>	
<b>Configuration Mode</b>		Config Interface VLAN Config Interface Ethernet configured as a router port interface Config Interface Port Channel configured as a router port interface
<b>History</b>	3.4.1100	
	3.6.4110	Added support for IPv6
<b>Role</b>	admin	
<b>Example</b>	switch (config vlan 10) # ipv6 nd ra lifetime 300	
<b>Related Commands</b>		
<b>Note</b>		

## ipv6 nd ra mtu suppress

**ipv6 nd ra mtu suppress**  
**no ipv6 nd ra mtu suppress**

Suppresses advertisement (RA) MTU option sent to router.  
MTU option ensures all nodes on a link use the same MTU value.  
The no form of the command restores the MTU option to enabled.

<b>Syntax Description</b>	N/A
<b>Default</b>	Suppressed
<b>Configuration Mode</b>	Config Interface VLAN Config Interface Ethernet configured as a router port interface Config Interface Port Channel configured as a router port interface
<b>History</b>	3.4.1100
	3.6.4110                          Updated command Syntax and configuration mode.
<b>Role</b>	admin
<b>Example</b>	switch (config vlan 10) # ipv6 nd ra mtu suppress
<b>Related Commands</b>	
<b>Note</b>	If not suppressed, MTU of the interface is advertised.

## ipv6 nd ra suppress

**ipv6 nd ra suppress [all]**  
**no ipv6 nd ra suppress**

Suppresses periodic and solicited IPv6 router advertisement (RA) transmissions.  
The no form of the command restores the transmission of RAs.

<b>Syntax Description</b>	all	Configures the switch to suppress all RAs, including those responding to a router solicitation.
<b>Default</b>	Only unsolicited RAs transmitted periodically are suppressed	
<b>Configuration Mode</b>	Config Interface VLAN Config Interface Ethernet configured as a router port interface Config Interface Port Channel configured as a router port interface	
<b>History</b>	3.4.1100	
	3.6.4110	Updated command syntax and configuration mode.
<b>Role</b>	admin	
<b>Example</b>	switch (config vlan 10) # ipv6 nd ra suppress all	
<b>Related Commands</b>		
<b>Note</b>		

## ipv6 nd reachable-time

**ipv6 nd reachable-time <time>**  
**no ipv6 nd reachable-time**

Sets the time period the switch includes in the reachable time field of out-going advertisements (RAs).

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

<b>Syntax Description</b>	time	In milliseconds; the reachable time defines the period that a node assumes a neighbor is reachable after having received a reachability confirmation. Values: <ul style="list-style-type: none"> <li>• 0 - unspecified by router</li> <li>• 1 - 3600000 the period that a node assumes a neighbor is reachable.</li> </ul>
<b>Default</b>	0 (unspecified)	
<b>Configuration Mode</b>	Config Interface VLAN Config Interface Ethernet configured as a router port interface Config Interface Port Channel configured as a router port interface	
<b>History</b>	3.4.1100  3.6.4110	Updated command syntax, configuration mode and notes.
<b>Role</b>	admin	
<b>Example</b>	switch (config vlan 10) # ipv6 nd reachable-time 30000	
<b>Related Commands</b>		
<b>Note</b>	<ul style="list-style-type: none"> <li>• RAs that advertise zero seconds indicate that the router does not specify a reachable time</li> </ul>	

## ipv6 nd router-preference

```
ipv6 nd router-preference {high | medium | low}  
no ipv6 nd router-preference
```

Sets the value the switch enters in the default router preference (DRP) field of router advertisements (RAs) it sends.

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

<b>Syntax Description</b>	N/A
<b>Default</b>	Medium
<b>Configuration Mode</b>	Config Interface VLAN Config Interface Ethernet configured as a router port interface Config Interface Port Channel configured as a router port interface
<b>History</b>	3.4.1100  3.6.4110                          Updated configuration modes.
<b>Role</b>	admin
<b>Example</b>	switch (config vlan 10) # ipv6 nd router-preference high
<b>Related Commands</b>	
<b>Note</b>	<ul style="list-style-type: none"><li>• IPv6 hosts maintain a default router list from which to select a router for traffic to offlink destinations. The router's address is then saved in the destination cache. The neighbor discovery protocol (NDP) prefers routers that are reachable or probably reachable over routers whose reachability is unknown or suspect. For reachable or probably reachable routers, NDP can either select the same router every time or cycle through the router list. DRP values specify a host's preferred router.</li><li>• If router lifetime is zero, preference value must be medium</li></ul>

## ipv6 nd retrans-timer

**ipv6 nd retrans-timer <time>**  
**no ipv6 nd retrans-timer**

Advertises the time between consecutive neighbor solicitation (NS) messages.  
The no form of the command resets the parameter to its default value.

<b>Syntax Description</b>	time	In milliseconds; the time between retransmitted neighbor solicitation messages. Possible values: <ul style="list-style-type: none"><li>• 0 – unspecified</li><li>• Range – 1000-4294967295</li></ul>		
<b>Default</b>	0 (unspecified)			
<b>Configuration Mode</b>	Config Interface VLAN Config Interface Ethernet configured as a router port interface Config Interface Port Channel configured as a router port interface			
<b>History</b>	3.4.1100  3.6.4110	Updated command syntax, configuration mode and example output.		
<b>Role</b>	admin			
<b>Example</b>	switch (config vlan 10) # ipv6 nd retrans-timer 1000			
<b>Related Commands</b>				
<b>Note</b>				

## ipv6 nd redirects

**ipv6 nd redirects**  
**no ipv6 nd redirects**

Enables sending ICMPv6 redirect messages.

The no form of the command disables sending ICMPv6 redirect messages.

<b>Syntax Description</b>	N/A
<b>Default</b>	Disabled
<b>Configuration Mode</b>	Config Interface VLAN
<b>History</b>	3.4.1100
<b>Role</b>	admin
<b>Example</b>	<code>switch (config interface vlan 10) # ipv6 nd redirects</code>
<b>Related Commands</b>	
<b>Note</b>	

## ipv6 nd dad attempts

**ipv6 nd dad attempts <number>**  
**no ipv6 nd dad attempts**

Sets the number of consecutive neighbor solicitation messages sent for duplicate address detection (DAD) validation.

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

<b>Syntax Description</b>	number	Number of attempts: • 0 – DAD is not performed • Valid range: 1-1000
<b>Default</b>	1	
<b>Configuration Mode</b>	Config Interface VLAN Config Interface Ethernet configured as a router port interface Config Interface Port Channel configured as a router port interface	
<b>History</b>	3.4.1100	
	3.6.4110	Updated configuration mode.
<b>Role</b>	admin	
<b>Example</b>	switch (config vlan 10) # ipv6 nd dad attempts 10	
<b>Related Commands</b>		
<b>Note</b>		

## ipv6 neighbor

```
ipv6 neighbor [vrf <name>] <ipv6-address> <mac-address>
ipv6 neighbor <ipv6-address> interface {ethernet <port> | vlan <vlan-id> |
port-channel <port-channel>} <mac-address>
no interface {ethernet <port> | vlan <vlan-id> | port-channel} ipv6 neighbor
<ipv6-address> <mac-address>
no ipv6 neighbor [vrf <name>] <ipv6-address>
```

Creates an IPv6 neighbor discovery cache static entry.  
The no form of the command removes the specified static entry from the IPv6 neighbor discovery cache.

<b>Syntax Description</b>	ipv6-address	IPv6 address
	ethernet <port>	Ethernet port. Format <slot>/<port>.
	vlan <vlan-id>	VLAN ID
<b>Default</b>	N/A	
<b>Configuration Mode</b>	Config	
<b>History</b>	3.4.1100	
	3.6.4110	Updated command syntax.
<b>Role</b>	admin	
<b>Example</b>	switch (config vlan 10) # ipv6 neighbor 2001:db01::1 vlan 10 4:4:4:4:4:4	
<b>Related Commands</b>		
<b>Note</b>	This command do not affect any dynamic entries in the cache.	

## clear ipv6 neighbors

```
clear ipv6 neighbors {ethernet <slot> /<port> | port-channel <port-channel> |  
vlan <vlan-id>} [<ipv6-addr>]
```

Removes the specified dynamic IPv6 neighbor discovery cache entries.

<b>Syntax Description</b>	ethernet vlan ipv6-addr	Ethernet port. Format: <slot>/<port>. VLAN interface IPv6 address
<b>Default</b>	N/A	
<b>Configuration Mode</b>	Config	
<b>History</b>	3.4.1100 3.6.4110	Updated command
<b>Role</b>	admin	
<b>Example</b>	switch (config) # clear ipv6 neighbors ethernet 1/4	
<b>Related Commands</b>		
<b>Note</b>	<ul style="list-style-type: none"><li>Commands that do not specify an IPv6 address remove all dynamic entries for the listed interface</li><li>Commands that do not specify an interface remove all dynamic entries</li></ul>	

## ipv6 route

- General route:  
`ipv6 route [vrf <vrf-name>] {<ipv6-prefix> | <ipv6-address> /<length>} <next-hop-ipv6-address> [<distance>]`
- Local route:  
`ipv6 route [vrf <vrf-name>] {<ipv6-prefix> | <ipv6-address> /<length>} [<ethernet <port> | vlan <id> | port-channel <id>] [<distance>]`
- Drop route:  
`ipv6 route [vrf <vrf-name>] {<ipv6-prefix> | <ipv6-address> /<length>} null0 [<distance>]`
- Delete route(s):  
`no ipv6 route [vrf <vrf-name>] {<ipv6-prefix> | <ipv6-address> /<length>} [<next-hop-ipv6-address>]`

Creates an IPv6 static route.

The no form of the command deletes static routes.

Syntax Description	ipv6-address	IPv6 address.
	ipv6-prefix	IPv6 address + mask length without space, e.g. a1:a2::33/64.
	length	Prefix length for the associated address space. Range: 1-128.
	next-hop-ipv6-address	IPv6 address of the next-hop
	distance	Administrative distance assigned to route. Options include: <ul style="list-style-type: none"> <li>No parameter – route is assigned a default administrative distance of 1</li> <li>1-255 – the administrative distance assigned to route</li> </ul>
	null0	Creates a black hole route with action DROP
<b>Default</b>	No distance parameter indicated: Administrative distance of 1	
<b>Configuration Mode</b>	Config	
<b>History</b>	3.4.1100	
	3.6.4110	Updated command
<b>Role</b>	admin	
<b>Example</b>	<pre>switch (config) # ipv6 route 3003:db01:: /64 2001:db01::1 switch (config) #</pre>	

---

**Related Commands****Note**

- Static routes have a default administrative distance of 1
  - Assigning a higher administrative distance to a static route configures it to be overridden by dynamic routing data.
  - Multiple routes which are configured to the same destination with the same administrative distance comprise an Equal Cost Multi-Path (ECMP) route
  - A no command not including a source deletes all statements to the destination
  - Route with distance value 255 is not inserted to the forwarding table
-

## ipv6 routing

### ipv6 routing no ipv6 routing

Enables forwarding IPv6 unicast packets.

The no form of the command disables IPv6 unicast routing.

<b>Syntax Description</b>	N/A
<b>Default</b>	Disabled
<b>Configuration Mode</b>	Config
<b>History</b>	3.4.1100
<b>Role</b>	admin
<b>Example</b>	<code>switch (config) # ipv6 routing</code>
<b>Related Commands</b>	
<b>Note</b>	<ul style="list-style-type: none"><li>When routing is enabled, the switch attempts to deliver inbound packets to destination addresses by forwarding them to interfaces or next hop addresses specified by the IPv6 routing table</li></ul>

## show ipv6 interface

**show ipv6 interface [{  
  {{ethernet <port> | port-channel <port-channel> | vlan  
  <vlan-id>}}| brief]**

Displays the status of specified routed interfaces that are configured for IPv6.

<b>Syntax Description</b>	ethernet <port>	Displays output pertaining to the specified Ethernet interface
	port-channel <port-channel>	Displays output pertaining to the specified LAG interface
	vlan <vlan-id>	Displays output pertaining to the specified VLAN interface
	brief	Shows basic IPv6 information regarding all IPv6 interfaces
<b>Default</b>	N/A	
<b>Configuration Mode</b>	Any Command Mode	
<b>History</b>	3.4.1100	
	3.6.4110	Added support for IPv6
<b>Role</b>	admin	
<b>Example</b>	<pre>switch (config) # show ipv6 interface  Vlan10 is Enabled , line protocol is UP   IPv6 : Enabled   Link-local address : fe80::f652:14ff:fe2d:9808   Global Unicast Addresses :     2001:db01::2 /64   Joined Group Addresses :     ff02::1     ff02::2     ff02::1:ff2d:9808   MTU : 1500 bytes   ICMP error messages limited to every milliseconds : 100   ICMP redirects : enabled   ND DAD : enabled   Number of DAD attempts : 1   ND reachable time (milliseconds) : 30000   ND advertised retransmit interval (milliseconds) : 0   ND router advertisements maximum interval (seconds) : 600   ND router advertisements minimum interval (seconds) : 198   ND router advertisements managed configuration flag : unset   ND router advertisements other configuration flag : unset   ND solicited router advertisement : suppressed   ND router advertisements lifetime (seconds) : 1800   ND advertised default router preference : medium   ND router advertisements hop-limit : 64</pre>	

```
switch (config) #
```

---

**Related Commands**

---

**Note**

---

## show ipv6 neighbors

```
show ipv6 neighbors [{ethernet <port> | port-channel <port-channel> | vlan <vlan-id>} | <ipv6 address> | summary]
```

Displays IPv6 neighbor discovery (ND) cache information.

<b>Syntax Description</b>	ethernet <port>	Shows output pertaining to the specified Ethernet interface.
	vlan <vlan-id>	Shows output pertaining to the specified VLAN interface.
	ipv6 address	IPv6 address of individual neighbor
<b>Default</b>	N/A	
<b>Configuration Mode</b>	Any Command Mode	
<b>History</b>	3.4.1100	
	3.6.4110	Updated command syntax and example output.
<b>Role</b>	admin	
<b>Example</b>	<pre>switch (config) # show ipv6 neighbors IPv6 Address           MAC Address      State       Interf ----- 2001:db01::1            f4:52:14:2d:98:88  Reachable   vlan10 switch (config) #</pre>	
<b>Related Commands</b>		
<b>Note</b>		

## show ipv6 route

```
show ipv6 route [vrf <vrf-name> {|<ipv6-address> <ipv6-address>/<length>
[longer-prefixes]}|[connected | bgp | static] }
```

Displays IPv6 neighbor discovery (ND) cache information.

<b>Syntax Description</b>	ipv6-addr longer-prefixes connected static summary	Filters routes by IPv6 address or prefix Displays output for longer prefix entries Displays entries for routes to networks directly connected to the switch Displays entries added through CLI commands Displays the current contents of the IPv6 routing table in summary format
<b>Default</b>	N/A	
<b>Configuration Mode</b>	Any Command Mode	
<b>History</b>	3.4.1100 3.6.4110	Update command
<b>Role</b>	admin	
<b>Example</b>	<pre>switch (config) # show ipv6 route Destination Mask Gateway      Interface Source    Distance/Metric fe80::   64   ::          mgmt0   Connected  256/1 fe80::   64   ::          mgmt1   Connected  256/1 2001:db01:: 64   ::          vlan10  Connected  1/1 3003:db01:: 64 2001:db01::1 vlan10  Static    1/20 switch (config) #</pre>	
<b>Related Commands</b>		
<b>Note</b>		

## show interfaces null0

**show interfaces null0 [vrf <vrf-name>]**

Displays blackhole route byte and packet counters.

<b>Syntax Description</b>	N/A	N/A		
<b>Default</b>	N/A			
<b>Configuration Mode</b>	Any Command Mode			
<b>History</b>	3.6.4110			
<b>Role</b>	admin			
<b>Example</b>	<pre>switch (config) # show interfaces null0 10          packets 740         bytes switch (config) #</pre>			
<b>Related Commands</b>				
<b>Note</b>				

## 6.3 OSPF

Open Shortest Path First (OSPF) is a link-state routing protocol for IP networks. It uses a link state routing algorithm and falls into the group of interior routing protocols, operating within a single autonomous system (AS).

OSPF-speaking routers send Hello packets to all OSPF-enabled IP interfaces. If two routers sharing a common data link agree on certain parameters specified in their respective Hello packets, they become neighbors.

Adjacencies, which can be thought of as virtual point-to-point links, are formed between some neighbors. OSPF defines several network types and several router types. The establishment of an adjacency is determined by the types of routers exchanging Hellos and the type of network over which the Hello packets are exchanged.

Each router sends link-state advertisements (LSAs) over all adjacencies. The LSAs describe all of the router's links, or interfaces, the router's neighbors, and the state of the links. These links might be to stub networks (those without another router attached), to other OSPF routers, to networks in other areas, or to external networks (those learned from another routing process). Because of the varying types of link-state information, OSPF defines multiple LSA types.

Each router receiving an LSA from a neighbor records the LSA in its link-state database and sends a copy of the LSA to all of its other neighbors. By flooding LSAs throughout an area, all routers will build identical link-state databases.

When the databases are complete, each router uses the SPF algorithm to calculate a loop-free graph describing the shortest (lowest cost) path to every known destination, with itself as the root.

When all link-state information has been flooded to all routers in an area, and neighbors have verified that their databases are identical, it means the link-state databases have been synchronized and the route tables have been built. Hello packets are exchanged between neighbors as keepalives, and LSAs are retransmitted. If the network topology is stable, no other activity should occur.

For OSPF network design over Mellanox L2 VMS, please refer to [Mellanox Virtual Modular Switch Reference Guide](#).

### 6.3.1 Router ID

The router ID is a 32-bit number assigned to the router running the OSPF protocol. This number uniquely identifies the router within an Autonomous System.

Router ID can be configured statically, however, if it is not configured, then the default election is as follows:

- If a loopback interface already exists, the router ID takes the loopback IP address;
- Otherwise, the lowest IP address is elected as router ID

### 6.3.2 ECMP

Equal-cost multi-path (ECMP) routing is a routing strategy where next-hop packet forwarding to a single destination can occur over multiple paths. The OSPF link-state routing algorithm can

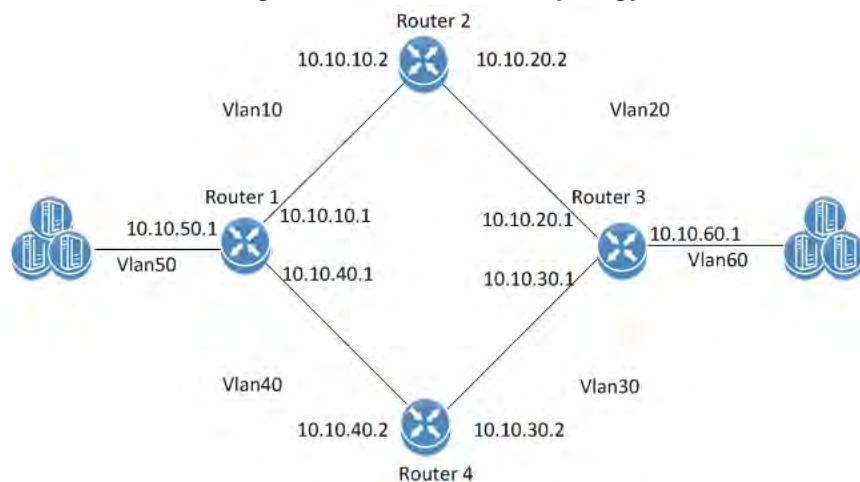
find multiple routes to the same destination, all multiple routes are added to the routing table only if those routes are equal-cost routes.

In case there are several routes with different cost, only the route with the lowest cost is selected. In case there are multiple routes with the same lowest cost, all of them are used (up to maximum of 64 ECMP routes).

ECMP is not configurable but is enabled by default for OSPF.

### 6.3.3 Configuring OSPF

**Figure 38: OSPF Basic Topology**



Precondition steps:



The following configuration example refers to Router 2 in Figure 38. The remainder of the routers in the figure are configured similarly.



It is recommended to disable STP before enabling OSPF. Use the command no spanning-tree.

**Step 1.** Make sure an L3 license is installed. For a list of the available licenses see [Section 2.5, “Licenses,” on page 60](#).

**Step 2.** Enable IP routing functionality. Run::

```
switch (config)# ip routing
```

**Step 3.** Enable the desired VLAN. Run::

```
switch (config)# vlan 10
switch (config)# vlan 20
```

**Step 4.** Add this VLAN to the desired interface. Run:

```
switch (config)# interface ethernet 1/1
switch (config ethernet 1/1)# switchport access vlan 10
switch (config ethernet 1/1)# exit
switch (config)# interface ethernet 1/2
switch (config ethernet 1/2)# switchport access vlan 20
```

**Step 5.** Create a VLAN interface. Run:

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

**Step 6.** Apply IP address to the VLAN interface. Run:

```
switch (config interface vlan 10)# ip address 10.10.10.2 /16
```

**Step 7.** Enable the interface. Run:

```
switch (config interface vlan 10)# no shutdown
```

**Step 8.** Create a second VLAN interface. Run:

```
switch (config)# interface vlan 20
```

**Step 9.** Apply IP address to the second VLAN interface. Run:

```
switch (config interface vlan 20)# ip address 10.10.20.2 /16
```

**Step 10.** Enable the second interface. Run:

```
switch (config interface vlan 20)# no shutdown
```

#### Basic OSPF Configuration:

**Step 1.** To enable OSPF configuration run:

```
switch (config)# protocol ospf
```

**Step 2.** To create a router OSPF instance run:

```
switch (config)# router ospf
```



Only one instance of OSPF is supported.

**Step 3.** Associate the VLAN interfaces to the OSPF area. Area 0 is the backbone area, run:

```
switch (config interface vlan 10)# ip ospf area 0
switch (config interface vlan 10)# exit
switch (config)# interface vlan 20
switch (config interface vlan 20)# ip ospf area 0
```

### 6.3.4 Verifying OSPF

- *To verify OSPF configuration and status:*

**Step 1.** Verify OSPF configuration and status. Run:

```
switch (config) # show ip ospf

Routing Process 1 with ID 10.10.10.10 vrf-default

Stateful High Availability disabled
Graceful-restart is not supported
Supports only single TOS (TOS 0) route
Opaque LSA not supported
OSPF Admin State is enabled
Redistributing External Routes: Disabled
Administrative distance 110
Reference Bandwidth is 40Gb
Initial SPF schedule delay 1 msec
SPF Hold time 10 msec
Maximum paths to destination 64
Router is not originating router LSA with maximum metric
Condition: Always
Number of external LSAs 0, checksum sum 0
Number of opaque AS LSAs 0,checksum sum 0
Number of areas is 1, 1 normal, 0 stub, 0 nssa
Number of active areas is 1, 1 normal, 0 stub, 0 nssa

Area (0.0.0.0) (Active)
Interfaces in this area: 2 Active Interfaces: 2
Passive Interfaces: 0
SPF Calculation has run 5 times
This area is Normal area
Number of LSAs: 1, checksum sum 7700

switch (config) #
```

**Step 2.** Verify the OSPF neighbors status. Make sure that each neighbor reaches FULL state with its peer to enable it take part in all dynamic routing changes in the network. Run:

```
switch (config) # show ip ospf neighbors

Neighbor 10.10.10.1, interface address 10.10.10.2
In the area 0.0.0.0 via interface Vlan 10
Neighbor priority is 1, State is FULL
BDR is 10.10.10.1
Options 0
Dead timer due in 35
```

```
Neighbor 10.10.20.1, interface address 10.10.20.2
In the area 0.0.0.0 via interface Vlan 20
Neighbor priority is 1, State is FULL
BDR is 10.10.20.1
Options 0
Dead timer due in 35

switch (config) #
```

**Step 3.** Verify the OSPF Interface configuration and status run:

```
switch (config) # show ip ospf interface

Interface Vlan is 10 Enabled, line protocol is Down
IP address 10.10.10.2, Mask 255.255.0.0
Process ID 1 VRF Default, Area 0.0.0.0
OSPF Interface Admin State is enabled
State DOWN, Network Type BROADCAST, Cost 1
Transmit delay 1 sec, Router Priority 1
No designated router on this network
No backup designated router on this network
Timer intervals (sec's): Hello 10, Dead 40, Wait 40, Retransmit 5
No authentication
Number of opaque link LSAs: 0, checksum sum 0

Interface Vlan is 20 Enabled, line protocol is Up
IP address 10.10.20.2, Mask 255.255.0.0
Process ID 1 VRF Default, Area 0.0.0.0
OSPF Interface Admin State is enabled
State DESIGNATED ROUTER, Network Type BROADCAST, Cost 1
Transmit delay 1 sec, Router Priority 1
No designated router on this network
No backup designated router on this network
Timer intervals (sec's): Hello 10, Dead 40, Wait 40, Retransmit 5
No authentication
Number of opaque link LSAs: 0, checksum sum 0

switch (config) #
```

## 6.3.5 Commands

### 6.3.5.1 Config

#### protocol ospf

```
protocol ospf
no protocol ospf
```

Enables Open Shortest Path First Protocol (OSPF), and unhides the related OSPF commands.

The no form of the command deletes the OSPF configuration and hides the OSPF related commands.

<b>Syntax Description</b>	N/A
<b>Default</b>	OSPF feature is disabled.
<b>Configuration Mode</b>	Config
<b>History</b>	3.3.3500
<b>Role</b>	admin
<b>Example</b>	switch (config)# protocol ospf
<b>Related Commands</b>	ip routing
<b>Note</b>	

## router ospf

**router ospf [<process-id> [vrf <vrf-name>]]**  
**no router ospf [<process-id> [vrf <vrf-name>]]**

Enters router OSPF configuration mode, and creates default OSPF instance on specific VRF with specific Process ID if one does not exist.  
The no form of the command deletes the OSPF instance.

<b>Syntax Description</b>	process-id vrf	OSPF instance ID VRF name (e.g. default)
<b>Default</b>	Process ID: 1 VRF: Active VRF routing-context	
<b>Configuration Mode</b>	Config	
<b>History</b>	3.3.3500 3.6.1002	Added VRF and process ID parameters and updated Example
<b>Role</b>	admin	
<b>Example</b>	<pre>switch (config)# router ospf 2 vrf myvrf switch (config router ospf 2)#+</pre>	
<b>Related Commands</b>	N/A	
<b>Note</b>	Only one OSPF instance is supported	

### 6.3.5.2 Config Router

#### router-id

```
router-id <ip-address>
no router-id
```

Sets Router ID for the OSPF instance.

The no form of the command causes automatic election of router ID by the router.

Syntax Description	ip-address	The Router id in IP address format.
<b>Default</b>		The router ID is a 32-bit number assigned to the router running the OSPF protocol. This number uniquely identifies the router within an Autonomous System. Router ID can be configured statically, however, if it is not configured, then the default election is as follows: <ul style="list-style-type: none"><li>• If a loopback interface already exists, the router ID takes the loopback IP address;</li><li>• Otherwise, the lowest IP address is elected as router ID.</li></ul>
<b>Configuration Mode</b>	Config OSPF Router	
<b>History</b>	3.3.3500	
<b>Role</b>	admin	
<b>Example</b>		switch (config router ospf)# router-id 10.10.10.10
<b>Related Commands</b>	N/A	
<b>Note</b>		

## shutdown

**shutdown**  
**no shutdown**

Disables the OSPF instance.

The no form of the command enables the OSPF instance.

<b>Syntax Description</b>	N/A
<b>Default</b>	Enable (no shutdown)
<b>Configuration Mode</b>	Config OSPF Router
<b>History</b>	3.3.3500
<b>Role</b>	admin
<b>Example</b>	switch (config router ospf)# shutdown
<b>Related Commands</b>	N/A
<b>Note</b>	

## auto-cost reference-bandwidth

**auto-cost reference-bandwidth <ref-bw> [Gbps | Mbps]**  
**no auto-cost reference-bandwidth**

Configures reference-bandwidth in Gb/s (Default) or Mb/s.  
The no form of the command resets this parameter to its default value.

Syntax Description	ref-bw	Range: 1-4294
	Gbps	Value in Gbps (default if not specified)
	Mbps	Value in Mbps
Default	100 Gbps on Spectrum™ based systems 40 Gbps on SwitchX®-2 based systems	
Configuration Mode	Config OSPF Router	
History	3.3.3500	
Role	admin	
Example	switch (config router ospf)# auto-cost reference-bandwidth 10 Gbps	
Related Commands	N/A	
Note		

## distance

**distance <value>**  
**no distance**

Configures the OSPF route administrative distance.  
The no form of the command resets this parameter to default.

Syntax Description	value	OSPF administrative distance. Range is 1-255.
<b>Default</b>	110	
<b>Configuration Mode</b>	Config OSPF Router	
<b>History</b>	3.3.3500	
<b>Role</b>	admin	
<b>Example</b>		switch (config router ospf)# distance 100
<b>Related Commands</b>		N/A
<b>Note</b>		

## redistribute

```
redistribute {bgp | direct | static | ebgp | ibgp}  
no redistribute {bgp | direct | static}
```

Enables importing routes from other routing protocols as well as any statically configured routers into OSPF.

The no form of the command disables the importing of the routes.

Syntax Description	direct	Redistribute directly connected routes
	bgp	Redistribute routes from BGP protocol
	ibgp	Redistribute IBGP routes
	ebgp	Redistribute EBGP routes
	static	Redistribute static configured routes
Default	Disable (no redistribution)	
Configuration Mode	Config OSPF Router	
History	3.6.3506 3.2.1000	
Role	admin	
Example	switch (config router ospf)# redistribute direct	
Related Commands	N/A	
Note	Routes from multiple protocols can be imported in parallel.	

## timers throttle spf

```
timers throttle spf <spf-delay> <spf-hold>
no timers throttle spf
```

Sets the OSPF throttle SPF timers.

The no form of the command resets the timers to default.

<b>Syntax Description</b>	spf-delay	The interval by which SPF calculations delayed after a topology change reception. Range is 0-100 milliseconds.
	spf-hold	The minimum delay between two consecutive delay calculations. Range is 0-1000 milliseconds.
<b>Default</b>	spf-delay: 1 millisecond spf-hold: 10 millisecond	
<b>Configuration Mode</b>	Config OSPF Router	
<b>History</b>	3.3.3500	
<b>Role</b>	admin	
<b>Example</b>	switch (config router ospf)# timers throttle spf 100 1000	
<b>Related Commands</b>	N/A	
<b>Note</b>		

## **area default-cost**

```
area <area-id> default-cost <cost>  
no area <area-id> default-cost
```

Specifies cost for the default summary route sent into an OSPF stub or not-so-stubby area (NSSA).

The `no` form of the command sets the cost to the default value.

<b>Syntax Description</b>	area-id cost	OSPF area-id. Range is 0-4294967295. The cost for the default summary route. Range is 1-16777215.
<b>Default</b>	The summary route cost is based on the area border router that generated the summary route.	
<b>Configuration Mode</b>	Config OSPF Router	
<b>History</b>	3.3.3500	
<b>Role</b>	admin	
<b>Example</b>	switch (config router ospf)# area 0 default-cost 100	
<b>Related Commands</b>	N/A	
<b>Note</b>	Base cost for all calculation is 56GbE.	

## area range

```
area <area-id> range <ip-address> <prefix> [not-advertise]  
no area <area-id> range <ip-address> <prefix> [not-advertise]
```

Consolidates and summarizes routes at an OSPF area boundary.  
The no form of the command removes the ip-prefix range from summarization.

<b>Syntax Description</b>	area-id	OSPF area-ID. Range is 0-4294967295.
	ip-address	IP Address.
	not-advertise	Suppresses routes that match the specified IP address.
	prefix	Network prefix (in the format of /24, or 255.255.255.0 for example).
<b>Default</b>	Disabled	
<b>Configuration Mode</b>	Config OSPF Router	
<b>History</b>	3.3.3500	
<b>Role</b>	admin	
<b>Example</b>	switch (config router ospf)# area 0 range 10.10.10.10 /24	
<b>Related Commands</b>	N/A	
<b>Note</b>		

## area stub

```
area <area-id> stub [no-summary]
no area <area-id> stub [no-summary]
```

Configures an area as an OSPF stub area (an area is created if non-existent).  
The no form of the command removes the stub area configuration and changes the area to normal, or deletes the area (if stub is not used).

<b>Syntax Description</b>	area-id no-summary	OSPF area-ID. Range is 0-4294967295. Summary route will not be advertised into the stub area.
<b>Default</b>	Summary route will be advertised.	
<b>Configuration Mode</b>	Config OSPF Router	
<b>History</b>	3.3.3500	
<b>Role</b>	admin	
<b>Example</b>	switch (config router ospf)# area 0 stub	
<b>Related Commands</b>	N/A	
<b>Note</b>		

## area nssa

```
area <area-id> nssa [default-information-originate [metric <m-value>] [metric-type <m-type>]] [nosummary] [translate type7 always]
no area <area-id> nssa [default-information-originate ] [no-summary] [translate type7 always]
```

Configures an area as an OSPF not-so-stubby (NSSA) area.

The no form of the command removes the NSSA area configuration and changes the area to default.

<b>Syntax Description</b>	area-id	OSPF area ID. Range is 0-4294967295.
	default-information-originate	A default type7 LSA (Link State Advertisements) is generated into the NSSA area.
	m-type	Metric type for OSPF. Range is 1-2.
	m-value	Metric value for OSPF. Range is 1-65535.
	no-summary	Summary route will not be advertised into the NSSA area.
	translate type7 always	Type7 LSAs is translated to type5 LSAs (Link State Advertisements).
<b>Default</b>	Default m-type:2 Default m-value:10	
<b>Configuration Mode</b>	Config OSPF Router	
<b>History</b>	3.3.3500	
<b>Role</b>	admin	
<b>Example</b>	switch (config router ospf)# area 0 nssa	
<b>Related Commands</b>	N/A	
<b>Note</b>	An area can be either stub, NSSA or normal.	

## no area

**no area <area-id>**

Deletes OSPF area and its related configuration.

<b>Syntax Description</b>	area-id	OSPF area ID Range is 0-4294967295
<b>Default</b>	N/A	
<b>Configuration Mode</b>	Config OSPF Router	
<b>History</b>	3.3.3500	
<b>Role</b>	admin	
<b>Example</b>	switch (config router ospf)# no area 1	
<b>Related Commands</b>	N/A	
<b>Note</b>	The command fails if the area is attached to active interfaces.	

## summary-address

```
summary-address <ip-address> <prefix> [not-advertise]  
no summary-address <ip-address> <prefix> [not-advertise]
```

Creates aggregate addresses for the OSPF protocol.  
The no form of the command disables the aggregation of the ip-address.

Syntax Description	ip-address	The summary IP address.
	not-advertise	Suppresses routes that match the specified ip-address.
	prefix	Network prefix (in the format of /24 or 255.255.255.0, for example).
<b>Default</b>	N/A	
<b>Configuration Mode</b>	Config OSPF Router	
<b>History</b>	3.3.3500	
<b>Role</b>	admin	
<b>Example</b>	switch (config router ospf)# summary-address 10.10.10.10 /24	
<b>Related Commands</b>	N/A	
<b>Note</b>	Maximum of 1500 summarized IP addresses can be configured.	

### 6.3.5.3 Interface

#### ip ospf cost

**ip ospf cost <cost>**  
**no ip ospf cost**

Sets OSPF cost of sending packet of this interface.  
The no form of the command resets this parameter to default.

<b>Syntax Description</b>	cost	The Interface cost used by the OSPF. Range is 1-65535.
<b>Default</b>	1	
<b>Configuration Mode</b>	Config Interface VLAN Config Interface Ethernet configured as a router port interface Config Interface Port Channel configured as a router port interface	
<b>History</b>	3.3.3500	
<b>Role</b>	admin	
<b>Example</b>	switch (config interface vlan 10)# ip ospf cost 100	
<b>Related Commands</b>	N/A	
<b>Note</b>		

## ip ospf dead-interval

**ip ospf dead-interval <seconds>**  
**no ip ospf dead-interval**

Configures the interval during which at least one Hello packet must be received from a neighbor before the router declares that neighbor as down.  
The no form of the command resets this parameter to its default.

<b>Syntax Description</b>	seconds	The dead-interval timer, in seconds. Range is 1-65535.
<b>Default</b>	40	
<b>Configuration Mode</b>	Config Interface VLAN Config Interface Ethernet configured as a router port interface Config Interface Port Channel configured as a router port interface	
<b>History</b>	3.3.3500	
<b>Role</b>	admin	
<b>Example</b>	switch (config interface vlan 10)# ip ospf dead-interval 10	
<b>Related Commands</b>	N/A	
<b>Note</b>	The value must be the same for all nodes on the network.	

## ip ospf hello-interval

```
ip ospf hello-interval <seconds>
no ip ospf hello-interval
```

Configures the interval between Hello packets that OSPF sends on the interface.  
The no form of the command resets this parameter to default.

<b>Syntax Description</b>	seconds	The Hello interval timer, in seconds. Range is 1-65535.
<b>Default</b>	10	
<b>Configuration Mode</b>	Config Interface VLAN Config Interface Ethernet configured as a router port interface Config Interface Port Channel configured as a router port interface	
<b>History</b>	3.3.3500	
<b>Role</b>	admin	
<b>Example</b>	switch (config interface vlan 10)# ip ospf hello-interval 20	
<b>Related Commands</b>	N/A	
<b>Note</b>	The value must be the same for all nodes on the network.	

## ip ospf priority

**ip ospf priority <number>**  
**no ip ospf priority**

Configures the priority for this OSPF interface.  
The no form of the command resets this parameter to default.

<b>Syntax Description</b>	number	The Interface priority used by the OSPF protocol. Range is 0-255
<b>Default</b>	1	
<b>Configuration Mode</b>	Config Interface VLAN Config Interface Ethernet configured as a router port interface Config Interface Port Channel configured as a router port interface	
<b>History</b>	3.3.3500	
<b>Role</b>	admin	
<b>Example</b>	switch (config interface vlan 10)# ip ospf priority 100	
<b>Related Commands</b>	N/A	
<b>Note</b>	<ul style="list-style-type: none"><li>• Use the “ip ospf priority” command to set the router priority, which determines the designated router for this network. When two routers are attached to a network, both attempt to become the designated router.</li><li>• The router with the higher router priority takes precedence. If there is a tie, the router with the higher router ID takes precedence. A router with a router priority set to zero cannot become the designated router or backup designated router.</li></ul>	

## ip ospf network

**ip ospf network <type>**  
**no ip ospf network**

Sets the OSPF interface network type.

The no form of the command resets the interface network type to its default.

<b>Syntax Description</b>	type	The network type on this interface. <ul style="list-style-type: none"><li>• broadcast</li><li>• point-to-point</li></ul>
<b>Default</b>	broadcast for VLAN interfaces point-to-point for router port interfaces	
<b>Configuration Mode</b>	Config Interface VLAN Config Interface Ethernet configured as a router port interface Config Interface Port Channel configured as a router port interface	
<b>History</b>	3.3.3500	
<b>Role</b>	admin	
<b>Example</b>	switch (config interface vlan 10)# ip ospf network point-to-point	
<b>Related Commands</b>	N/A	
<b>Note</b>	<ul style="list-style-type: none"><li>• The network type influences the behavior of the OSPF interface. An OSPF network type is usually broadcast, which uses OSPF multicasting capabilities. Under this network type, a designated router and backup designated router are elected. For point-to-point networks, there are only two neighbors and multicast is not required.</li><li>• All routers on the same network must have the same network type.</li></ul>	

## ip ospf retransmit-interval

```
ip ospf retransmit-interval <seconds>
no ip ospf retransmit-interval
```

Configures the time between OSPF link-state advertisement (LSA) retransmissions for adjacencies that belongs to the interface.

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

<b>Syntax Description</b>	seconds	The retransmit interval in seconds. Range is 0-3600.
<b>Default</b>	5	
<b>Configuration Mode</b>	Config Interface VLAN Config Interface Ethernet configured as a router port interface Config Interface Port Channel configured as a router port interface	
<b>History</b>	3.3.3500	
<b>Role</b>	admin	
<b>Example</b>	switch (config interface vlan 10)# ip ospf retransmit-interval 10	
<b>Related Commands</b>	N/A	
<b>Note</b>		

## ip ospf passive-interface

**ip ospf passive-interface**  
**no ip ospf passive-interface**

Suppresses flooding of OSPF routing updates on an interface.  
The no form of the command reverts the status to active OSPF interface.

<b>Syntax Description</b>	N/A
<b>Default</b>	Active interface (no ip ospf passive-interface)
<b>Configuration Mode</b>	Config Interface VLAN Config Interface Ethernet configured as a router port interface Config Interface Port Channel configured as a router port interface
<b>History</b>	3.3.3500
<b>Role</b>	admin
<b>Example</b>	switch (config interface vlan 10)# ip ospf passive-interface
<b>Related Commands</b>	N/A
<b>Note</b>	

## ip ospf transmit-delay

```
ip ospf transmit-delay <seconds>
no ip ospf transmit-delay
```

Sets the estimated time required to send an OSPF link-state update packet.  
The no form of the command resets this parameter to its default.

<b>Syntax Description</b>	seconds	The transmit-delay interval in seconds. Range is 0-3600.
<b>Default</b>	1	
<b>Configuration Mode</b>	Config Interface VLAN Config Interface Ethernet configured as a router port interface Config Interface Port Channel configured as a router port interface	
<b>History</b>	3.3.3500	
<b>Role</b>	admin	
<b>Example</b>	switch (config interface vlan 10)# ip ospf transmit-delay 2	
<b>Related Commands</b>	N/A	
<b>Note</b>		

## ip ospf shutdown

**ip ospf shutdown**  
**no ip ospf shutdown**

Disables the OSPF instance on the interface.  
The no form of the command enables the OSPF on this interface.

<b>Syntax Description</b>	N/A
<b>Default</b>	Enabled (no shutdown)
<b>Configuration Mode</b>	Config Interface VLAN Config Interface Ethernet configured as a router port interface Config Interface Port Channel configured as a router port interface
<b>History</b>	3.3.3500
<b>Role</b>	admin
<b>Example</b>	switch (config interface vlan 10)# ip ospf shutdown
<b>Related Commands</b>	N/A
<b>Note</b>	

## ip ospf authentication

**ip ospf authentication [message-digest]**  
**no ip ospf authentication**

Specifies the authentication type for OSPF.  
The no form of the command disables the authentication.

<b>Syntax Description</b>	message-digest	Specifies that message-digest authentication (MD5) is used.
<b>Default</b>	Disabled (no)	
<b>Configuration Mode</b>	Config Interface VLAN Config Interface Ethernet configured as a router port interface Config Interface Port Channel configured as a router port interface	
<b>History</b>	3.3.3500	
<b>Role</b>	admin	
<b>Example</b>	switch (config interface vlan 10)# ip ospf authentication	
<b>Related Commands</b>	N/A	
<b>Note</b>	<ul style="list-style-type: none"><li>Without message-digest option, a simple password authentication will be used.</li><li>Message-digest authentication can be enabled only if a key is configured.</li></ul>	

## ip ospf authentication-key

```
ip ospf authentication-key [<auth-type>] <password>
no ip ospf authentication-key
```

To assign a password for simple password authentication for the OSPF.  
The no form of the command deletes the simple password authentication key.

<b>Syntax Description</b>	auth-type	The authentication type: 0 – unencrypted password 7 – MD5 key
	password	Authentication password (up to 8 alphanumeric string)
<b>Default</b>	Unencrypted password	
<b>Configuration Mode</b>	Config Interface VLAN Config Interface Ethernet configured as a router port interface Config Interface Port Channel configured as a router port interface	
<b>History</b>	3.3.3500	
<b>Role</b>	admin	
<b>Example</b>	switch (config interface vlan 10)# ip ospf authentication-key 0 mycleartextpassword	
<b>Related Commands</b>	N/A	
<b>Note</b>	<ul style="list-style-type: none"><li>When selecting an encrypted password “7”, the user must input a password encrypted with an MD5 key.</li><li>When selecting an unencrypted password “0”, the user must input a cleartext password. Then when examining the running-config, it exhibits the encrypted password.</li></ul>	

## ip ospf message-digest-key

```
ip ospf message-digest-key <key-id> md5 [auth-type] <key>
no ip ospf message-digest-key <key-id>
```

Sets the message digest key for MD5 authentication.

The no form of the command deletes the key for MD5 authentication.

<b>Syntax Description</b>	auth-type	The authentication type: 0 - Unencrypted password 7 - MD5 key
	key	Authentication password, up to 8 alphanumeric string.
	key-id	Alphanumeric password of up to 16 bytes.
<b>Default</b>	Unencrypted (no)	
<b>Configuration Mode</b>	Config Interface VLAN Config Interface Ethernet configured as a router port interface Config Interface Port Channel configured as a router port interface	
<b>History</b>	3.3.3500	
<b>Role</b>	admin	
<b>Example</b>	switch (config interface vlan 10)# ip ospf message-digest-key mykeyid md5 7 mykey	
<b>Related Commands</b>	N/A	
<b>Note</b>	The user cannot delete the last key until authentication is disabled.	

## ip ospf area

**ip ospf area <area-id>**  
**no ip ospf area**

Sets OSPF area of this interface (and creates the area if non-existent).  
The no form of the command removes the interface from the area.

<b>Syntax Description</b>	area-id OSPF area ID Range is 0-4294967295
<b>Default</b>	N/A
<b>Configuration Mode</b>	Config Interface VLAN Config Interface Ethernet configured as a router port interface Config Interface Port Channel configured as a router port interface Config Interface Loopback
<b>History</b>	3.3.3500
<b>Role</b>	admin
<b>Example</b>	switch (config interface vlan 10)# ip ospf area 0
<b>Related Commands</b>	N/A
<b>Note</b>	

### 6.3.5.4 Show

#### show ip ospf

**show ip ospf [<process-id> [vrf <vrf-name>]]**

Displays general OSPF configuration on specific VRF and status.

<b>Syntax Description</b>	process-id vrf	OSPF instance ID VRF instance
<b>Default</b>	Process ID: 1 VRF: Active VRF routing-context	
<b>Configuration Mode</b>	Any Command Mode	
<b>History</b>	3.3.3500 3.6.1002	Added VRF and process ID parameters and updated Example
<b>Role</b>	admin	
<b>Example</b>	<pre>switch (config)# show ip ospf 2 vrf myvrf Routing Process 2 with ID 2.2.2.2 myvrf Stateful High Availability is not supported Graceful-restart is not supported Supports only single TOS (TOS 0) route Opaque LSA not supported OSPF Admin State is enabled Redistributing External Routes: Disabled Administrative distance 110 Reference Bandwidth is 40 Gbps Initial SPF schedule delay 1 msec SPF Hold time 5000 msec Maximum paths to destination 64 Router LSA with maximum metric is not supported Condition: Always Number of external LSAs 0, checksum sum 0 Number of opaque AS LSAs 0, checksum sum 0 Number of areas is 1, 1 normal, 0 stub, 0 nssa Number of active areas is 1, 1 normal, 0 stub, 0 nssa  Area (0.0.0.0) (Active) Interfaces in this area: 2 Active Interfaces: 2 Passive Interfaces: 0 SPF Calculation has run 6 times This area is Normal area Number of LSAs: 3, checksum sum 161346</pre>	
<b>Related Commands</b>	N/A	
<b>Note</b>		

## show ip ospf border-routers

**show ip ospf border-routers [vrf <vrf-name>]**

Displays routing table entries to an Area Border Routers.

<b>Syntax Description</b>	vrf	OSPF routing table entries to an Area Border Routers on specific VRF.
<b>Default</b>	VRF: Active VRF routing-context	
<b>Configuration Mode</b>	Any Command Mode	
<b>History</b>	3.3.3500	
	3.6.1002	Added VRF parameter and updated Example
<b>Role</b>	admin	
<b>Example</b>	<pre>switch (config)# show ip ospf border-routers vrf myvrf  OSPF Process ID 2, vrf myvrf Internal Routing Table Codes: i - Intra-area route, I - Inter-area route i 1.1.1.1 [0] ABR Area: 0.0.0.0, Next Hop: 21.21.21.1</pre>	
<b>Related Commands</b>	N/A	
<b>Note</b>		

## **show ip ospf database**

```
show ip ospf database [summary] [<process-id> <area-id> [<link-state-id>]]  
[adv-router <ip-address> | self-originated] [vrf <vrf-name>]
```

Displays the OSPF database.

<b>Syntax Description</b>	adv-router <ip-address>	Filters per advertise router																																							
	area-id	Filters the command per OSPF Area ID. Range is 0-4294967295.																																							
	link-state-id	The link state ID																																							
	self-originated	Self Originate																																							
	summary	Summarizes the output of the OSPF database.																																							
	process-id	Displays OSPF database on specific instance ID																																							
	vrf	Displays OSPF database on specific VRF																																							
<b>Default</b>	Process ID: 1 VRF: Active VRF routing-context																																								
<b>Configuration Mode</b>	Any Command Mode																																								
<b>History</b>	3.3.3500  3.6.1002	Added VRF and process ID parameters and updated Example																																							
<b>Role</b>	admin																																								
<b>Example</b>	<pre>switch (config)# show ip ospf database 2 vrf myvrf</pre> <pre>OSPF Router with ID (2.2.2.2) (Process ID 2 VRF myvrf)</pre> <table border="1"> <thead> <tr> <th colspan="6">Router Link States (Area 0.0.0.0)</th> </tr> <tr> <th>Link ID</th> <th>ADV Router</th> <th>Age</th> <th>Seq</th> <th>Checksum</th> <th>LinkCount</th> </tr> </thead> <tbody> <tr> <td>2.2.2.2</td> <td>2.2.2.2</td> <td>1150</td> <td>0x80000006</td> <td>0xbd2a</td> <td>3</td> </tr> <tr> <td>1.1.1.1</td> <td>1.1.1.1</td> <td>1152</td> <td>0x80000006</td> <td>0xf7f5</td> <td>3</td> </tr> </tbody> </table> <table border="1"> <thead> <tr> <th colspan="5">Network Link States (Area 0.0.0.0)</th> </tr> <tr> <th>Link ID</th> <th>ADV Router</th> <th>Age</th> <th>Seq</th> <th>Checksum</th> </tr> </thead> <tbody> <tr> <td>21.21.21.2</td> <td>2.2.2.2</td> <td>1150</td> <td>0x80000003</td> <td>0xbb26</td> </tr> </tbody> </table>		Router Link States (Area 0.0.0.0)						Link ID	ADV Router	Age	Seq	Checksum	LinkCount	2.2.2.2	2.2.2.2	1150	0x80000006	0xbd2a	3	1.1.1.1	1.1.1.1	1152	0x80000006	0xf7f5	3	Network Link States (Area 0.0.0.0)					Link ID	ADV Router	Age	Seq	Checksum	21.21.21.2	2.2.2.2	1150	0x80000003	0xbb26
Router Link States (Area 0.0.0.0)																																									
Link ID	ADV Router	Age	Seq	Checksum	LinkCount																																				
2.2.2.2	2.2.2.2	1150	0x80000006	0xbd2a	3																																				
1.1.1.1	1.1.1.1	1152	0x80000006	0xf7f5	3																																				
Network Link States (Area 0.0.0.0)																																									
Link ID	ADV Router	Age	Seq	Checksum																																					
21.21.21.2	2.2.2.2	1150	0x80000003	0xbb26																																					
<b>Related Commands</b>	N/A																																								
<b>Note</b>																																									

## show ip ospf interface

**show ip ospf interface [<process-id>] [vlan <vlan-id> | Ethernet <slot/port | port-channel <number>] [brief]**

Displays the OSPF related interface configuration.

<b>Syntax Description</b>	brief	Gives a brief summary of the output
	process-id	Displays OSPF interface configuration on specific instance ID
	vlan <vlan-id>	Displays OSPF interface configuration and status per VLAN interface
	vrf	Displays OSPF interface configuration on specific VRF
<b>Default</b>	Process ID: 1 VRF: Active VRF routing-context	
<b>Configuration Mode</b>	Any Command Mode	
<b>History</b>	3.3.3500 3.6.1002 3.6.4070	Added VRF and process ID parameters and updated Example Added Ethernet variable
<b>Role</b>	admin	
<b>Example</b>	<pre>switch (config) # show ip ospf interface 2 vrf myvrf  Interface Vlan is 21 Enabled, line protocol is Up IP address 21.21.21.2, Mask 255.255.255.0 Process ID 2 VRF myvrf, Area 0.0.0.0 OSPF Interface Admin State is enabled State DESIGNATED ROUTER, Network Type BROADCAST, Cost 10 Transmit delay 1 sec, Router Priority 1 DR is 2.2.2.2 Backup Designated Router is 1.1.1.1 Timer intervals (secs): Hello 10, Dead 40, Wait 40, Retransmit 5 No authentication Number of opaque link LSAs: 0, checksum sum 0  switch (config) # show ip ospf interface 2 vrf myvrf brief</pre>	
	<pre>OSPF Process ID 2 VRF myvrf Total number of interface: 2 Interface Id      Area          Cost      State      Neighbors      Status Vlan21           0.0.0.0       10        Enabled      1            Up Ethernet1/22     0.0.0.0       1         Enabled      1            Up</pre>	

---

**Related Commands** N/A

---

**Note**

---

## show ip ospf neighbors

```
show ip ospf [vrf <vrf-name>] neighbors [vlan <vlan-id> | interface <name>]
[<neighbor ip address>]
```

Displays the OSPF related interface neighbor configuration.

<b>Syntax Description</b>	vlan-id	Displays OSPF interface configuration and status per VLAN interface
	neighbor ip address	Filters the output per a specific OSPF neighbor
	vrf	Displays OSPF interface neighbor configuration on specific VRF
<b>Default</b>	VRF: Active VRF routing-context	
<b>Configuration Mode</b>	Any Command Mode	
<b>History</b>	3.3.3500 3.6.1002                  Added VRF parameter and updated Example 3.6.4070                  Added support for BFD	
<b>Role</b>	admin	
<b>Example</b>	<pre>switch (config) # show ip ospf neighbors vrf myvrf  Neighbor 1.1.1.1, interface address 21.21.21.1 In the area 0.0.0.0 via Interface Vlan 21 Neighbor priority is 1, State is FULL DR is 2.2.2.2 Backup Designated Router is 1.1.1.1 Options 2 Dead timer due in 36  Neighbor 1.1.1.1, interface address 22.22.22.1 In the area 0.0.0.0 via Interface Ethernet 1/22 Neighbor priority is 1, State is FULL No designated router on this network No backup designated router on this network Options 2 Dead timer due in 36 switch (config) # show ip ospf neighbors interface ethernet 1/22 vrf myvrf  Neighbor 1.1.1.1, interface address 22.22.22.1 In the area 0.0.0.0 via interface Ethernet 1/22 Neighbor priority is 1, State is FULL No designated router on this network No backup designated router on this network Options 2 Dead timer due in 29</pre>	

---

**Related Commands**

N/A

**Note**

BFD session state is displayed as: established, failed or not established. When BFD is not defined in the command, it is not displayed in the output.

---

## show ip ospf request-list

```
show ip ospf request-list <neighbor-id> {vlan <vlan-id> | ethernet <slot/port> | port-channel <id>} [vrf <vrf-name>]
```

Displays the OSPF list of all link-state advertisements (LSAs) requested by a router.

<b>Syntax Description</b>	neighbor-id vlan-id vrf <vrf-name>	Filers the output per a specific OSPF neighbor. Filers the output per a specific VLAN ID. Displays OSPF request-list on specific VRF
<b>Default</b>	vrf: active VRF routing-context	
<b>Configuration Mode</b>	Any Command Mode	
<b>History</b>	3.6.3506 3.3.3500	
<b>Role</b>	admin	
<b>Example</b>	<pre>switch (config) # show ip ospf request-list 4.4.4.4 vlan 7 OSPF Router with ID (7.7.7.1) (Process ID 1) Neighbor 4.4.4.4, Interface vlan 7, Address 7.7.7.2 42 LSAs on request-list        Type        LS-ID          ADV-RTR        Seq No       Age      Checksum       1           10.10.10.23    10.10.10.23   0x8000012f   37      0xa7b9       1           10.10.10.24    10.10.10.24   0x8000012f   38      0xbd61</pre>	
<b>Related Commands</b>	N/A	
<b>Note</b>		

## show ip ospf retransmission-list

```
show ip ospf retransmission-list <neighbor-id> {vlan <vlan-id> | ethernet <slot/port> | port-channel <id>} [vrf <vrf-name>]
```

Displays the OSPF list of all link-state advertisements (LSAs) waiting to be resent to neighbors.

<b>Syntax Description</b>	<b>neighbor-id</b> <b>vrf &lt;vrf-name&gt;</b> <b>vlan-id</b>	Filters the output per a specific OSPF neighbor. Displays OSPF retransmission-list on specific VRF. Filters the output per a specific VLAN ID.
<b>Default</b>	vrf: Active VRF routing-context	
<b>Configuration Mode</b>	Any Command Mode	
<b>History</b>	3.6.3506 3.3.3500	
<b>Role</b>	admin	
<b>Example</b>	<pre>switch (config) # show ip ospf retransmission-list 4.4.4.4 vlan 6 OSPF Router with ID (7.7.7.1) (Process ID 1) Neighbor 4.4.4.4, Interface vlan 6, Address 6.6.6.2 Link state retransmission due in 3780 msec, Queue length 207        Type        LS-ID          ADV-RTR        Seq No        Age        Checksum       3           22.22.22.22    7.7.7.1       0x80000045    0         0xaaf4       3           192.168.23.2   7.7.7.1       0x80000001    353       0x6752</pre>	
<b>Related Commands</b>	N/A	
<b>Note</b>		

## show ip ospf summary-address

**show ip ospf summary-address [vrf <vrf-name>]**

Displays a list of all summary address redistribution information configured on the OSPF.

<b>Syntax Description</b>	vrf <vrf-name>	Display summary address and area range information on specific VRF.
<b>Default</b>	vrf : Active VRF routing-context	
<b>Configuration Mode</b>	Any Command Mode	
<b>History</b>	3.6.3506 3.3.3500	
<b>Role</b>	admin	
<b>Example</b>	<pre>switch (config)# show ip ospf summary-address OSPF Process ID 1 VRF default Network          Mask           Area       Advertise      LSA type     Metric   Tag -----  -----  -----  -----  -----  -----  -----  ----- 66.66.66.0      255.255.255.0 0.0.0.1  Advertise    Type 3      Auto     N/A 66.66.66.0      255.255.255.0 0.0.0.1  Advertise    Type 7      Auto     N/A 55.55.55.0      255.255.255.0 0.0.0.5  Advertise    Type 3      Auto     N/A 33.33.0.0       255.255.0.0   N/A       Advertise    Type 5      Auto     N/A 44.44.0.0       255.255.0.0   N/A       Advertise    Type 5      Auto     N/A arc-switch11 [standalone: master] (config) #</pre>	
<b>Related Commands</b>	N/A	
<b>Note</b>		

## 6.4 BGP

Border Gateway Protocol (BGP) is an exterior gateway protocol which is designed to transfer routing information between routers. It maintains and propagates a table of routes which designates network reachability among autonomous systems (ASs).

BGP neighbors, or peers, are routers configured manually to converse using the BGP protocol on top of a TCP session on port 179. A BGP speaker periodically sends keep-alive messages to maintain the connection. Network reachability includes such information as forwarding destinations (IPv4 or IPv6) together with a list of ASs that this information traverses and other attributes, so it becomes possible to construct a graph of AS connectivity without routing loops. BGP makes possible to apply policy rules to enforce connectivity graph.

BGP routers communicate through TCP connection on port 179. Connection between BGP neighbors is configured manually or can be established dynamically by configuring dynamic listen groups. When BGP runs between two peers in the same AS, it is referred to as Internal BGP (iBGP, or Interior Border Gateway Protocol). When it runs between separate ASs, it is called External BGP (eBGP, or Exterior Border Gateway Protocol). Both sides can initiate a connection, after the initial connectivity is created, BGP state machine drives both sides to enter into ESTABLISHED state where they can exchange UPDATE messages with reachability information.

### 6.4.1 State Machine

In order to make decisions in its operations with peers, a BGP peer uses a simple finite state machine (FSM) that consists of six states: Idle; Connect; Active; OpenSent; OpenConfirm; and Established. For each peer-to-peer session, a BGP implementation maintains a state variable that tracks which of these six states the session is in. The BGP protocol defines the messages that each peer should exchange in order to change the session from one state to another.

The first state is the “Idle” state. In “Idle” state, BGP initializes all resources, refuses all inbound BGP connection attempts and initiates a TCP connection to the peer. The second state is “Connect”. In the “Connect” state, the router awaits the TCP connection to complete and transitions to the “OpenSent” state if successful. If unsuccessful, it initializes the ConnectRetry timer and transitions to the “Active” state upon expiration. In the “Active” state, the router resets the ConnectRetry timer to zero and returns to the “Connect” state. In the “OpenSent” state, the router sends an Open message and waits for one in return in order to transition to the “OpenConfirm” state. KeepAlive messages are exchanged and, upon successful receipt, the router is placed into the “Established” state. In the “Established” state, the router can send/receive: KeepAlive; Update; and Notification messages to/from its peer.

### 6.4.2 Default Address Family

Default Address Family defines which address family is activated when peer or peer-group becomes active.

When the default address family configuration is modified - it will cause a renegotiation of capabilities for all neighbors that do not have explicit configuration of active address families.

The default address family in BGP IPv6 is IPv4.

### 6.4.3 Default Route Originate

Default Route Originate initial value is set to “false”.

### 6.4.4 Peer Groups and Update Groups

Any BGP peer can be defined as part of a peer group and it will inherit peer group configuration or have its own configuration.

A system will automatically generate an update group from peer groups members.

Peer that has a different outbound policy from peer-group will not become a part of update group.

### 6.4.5 Configuring BGP

**Figure 39: Basic BGP Configuration**



Follow these steps for basic BGP configuration on two switches (Router 1 and Router 2):

Preconditions:

**Step 1.** Make sure the license installed supports L3.

**Step 2.** Enable IP routing functionality. Run:

```
switch (config)# ip routing
```

**Step 3.** Enable the desired VLAN. Run:

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



The same VLAN must be configured on both switches.

**Step 4.** Add this VLAN to the desired interface. Run:

```
switch (config)# interface ethernet 1/1
switch (config ethernet 1/1)# switchport access vlan 10
```

**Step 5.** Create a VLAN interface. Run:

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

**Step 6.** Apply IP address to the VLAN interface on Router 1. Run:

```
switch (config interface vlan 10)# ip address 10.10.10.1 /24
```

**Step 7.** Apply IP address to the VLAN interface on Router 2. Run:

```
switch (config interface vlan 10)# ip address 10.10.10.2 /24
```

**Step 8.** Enable the interface. Run:

```
switch (config interface vlan 10)# no shutdown
```

#### Configure BGP:

**Step 1.** Enable BGP. Run:

```
switch (config)# protocol bgp
```

**Step 2.** Configure an AS number that identifies the BGP router. Run:

```
switch (config)# router bgp 100
```



To run iBGP, the AS number of all remote neighbors should be similar to the local AS number of the configured router.

**Step 3.** Configure BGP Router 1 neighbor. Run:

```
switch (config router bgp 100)# neighbor 10.10.10.2 remote-as 100
```

**Step 4.** Configure BGP Router 2 neighbor. Run:

```
switch (config router bgp 100)# neighbor 10.10.10.1 remote-as 100
```

## 6.4.6 Verifying BGP

**Step 1.** Check the general status of BGP. Run:

```
switch (config)# show ip bgp summary
BGP router identifier 10.10.10.1, local AS number 100
BGP table version is 100, main routing table version 100
0 network entries using 0 bytes of memory
0 path entries using 0 bytes of memory
0 BGP AS-PATH entries using 0 bytes of memory
0 BGP community entries using 0 bytes of memory
0 BGP extended community entries using 0 bytes of memory
Neighbor      V      AS MsgRcvd MsgSent TblVer  InQ OutQ Up/Down      State/PfxRcd
10.10.10.2      0      100      100      76      3      0      0 00:0:10:19 ESTABLISHED
switch (config)#
BGP summary information for VRF default, address family IPv4
```

- Verify that the state of each BGP neighbor reached to ESTABLISHED state.
- In case the neighbor is disabled (shutdown). The state of the neighbor will be IDLE.
- BGP incoming and outgoing messages should be incremented.
- The AS number of each neighbor is the correct one.

**Step 2.** Check the status of the neighbors. Run:

```
switch (config)# show ip bgp neighbors
BGP neighbor is 10.10.10.2, remote AS 100, external link
    BGP version 0, remote router ID 0.0.0.0
    BGP State = ESTABLISHED
    Last read 0:00:00:00, last write 0:00:00:00, hold time is 180, keepalive
    interval is 60 seconds
        Configured hold time is 180, keepalive interval is 60 seconds
        Minimum holdtime from neighbor is 0 seconds
switch (config)#

```

You should be able to see running BGP counters and ESTABLISHED state per active neighbor.

## 6.4.7 Commands

### 6.4.7.1 Config

#### protocol bgp

```
protocol bgp
no protocol bgp
```

Enables BGPv4, and unhides BGP related commands.  
The no form of the command deletes all BGP configuration and hides BGP related commands.

<b>Syntax Description</b>	N/A
<b>Default</b>	Disabled
<b>Configuration Mode</b>	Config
<b>History</b>	3.3.5006
<b>Role</b>	admin
<b>Example</b>	<pre>switch (config)# protocol bgp switch (config)#</pre>
<b>Related Commands</b>	ip routing
<b>Note</b>	

## clear ip bgp

**clear ip bgp [{<ipv4\_addr | ipv6\_addr> | all} [soft] [in]]**

Clears BGP learned routes from the BGP table and resets the connection to the neighbor.

<b>Syntax Description</b>	ip-address	A BGP peer IP address. Only the specified neighbor is reset.
	all	All BGP peers. All BGP neighbors are reset.
	soft	Clears BGP learned routes from the BGP table without resetting the connection to the neighbor
	in	Inbound routes are reset
<b>Default</b>	N/A	
<b>Configuration Mode</b>	Config	
<b>History</b>	3.3.5006	First release
	3.3.5200	Updated description
	3.6.3004	Removed “out” parameter
	3.6.4070	Added support for IPv4 and IPv6
<b>Role</b>	admin	
<b>Example</b>	<pre>switch (config)# clear ip bgp all switch (config)#</pre>	
<b>Related Commands</b>	N/A	
<b>Note</b>	This command removes BGP IPv4 learned routes from the routing table, reads all routes from designated peers, and sends routes to those peers as required.	

## router bgp

```
router bgp <as-number>
no router bgp <as-number>
```

Creates and enters a BGP instance with the specified AS number.  
The no form of the command deletes all router BGP instance configuration.

<b>Syntax Description</b>	as-number	Autonomous system number: A unique number to be used to identify the AS. The AS is a number which identifies the BGP router to other routers and tags the routing information passed along. Range: 1-65535.
<b>Default</b>	N/A	
<b>Configuration Mode</b>	Config	
<b>History</b>	3.3.5006	
	3.3.5200	Updated syntax description
<b>Role</b>	admin	
<b>Example</b>	<pre>switch (config)# router bgp 100 switch (config router bgp 100)# </pre>	
<b>Related Commands</b>	ip routing	
<b>Note</b>		

### 6.4.7.2 Config Router

#### shutdown

**shutdown**  
**no shutdown**

Gracefully disables BGP protocol without removing existing configuration.  
The no form of the command enables BGP.

<b>Syntax Description</b>	N/A
<b>Default</b>	Enabled
<b>Configuration Mode</b>	Config Router BGP
<b>History</b>	3.3.5006
<b>Role</b>	admin
<b>Example</b>	<pre>switch (config router bgp 100)# no shutdown</pre>
<b>Related Commands</b>	
<b>Note</b>	

## aggregate-address

```
aggregate-address <ipv4_prefix length | ipv6_prefix length> [summary-only]
[as-set] [attribute-map]
no aggregate-address <ipv4_prefix length | ipv6_prefix length> [summary-only]
[as-set] [attribute-map]
```

Creates an aggregate route in the BGP database.  
The no form of the command disables ECMP across AS paths.

<b>Syntax Description</b>	ipv4_prefix, ipv6_prefix	Destination to aggregate
	summary-only	Contributor routes are not advertised
	as-set	Includes AS_PATH information from contributor routes as AS_SET attributes
	attribute-map	Assigns attribute values in set commands of the map's permit clauses. Deny clauses and match commands in permit clauses are ignored.
<b>Default</b>	Disabled	
<b>Configuration Mode</b>	Config Router BGP	
<b>History</b>	3.4.0000	
	3.6.4070	Added support for IPv4 and IPv6
<b>Role</b>	admin	
<b>Example</b>	<pre>switch-e07c04 [standalone: master] (config router bgp 4) # aggregate- address 3.5.3.7 /32</pre>	
<b>Related Commands</b>		
<b>Note</b>	<ul style="list-style-type: none"> <li>Aggregate routes combine the characteristics of multiple routes into a single route that the switch advertises</li> <li>Aggregation can reduce the amount of information that a BGP speaker is required to store and transmit when advertising routes to other BGP speakers</li> <li>Aggregate routes are advertised only after they are redistributed</li> </ul>	

## bestpath as-path multipath-relax

**bestpath as-path multipath-relax [force]**  
**no bestpath as-path multipath-relax [force]**

Enables ECMP across AS paths.

The no form of the command disables ECMP across AS paths.

<b>Syntax Description</b>	force	Applies configuration while BGP is admin-up
<b>Default</b>	Disabled	
<b>Configuration Mode</b>	Config Router BGP	
<b>History</b>	3.3.5006	
	3.3.5200	Updated description and notes
	3.6.3004	Added “force” parameter
<b>Role</b>	admin	
<b>Example</b>	switch (config router bgp 100)# bestpath as-path multipath-relax	
<b>Related Commands</b>	maximum-paths	
<b>Note</b>	<ul style="list-style-type: none"><li>With this option disabled, only routes with exactly the same AS path as the best route to a destination are considered for ECMP</li><li>With this option enabled, all routes with similar length AS path as the best route are considered for ECMP</li></ul>	

## bgp fast-external-fallover

**bgp fast-external-fallover**  
**no bgp fast-external-fallover**

Terminates eBGP sessions of any directly adjacent peer without waiting for the hold-down timer to expire if the link used to reach the peer goes down.

The no form of the command waits for hold-down timer to expire before terminating eBGP sessions.

<b>Syntax Description</b>	N/A
<b>Default</b>	no bgp fast-external-fallover
<b>Configuration Mode</b>	Config Router BGP
<b>History</b>	3.4.0000
<b>Role</b>	admin
<b>Example</b>	<pre>switch (config router bgp 100)# bgp fast-external-fallover</pre>
<b>Related Commands</b>	maximum-paths
<b>Note</b>	Although this feature improves BGP conversion time, it may cause instability in your BGP table due to a flapping interface.

## bgp listen limit

**bgp listen limit <maximum>**  
**no bgp listen limit**

Limits the number of dynamic BGP peers allowed on the switch.  
The no form of the command resets to the default value.

<b>Syntax Description</b>	maximum	The maximum number of dynamic BGP peers to be allowed on the switch. Range: 1-128.
<b>Default</b>	100	
<b>Configuration Mode</b>	Config Router BGP	
<b>History</b>	3.4.0000	
<b>Role</b>	admin	
<b>Example</b>	switch (config router bgp 100)# bgp listen limit 101	
<b>Related Commands</b>		
<b>Note</b>		

## **bgp listen range peer-group**

```
bgp listen range <ipv4_prefix_length | ipv6_prefix_length> peer-group <peer-group-name> remote-as <as-number>
no bgp listen range <ipv4_prefix_length | ipv6_prefix_length> <length>
```

Identifies a range of IP addresses from which the switch will accept incoming dynamic BGP peering requests.

After applying the no form of the command, the switch will no longer accept dynamic peering requests on the range.

<b>Syntax Description</b>	ipv4_prefix, ipv6_prefix	IP address
	length	Mask length (e.g. /24 or 255.255.255.254)
	peer-group-name	Peer group name
	remote-as <as-number>	Remote peer's number
<b>Default</b>	100	
<b>Configuration Mode</b>	Config Router BGP	
<b>History</b>	3.4.0000	
	3.6.3004	Added note
	3.6.4070	Added support for IPv4 and IPv6
<b>Role</b>	admin	
<b>Example</b>	<pre>switch (config router bgp 100)# bgp listen range 10.10.10.10 /24 peer-group my-group remote-as 13</pre>	
<b>Related Commands</b>		
<b>Note</b>	<ul style="list-style-type: none"> <li>To create a static peer group, use the command neighbor peer-group</li> <li>Neighbors in a dynamic peer group are configured as a group and cannot be configured individually</li> <li>The no form of the command may take up to a few seconds to take effect if there are many dynamic peers and/or a lot of routes. While the clean-up process is running, creation of a new listen range that overlaps the deleted one will fail.</li> <li>If dynamic peer range is defined with an overlap to another defined range, the longest remote address prefix take affect</li> </ul>	

## cluster-id

```
cluster-id <ip-address> [force]
no cluster-id <ip-address> [force]
```

Configures the cluster ID in a cluster with multiple route reflectors.  
The no form of the command resets the cluster ID for route reflector.

<b>Syntax Description</b>	ip-address	The route reflector cluster ID <ul style="list-style-type: none"><li>• 0.0.0.1 to 255.255.255.255 Valid cluster ID number</li><li>• 0.0.0.0 removes the cluster-ID from the switch (similar to “no cluster-id”)</li></ul>
	force	Applies configuration while BGP is admin-up
<b>Default</b>	Cluster ID is the same as Router ID	
<b>Configuration Mode</b>	Config Router BGP	
<b>History</b>	3.2.1000 3.4.0000 Updated syntax description 3.6.3004 Added “force” parameter	
<b>Role</b>	admin	
<b>Example</b>	switch (config router bgp 100)# cluster-id 10.10.10.10	
<b>Related Commands</b>	N/A	
<b>Note</b>		

## client-to-client reflection

**client-to-client reflection**  
**no client-to-client reflection**

The switch will be configured as a route reflector.

The no form of the command stops the switch from being a route reflector

<b>Syntax Description</b>	N/A
<b>Default</b>	client-to-client reflection is enabled
<b>Configuration Mode</b>	Config Router BGP
<b>History</b>	3.2.1000
<b>Role</b>	admin
<b>Example</b>	switch (config router bgp 100)# client-to-client reflection
<b>Related Commands</b>	N/A
<b>Note</b>	

## distance

**distance <external> <internal> <local>**  
**no distance**

Sets the administrative distance of the routes learned through BGP.  
The no form of the command resets the administrative distance its default.

<b>Syntax Description</b>	external internal local	Administrative distance for external BGP routes. Range: 1-255.  Administrative distance for internal BGP routes. Range: 1-255.  Administrative distance for local BGP routes. Range: 1-255.
<b>Default</b>	external: 20 internal: 200 local: 200	
<b>Configuration Mode</b>	Config Router BGP	
<b>History</b>	3.3.5006	
<b>Role</b>	admin	
<b>Example</b>	switch (config router bgp 100)# distance 10 20 30	
<b>Related Commands</b>	N/A	
<b>Note</b>	<ul style="list-style-type: none"> <li>• Routers use administrative distances to decide on a route when two protocols provide routing information to the same destination.</li> <li>• Lower distance values correspond to higher reliability.</li> <li>• Routes are external when learned from an external autonomous system.</li> <li>• Routes are internal when learned from a peer in the local autonomous system.</li> <li>• Local routes are those networks listed with a network router configuration command, often as back doors, for the router or for the networks being redistributed from another process.</li> <li>• BGP routing tables do not include routes with a distance of 255.</li> </ul>	

## graceful-restart stalepath-time

```
graceful-restart stalepath-time <interval>
no graceful-restart stalepath-time
```

Configures the maximum time that stale routes from a restarting BGP neighbor are retained after a BGP session is reestablished with that peer.  
The no form of the command resets to the default value.

<b>Syntax Description</b>	interval	Time in seconds. Range: 1-3600.
<b>Default</b>	300 seconds	
<b>Configuration Mode</b>	Config Router BGP	
<b>History</b>	3.4.0000	
<b>Role</b>	admin	
<b>Example</b>	switch (config router bgp 100)# graceful-restart stalepath-time 350	
<b>Related Commands</b>	N/A	
<b>Note</b>		

## maximum-paths

**maximum-paths [ibgp] <maximum-path>**

Configures the maximum number of parallel eBGP/iBGP routes that the switch installs in the routing table.

<b>Syntax Description</b>	ibgp maximum-path	Sets the configuration on the internal BGP. The number of routes to install to the routing table. Range: 1-32
<b>Default</b>	1	
<b>Configuration Mode</b>	Config Router BGP	
<b>History</b>	3.3.5006 3.3.5200 3.6.4070	Updated description and notes Updated maximum-path range.
<b>Role</b>	admin	
<b>Example</b>	switch (config router bgp 100)# maximum-paths ibgp 10 switch (config router bgp 100)#	
<b>Related Commands</b>	N/A	
<b>Note</b>	<ul style="list-style-type: none"> <li>This command provides an ECMP parameter that controls the number of equal-cost paths that the switch installs in the routing table for each destination.</li> <li>The action is effective after BGP restart.</li> <li>If the parameter “ibgp” is not used, the setting is applied on routes learned from peers from other ASs; if “ibgp” is used, the setting is applied to routes learned from peers of the same AS.</li> </ul>	

## neighbor advertisement-interval

**neighbor {<ipv4\_addr | ipv6\_addr> | <peer-group-name>} advertisement-interval <delay>**

**no neighbor {<ipv4\_addr | ipv6\_addr> | <peer-group-name>} advertisement-interval**

Sets the minimum route advertisement interval (MRAI) between the sending of BGP routing updates.

The no form of the command disables this function.

<b>Syntax Description</b>	ipv4_addr, ipv6_addr	A BGP peer IP address
	peer-group-name	Peer group name
	delay	Time (in seconds) is specified by an integer Range: 0-600 where “0” disables this function and prevents the system from inheriting this parameter’s group configuration
<b>Default</b>	30 seconds	
<b>Configuration Mode</b>	Config Router BGP	
<b>History</b>	3.4.0000	
	3.6.3004	Updated description of “delay” parameter
	3.6.4070	Added support for IPv6 and IPv4
<b>Role</b>	admin	
<b>Example</b>	switch (config router bgp 100)# neighbor 10.10.10.10 advertisement-interval 90	
<b>Related Commands</b>		
<b>Note</b>		

## neighbor allowas-in

```
neighbor {<ipv4_addr | ipv6_addr> | <peer-group-name>} allowas-in [number]
no neighbor {<ipv4_addr | ipv6_addr> | <peer-group-name>} allowas-in
```

Configures the switch to permit the advertisement of prefixes containing duplicate autonomous switch numbers (ASNs).

The no form of the command disables this function.

<b>Syntax Description</b>	ipv4_addr, ipv6_addr	A BGP peer IP address
	peer-group-name	Peer group name
	number	Number of switch's (ASN) allowed in path Range: 0-10 where "0" disables this function and prevents the system from inheriting this parameter's group configuration
<b>Default</b>	N/A	
<b>Configuration Mode</b>	Config Router BGP	
<b>History</b>	3.4.0000	
	3.6.3004	Updated description of "number" parameter
	3.6.4070	Added support for IPv6 and IPv4
<b>Role</b>	admin	
<b>Example</b>	switch (config router bgp 100)# neighbor 10.10.10.10 allowas-in 2	
<b>Related Commands</b>	ip routing router bgp <as-number>	
<b>Note</b>	Neighbors from the same AS as the router are considered as iBGP peers, and neighbors from other ASs are considered eBGP peers.	

## neighbor description

```
neighbor {<ipv4_addr | ipv6_addr> | <peer-group-name>} description <string>
no neighbor {<ipv4_addr | ipv6_addr> | <peer-group-name>} description
```

Associates descriptive text with the specified peer or peer group.  
The no form of the command removes the description from the peer.

<b>Syntax Description</b>	ipv4_addr, ipv6_addr	IP address of the neighbor
	peer-group-name	Peer group name
	string	Free string, up to 80 characters in length
<b>Default</b>	No description	
<b>Configuration Mode</b>	Config Router BGP	
<b>History</b>	3.3.5006	
	3.3.5200	Updated example
	3.6.4070	Added support for IPv6 and IPv4
<b>Role</b>	admin	
<b>Example</b>	switch (config router bgp 100)# neighbor 10.10.10.10 description The next door neighbor	
<b>Related Commands</b>	N/A	
<b>Note</b>	The peer description only appears in the show commands.	

## neighbor ebgp-multipath

```
neighbor {<ipv4_addr | ipv6_addr> | <peer-group-name>} ebgp-multipath
[<ttl>]
no neighbor {<ipv4_addr | ipv6_addr> | <peer-group-name>} ebgp-multipath
```

Enables BGP to connect to external peers that are not directly connected to the switch.  
The no form of the command disables connecting to external peers.

<b>Syntax Description</b>	ipv4_addr, ipv6_addr	IP address of the BGP-speaking neighbor
	peer-group-name	Peer group name
	ttl	Time-to-live Range: 1-255 hops where “1” disables connecting to external peers and prevents the system from inheriting this parameter’s group configuration
<b>Default</b>	ttl: 1	
<b>Configuration Mode</b>	Config Router BGP	
<b>History</b>	3.3.5006	
	3.3.5200	Updated default
	3.6.3004	Updated description of “ttl” parameter
	3.6.4070	Added support for IPv6 and IPv4
<b>Role</b>	admin	
<b>Example</b>	switch (config router bgp 100)# neighbor 10.10.10.10 ebgp-multipath 5	
<b>Related Commands</b>	ip routing neighbor <ip-address> remote-as <as-number>	
<b>Note</b>	The command does not establish the multi-hop if the only route to the peer is the default route (0.0.0.0).	

## neighbor export-localpref

```
neighbor {<ipv4_addr | ipv6_addr> | <peer-group-name>} export-localpref
<value>
no neighbor {<ipv4_addr | ipv6_addr> | <peer-group-name>} export-localpref
```

Configures the local preference value sent to the specified peer or peer group.  
The no form of the command resets the local preference to its default value.

<b>Syntax Description</b>	ipv4_addr, ipv6_addr	IP address of the BGP-speaking neighbor
	peer-group-name	Peer group name
	value	Preference value Range: 0-2147483647 where “100” configures the default, and prevents the system from inheriting this parameter’s group configuration
<b>Default</b>	100	
<b>Configuration Mode</b>	Config Router BGP	
<b>History</b>	3.4.0000	
	3.6.3004	Updated description of “value” parameter
	3.6.4070	Added support for IPv6 and IPv4
<b>Role</b>	admin	
<b>Example</b>	switch (config router bgp 100)# neighbor 10.10.10.10 export-localpref 100	
<b>Related Commands</b>		
<b>Note</b>		

## neighbor import-localpref

[no] neighbor {<ipv4\_addr | ipv6\_addr> | <peer-group-name>} import-localpref <value>

Configures the local preference value assigned to routes received from the specified peer or peer group.

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

<b>Syntax Description</b>	ipv4_addr, ipv6_addr	IP address of the BGP-speaking neighbor
	peer-group-name	Peer group name
	value	Preference value Range: 0-2147483647 where “100” configures the default, and prevents the system from inheriting this parameter’s group configuration
<b>Default</b>	100	
<b>Configuration Mode</b>	Config Router BGP	
<b>History</b>	3.4.0000	
	3.6.3004	Updated description of “value” parameter
	3.6.4070	Added support for IPv6 and IPv4
<b>Role</b>	admin	
<b>Example</b>	switch (config router bgp 100)# neighbor 10.10.10.10 import-localpref 100	
<b>Related Commands</b>		
<b>Note</b>		

## neighbor local-as

```
neighbor {<ipv4-address> | <ipv6-address> | <peer-group-name>} local-as <asn-id> [no-prepend | replace-as]
no neighbor {<ipv4-address> | <ipv6-address> | <peer-group-name>} local-as
```

Enables the modification of the AS path attribute for routes received from an eBGP neighbor.

The no form of the command disables AS path modification for the specified peer or peer group.

<b>Syntax Description</b>	ipv4-address   ipv6-address peer-group-name asn-id no-prepend replace-as	IP address of the BGP-speaking neighbor Peer group name AS number that is sent instead of the actual AS of the switch. Range: 0-4294967295 local-as number is not pre-pended to the routes received from external neighbors Prepends only the local autonomous system number (as configured with the IP address argument) to the AS path attribute
<b>Default</b>	N/A	
<b>Configuration Mode</b>	Config Router BGP	
<b>History</b>	3.4.0000 3.6.3004 3.6.4070 3.6.4110	Updated description of “as-id” parameter Added support for IPv6 and IPv4 Updated command.
<b>Role</b>	admin	
<b>Example</b>	switch-e07c04 [standalone: master] (config router bgp 4) # neighbor 100.100.100.100 local-as 123	
<b>Related Commands</b>	ip routing neighbor <ip-address> remote-as <as-number>	
<b>Note</b>	<ul style="list-style-type: none"> <li>This function allows the switch to appear as a member of a different autonomous system (AS) to external peers.</li> <li>To disable peering with the neighbor run the command <code>clear ip bgp</code></li> </ul>	

## neighbor local-v6-addr

```
neighbor {<ipv4-address > | <peer-group-name>} local-v6-addr <ipv6_local>
no neighbor {<ipv6-address > | <peer-group-name>} local-v6-addr
```

Specifies the switch's next-hop value sent using IPv6 NLRI in IPv4 transport session.

The no form of the command removes next-hop value.

<b>Syntax Description</b>	ipv4-address, ipv6-address	IP address of the BGP-speaking neighbor
	peer-group-name	Peer group name
	ipv6_local	IPv6 next hop address.
<b>Default</b>	N/A	
<b>Configuration Mode</b>	Config Router BGP	
<b>History</b>	3.6.4070	
	3.6.4110	Added support for IPv6
<b>Role</b>	admin	
<b>Example</b>	switch (config router bgp 4) # neighbor 10.10.10.1 local-v6-addr 2001::2	
<b>Related Commands</b>		
<b>Note</b>		

## neighbor maximum-prefix

```
neighbor {<ipv4_addr | ipv6_addr> | <peer-group-name>} maximum-prefix
<maximum> [warning-only]
no neighbor {<ipv4_addr | ipv6_addr> | <peer-group-name>} maximum-prefix
```

Configures the number of BGP routes the switch accepts from a specified neighbor and defines an action when the limit is exceeded.

The no form of the command removes the limitation

<b>Syntax Description</b>	ipv4_addr, ipv6_addr	IP address of the BGP-speaking neighbor
	peer-group-name	Peer group name
	maximum	Number of BGP routes the switch accepts from a specified neighbor Range: 1-2147483647 where “12000” configures the default, and prevents the system from inheriting this parameter’s group configuration
	warning-only	Only generates a warning rather than disconnecting the neighbor
<b>Default</b>	12000	
<b>Configuration Mode</b>	Config Router BGP	
<b>History</b>	3.4.0000	
	3.6.3004	Updated description of “maximum” parameter
	3.6.4070	Added support for IPv6 and IPv4
<b>Role</b>	admin	
<b>Example</b>	switch (config router bgp 100)# neighbor 10.10.10.10 maximum-prefix 12000 warning-only	
<b>Related Commands</b>	ip routing neighbor <ip-address> remote-as <as-number>	
<b>Note</b>		

## neighbor next-hop-peer

```
neighbor {<ipv4_addr | ipv6_addr> | <peer-group-name>} next-hop-peer [dis-
able]
no neighbor {<ipv4_addr | ipv6_addr> | <peer-group-name>} next-hop-peer
```

Configures the switch to list the peer address as the next hop in routes that it receives from the specified peer BGP-speaking neighbor or members of the specified peer group.

The no form of the command disables this function.

<b>Syntax Description</b>	ipv4_addr, ipv6_addr peer-group-name disable	IP address of the neighbor Peer group name Disables this function and prevents the system from inheriting this parameter's group configuration
<b>Default</b>	no next-hop-peer	
<b>Configuration Mode</b>	Config Router BGP	
<b>History</b>	3.3.5006 3.6.3004 3.6.4070	Added “disable” parameter Added support for IPv6 and IPv4
<b>Role</b>	admin	
<b>Example</b>	switch (config router bgp 100)# neighbor 10.10.10.10 next-hop-peer	
<b>Related Commands</b>		
<b>Note</b>	This command overrides the next hop for all routes received from this neighbor or peer group	

## neighbor next-hop-self

```
neighbor {<ipv4_addr | ipv6_addr> | <peer-group-name>} next-hop-self [dis-
able]
no neighbor {<ipv4_addr | ipv6_addr> | <peer-group-name>} next-hop-self
```

Configures the IP address of the router as the next hop address in routes advertises to the specific neighbor.

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

<b>Syntax Description</b>	ipv4_addr, ipv6_addr	IP address of the neighbor
	peer-group-name	Peer group name
	disable	Disables this function and prevents the system from inheriting this parameter's group configuration
<b>Default</b>	no next-hop-self	
<b>Configuration Mode</b>	Config Router BGP	
<b>History</b>	3.3.5006	
	3.6.4070	Added support for IPv6
<b>Role</b>	admin	
<b>Example</b>	switch (config router bgp 100)# neighbor 10.10.10.10 next-hop-self	
<b>Related Commands</b>	neighbor <ip-address> remote-as <as-number>	
<b>Note</b>	<ul style="list-style-type: none"> <li>This function is used in networks where BGP neighbors do not directly access all other neighbors on the same subnet.</li> <li>In the default state, the next hop is generated based on the IP address and the present next hop in the route information.</li> </ul>	

## neighbor password

```
neighbor {<ipv4_addr | ipv6_addr> | <peer-group-name>} password [<encryption>] <string>
no neighbor {<ipv4_addr | ipv6_addr> | <peer-group-name>} password
```

Enables authentication on a TCP connection with a BGP peer.  
The no form of the command resets the value to its default.

<b>Syntax Description</b>	ipv4_addr, ipv6_addr	IP address of the neighbor
	peer-group-name	Peer group name
	encryption	Possible values: • no parameter – clear text • 0 – clear text • 7 – obfuscated
	string	Up to 8 bytes in length
<b>Default</b>	no neighbor password	
<b>Configuration Mode</b>	Config Router BGP	
<b>History</b>	3.4.0000	
	3.6.4070	Added support for IPv6 and IPv4
<b>Role</b>	admin	
<b>Example</b>	<pre>switch (config router bgp 100)# neighbor 10.10.10.10 password 7 admin123</pre>	
<b>Related Commands</b>		
<b>Note</b>	<ul style="list-style-type: none"> <li>Peers must use the same password to ensure communication.</li> <li>neighbor &lt;ip-address&gt; password 7 &lt;password&gt;' can only accept data that was created using 'show config'.</li> <li>'show config' will never show the clear-test password, it will always be obfuscated (and thus displayed using the 'password 7' syntax).</li> <li>Router BGP neighbor password cannot be set when enabling secure mode</li> <li>Router BGP peer-group password cannot be set when enabling with secure mode</li> </ul>	

## neighbor no-password

**neighbor {<ip-address> | <peer-group-name>} no-password**

Disables authentication for peer without inheritance.

<b>Syntax Description</b>	ip-address peer-group-name	IP address of the neighbor Peer group name
<b>Default</b>	N/A	
<b>Configuration Mode</b>	Config Router BGP	
<b>History</b>	3.6.3004	
<b>Role</b>	admin	
<b>Example</b>	switch (config router bgp 100)# neighbor 10.10.10.10 no-password	
<b>Related Commands</b>	neighbor password	
<b>Note</b>		

## neighbor peer-group

1. neighbor {<ipv4\_addr | ipv6\_addr >} peer-group <peer-group-name>
2. neighbor {<peer-group-name>} peer-group
3. no neighbor {<ipv4\_addr | ipv6\_addr >} peer-group <peer-group-name>
4. no neighbor {<peer-group-name>} peer-group

1. Assigns BGP neighbors to an existing peer group
2. Creates a peer-group
3. Unassigns a BGP neighbor from a peer-group
4. Deletes the peer-group

<b>Syntax Description</b>	ipv4_addr, ipv6_addr peer-group-name	IP address of the neighbor Peer group name
<b>Default</b>	N/A	
<b>Configuration Mode</b>	Config Router BGP	
<b>History</b>	3.4.0000 3.6.3004 3.6.4070	Added notes Added support for IPv6 and IPv4
<b>Role</b>	admin	
<b>Example</b>	<pre>switch (config router bgp 100)# neighbor groupA peer-group switch (config router bgp 100)# neighbor 1.2.3.4 peer-group groupA</pre>	
<b>Related Commands</b>		
<b>Note</b>	<ul style="list-style-type: none"> <li>• Once a peer group is created, the group name can be used as a parameter in neighbor configuration commands, and the configuration will be applied to all members of the group.</li> <li>• Settings applied to an individual neighbor in the peer group override group settings.</li> <li>• A neighbor can only belong to one peer group, so issuing this command for a neighbor that is already a member of another group removes it from that group.</li> <li>• When a neighbor is removed from a peer group, the neighbor retains the configuration inherited from the peer group.</li> <li>• Router BGP peer-group password cannot be set when enabling with secure mode</li> <li>• A BGP group must be used by either a single listen range, or by a set of neighbors sharing the same type (iBGP or eBGP)</li> <li>• A group must already exist before a node is configured to use it</li> <li>• Any configuration change on a group affects each of the peers inheriting this specific parameter from the group only after undergoing admin state toggle</li> </ul>	

## neighbor remote-as

```
neighbor {<ipv4_addr | ipv6_addr>} remote-as <as-number>
no neighbor {<ipv4_addr | ipv6_addr>} remote-as <as-number>
```

Configures a neighbor.

The no form of the command removes the neighbor, dropping the connection and all routes if already connected.

<b>Syntax Description</b>	ipv4_addr, ipv6_addr peer-group-name as-number	IP address of the neighbor Peer group name The BGP peer as-number. Range: 1-65535.
<b>Default</b>	N/A	
<b>Configuration Mode</b>	Config Router BGP	
<b>History</b>	3.3.5006 3.3.5200 3.6.4070	Updated description and note Added support for IPv6 and IPv4
<b>Role</b>	admin	
<b>Example</b>	<pre>switch (config router bgp 100)# neighbor 10.10.10.10 remote-as 200 switch (config router bgp 100)# </pre>	
<b>Related Commands</b>	ip routing router bgp <as-number>	
<b>Note</b>	Neighbors from the same AS as the router are considered as iBGP peers, and neighbors from other ASs are considered eBGP peers.	

## neighbor remove-private-as

```
neighbor {<ipv4_addr | ipv6_addr> | <peer-group-name>} remove-private-as
[disable]
no neighbor {<ipv4_addr | ipv6_addr> | <peer-group-name>} remove-private-as
```

Removes private autonomous system numbers from outbound routing updates for external BGP (eBGP) neighbors.

The no form of the command preserves private AS numbers for the specified peer.

<b>Syntax Description</b>	ipv4_addr, ipv6_addr	A BGP peer IP address
	peer-group-name	Peer group name
	disable	Preserves private AS numbers for the specified peer and prevents the system from inheriting this parameter's group configuration
<b>Default</b>	N/A	
<b>Configuration Mode</b>	Config Router BGP	
<b>History</b>	3.4.0000	
	3.6.4070	Added support for IPv6 and IPv4
<b>Role</b>	admin	
<b>Example</b>	<pre>switch (config router bgp 100)# neighbor 10.10.10.10 remove-private-as switch (config router bgp 100)# </pre>	
<b>Related Commands</b>	ip routing router bgp <as-number>	
<b>Note</b>	<ul style="list-style-type: none"> <li>This can only be used with external BGP (eBGP) peers.</li> <li>If the update has only private AS numbers in the AS path, BGP removes these numbers.</li> <li>If the AS path includes both private and public AS numbers, BGP does not remove the private AS numbers. This situation is considered a configuration error.</li> <li>If the AS path contains the AS number of the eBGP neighbor, BGP does not remove the private AS number.</li> <li>If the AS path contains confederations, BGP removes the private AS numbers only if they come after the confederation portion of the AS path.</li> </ul>	

## neighbor route-map

```
neighbor {<ipv4_addr | ipv6_addr> | <peer-group-name>} route-map <route-map-name> [in | out]
no neighbor {<ipv4_addr | ipv6_addr> | <peer-group-name>} route-map <route-map-name> [in | out]
```

Configures a route map to inbound BGP routes.  
The no form of the command undoes the configuration.

<b>Syntax Description</b>	ipv4_addr, ipv6_addr	IP address of the neighbor
	peer-group-name	Peer group name
	route-map-name	String. The name of the route-map
	in	Applies route map to inbound routes
	out	Applies route map to out-bound routes
<b>Default</b>	N/A	
<b>Configuration Mode</b>	Config Router BGP	
<b>History</b>	3.3.5006 3.3.5200                  Updated notes and default 3.4.1100                  Added “out” parameter 3.6.3004                  Added note 3.6.4070                  Added support for IPv6 and IPv4	
<b>Role</b>	admin	
<b>Example</b>	switch (config router bgp 100)# neighbor 10.10.10.10 route-map MyRoute-Map in	
<b>Related Commands</b>	neighbor <ip-address> remote-as <as-number> route-map <map-name> [deny   permit] [sequence-number] clear ip bgp {<ip-address>   all}	
<b>Note</b>	<ul style="list-style-type: none"> <li>Only one inbound route-map can be applied to a given neighbor</li> <li>If a new route-map is applied to a neighbor, it replaces the previous route map</li> <li>Changing a route-map only takes effect on routes received or sent after the change</li> <li>A route-map must already exist before a node is configured to use it</li> </ul>	

## neighbor no-route-map

**neighbor {<ip-address> | <peer-group-name>} no-route-map**

Unsets route-map for neighbor and prevents the system from inheriting this parameter's group configuration.

<b>Syntax Description</b>	ip-address peer-group-name	IP address of the neighbor Peer group name
<b>Default</b>	N/A	
<b>Configuration Mode</b>	Config Router BGP	
<b>History</b>	3.6.3004	
<b>Role</b>	admin	
<b>Example</b>	switch (config router bgp 100)# neighbor 10.10.10.10 no-route-map	
<b>Related Commands</b>	neighbor <ip-address> remote-as <as-number> route-map <map-name> [deny   permit] [sequence-number]	
<b>Note</b>		

## neighbor route-reflector-client

```
neighbor {<ipv4_addr | ipv6_addr> | <peer-group-name>} route-reflector-client
[disable]
no neighbor {<ipv4_addr | ipv6_addr> | <peer-group-name>} route-reflector-client
```

Sets the neighbor as a client but does not set up the reflection itself.  
The no form of the command disables route reflection for the specific peer.

<b>Syntax Description</b>	ipv4_addr, ipv6_addr	IP address of the neighbor.
	peer-group-name	Peer group name
	disable	Unsets neighbor as route reflector client and prevents the system from inheriting this parameter's group configuration
<b>Default</b>	N/A	
<b>Configuration Mode</b>	Config Router BGP	
<b>History</b>	3.3.5006	
	3.3.5200	Updated notes and default
	3.6.3004	Added “disable” parameter
	3.6.4070	Added support for IPv6 and IPv4
<b>Role</b>	admin	
<b>Example</b>	switch (config router bgp 100)# neighbor 10.10.10.10 route-reflector-client	
<b>Related Commands</b>		
<b>Note</b>		

## neighbor send-community

```
neighbor {<ipv4_addr | ipv6_addr> | <peer-group-name>} send-community
[extended] [disable]
no neighbor {<ipv4_addr | ipv6_addr> | <peer-group-name>} send-community
[extended]
```

Configures the switch to send community attributes to the specified BGP neighbor. The no form of the command disables sending community attributes for the specified peer.

<b>Syntax Description</b>	ipv4_addr, ipv6_addr	IP address of the neighbor
	peer-group-name	Peer group name
	extended	Sends extended community attributes to neighbor
	disable	Disables sending community attributes for the specified peer and prevents the system from inheriting this parameter's group configuration
<b>Default</b>	Enabled	
<b>Configuration Mode</b>	Config Router BGP	
<b>History</b>	3.4.0000 3.6.3004                          Added “disable” parameter 3.6.4070                          Added support for IPv6 and IPv4	
<b>Role</b>	admin	
<b>Example</b>	switch (config router bgp 100)# neighbor 10.10.10.10 send-community	
<b>Related Commands</b>	N/A	
<b>Note</b>		

## neighbor shutdown

```
neighbor {<ipv4_addr | ipv6_addr> | <ipv4_addr | ipv6_addr> | <peer-group-name>} shutdown [disable]
no neighbor {<ipv4_addr | ipv6_addr> | <ipv4_addr | ipv6_addr> | <peer-group-name>} shutdown
```

Disables BGP neighbor gracefully.

The no form of the command enables BGP neighbor.

<b>Syntax Description</b>	ipv4_addr, ipv6_addr	IP address of the neighbor
	peer-group-name	Peer group name
	disable	Enables BGP neighbor and prevents the system from inheriting this parameter's group configuration
<b>Default</b>	Enabled	
<b>Configuration Mode</b>	Config Router BGP	
<b>History</b>	3.3.5006 3.3.5200                  Updated note 3.6.4070                  Added IPv6 and IPv4 support	
<b>Role</b>	admin	
<b>Example</b>	switch (config router bgp 100)# neighbor 10.10.10.10 shutdown	
<b>Related Commands</b>	N/A	
<b>Note</b>	<ul style="list-style-type: none"> <li>Disabling a neighbor terminates all its active sessions and removes associated routing information</li> <li>A group's shutdown immediately impacts every peer in this group, making them inherit this parameter</li> </ul>	

## neighbor fall-over bfd

[no] neighbor {<ip-address> | < ipv4\_addr | ipv6\_addr >} | <peer-group-name>  
fall-over bfd

Disables BFD as a mechanism to detect failure.  
The no form of the command enables BFD neighbor.

Syntax Description	peer-group-name	Peer group name
	ipv4_addr	IPv4 address of the neighbor
	ipv6_addr	IPv6 address of the neighbor
Default	Enabled	
Configuration Mode	Config Router BGP	
History	3.6.4070	
Role	admin	
Example	switch (config router bgp 100)# neighbor 10.10.10.10 bfd	
Related Commands		
Note	The command "no neighbor <ip_address> fall-over bfd" affects traffic, BGP will restore the connection based on Hello protocol.	

## neighbor soft-reconfiguration

```
neighbor {< ipv4_addr | ipv6_addr > | <peer-group-name>} soft-reconfiguration
inbound
no neighbor {< ipv4_addr | ipv6_addr > | <peer-group-name>} soft-reconfigura-
tion
```

Enables neighbor soft reconfiguration.

The no form of the command disables neighbor soft reconfiguration.

<b>Syntax Description</b>	peer-group-name	Peer group name
	ipv4_addr	IPv4 address of the neighbor
	ipv6_addr	IPv6 address of the neighbor
<b>Default</b>	Enabled	
<b>Configuration Mode</b>	Config Router BGP	
<b>History</b>	3.6.4070	
<b>Role</b>	admin	
<b>Example</b>	switch (config router bgp 100)# neighbor 10.10.10.1 soft-reconfigura- tion inbound	
<b>Related Commands</b>		
<b>Note</b>		

## neighbor timers

```
neighbor {<ipv4_addr | ipv6_addr> | <peer-group-name>} timers <keep-alive>
<hold-time>
no neighbor {<ipv4_addr | ipv6_addr> | <peer-group-name>} timers
```

Configures the keepalive and hold times for a specified peer.

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

<b>Syntax Description</b>	ipv4_addr, ipv6_addr	IP address of the neighbor.
	peer-group-name	Peer group name
	keep-alive	<p>The period between the transmission of consecutive keep-alive messages</p> <ul style="list-style-type: none"> <li>• Range: 1-3600 seconds</li> <li>• “0” means that keepalive is not sent and the connection does not expire</li> <li>• Explicitly configuring the default, “60”, prevents the system from inheriting this parameter’s group configuration</li> </ul>
	hold-time	<p>The period the switch waits for a keepalive or update message before it disables peering</p> <ul style="list-style-type: none"> <li>• Range: 3-7200 seconds</li> <li>• “0” means that keepalive is not sent and the connection does not expire</li> <li>• Explicitly configuring the default, “180”, prevents the system from inheriting this parameter’s group configuration</li> </ul>
<b>Default</b>	keep-alive: 60 seconds hold-time: 180 seconds	
<b>Configuration Mode</b>	Config Router BGP	
<b>History</b>	3.3.5006	
	3.3.5200	Updated description
	3.6.3004	Updated “hold-time” and “keep-alive” parameter’s syntax description
	3.6.4070	Added IPv6 and IPv4 support
<b>Role</b>	admin	
<b>Example</b>	switch (config router bgp 100)# neighbor 10.10.10.10 timers 65 195	
<b>Related Commands</b>	neighbor <ip-address> remote-as <as-number>	
<b>Note</b>	Hold time must be at least 3 seconds and should be three times longer than the keepalive setting.	

## neighbor transport connection-mode passive

```
neighbor {<ipv4_addr | ipv6_addr> | <peer-group-name>} transport connection-mode
passive [disable]
no neighbor {<ipv4_addr | ipv6_addr> | <peer-group-name>} transport connection-mode passive
```

Sets the TCP connection for the specified BGP neighbor or peer group to passive mode.

The no form of the command sets the specified BGP neighbor or peer group to active connection mode.

<b>Syntax Description</b>	ipv4_addr, ipv6_addr peer-group-name disable	IP address of the neighbor Peer group name Sets the specified BGP neighbor or peer group to active connection mode and prevents the system from inheriting this parameter's group configuration
<b>Default</b>	TCP sessions initiated	
<b>Configuration Mode</b>	Config Router BGP	
<b>History</b>	3.4.0000 3.6.3004 3.6.4070	Added “disable” parameter Added IPv6 and IPv4 support
<b>Role</b>	admin	
<b>Example</b>	switch (config router bgp 100)# neighbor 10.10.10.10 transport connection-mode passive	
<b>Related Commands</b>		
<b>Note</b>	<ul style="list-style-type: none"> <li>When the peer’s transport connection mode is set to passive, it accepts TCP connections for BGP, but does not initiate them</li> <li>BGP peers in active mode can both accept and initiate TCP connections for BGP</li> </ul>	

## neighbor update-source

```
neighbor <ipv4_addr | ipv6_addr> update-source {ethernet <slot/port> | loopback <number> | port-channel <number> | vlan <vlan-id>}
no neighbor <ipv4_addr | ipv6_addr> update-source
```

Configures the source-address for routing updates and to establish TCP connections with peers.

The no form of the command disables configured source-address for routing updates and for TCP connection establishment with a peer.

<b>Syntax Description</b>	ipv4_addr, ipv6_addr	IP address of the neighbor.
	ethernet <slot/port>	Ethernet interface.
	loopback <number>	Loopback interface number.
	vlan <vlan-id>	VLAN interface. Range: 1-4094.
	port-channel <number>	LAG interface. Range is 1-4094.
<b>Default</b>	BGP uses best local address	
<b>Configuration Mode</b>	Config Router BGP	
<b>History</b>	3.3.5006	
	3.3.5200	Updated example
	3.6.4070	Added IPv6 and IPv4 support
<b>Role</b>	admin	
<b>Example</b>	<pre>switch (config router bgp 100)# neighbor 10.10.10.2 update-source vlan 10</pre>	
<b>Related Commands</b>	N/A	
<b>Note</b>		

## neighbor no-update-source

**neighbor <ip-address> no-update-source**

Disables configured source-address for routing updates and for TCP connection establishment with a peer and prevents the system from inheriting this parameter's group configuration.

<b>Syntax Description</b>	N/A
<b>Default</b>	BGP uses best local address
<b>Configuration Mode</b>	Config Router BGP
<b>History</b>	3.6.3004
<b>Role</b>	admin
<b>Example</b>	switch (config router bgp 100)# neighbor 10.10.10.2 no-update-source
<b>Related Commands</b>	N/A
<b>Note</b>	

## neighbor weight

```
neighbor {<ipv4_addr | ipv6_addr> | <peer-group-name>} weight <value>
no neighbor {<ipv4_addr | ipv6_addr> | <peer-group-name>} weight
```

Assigns a weight attribute to paths from the specified neighbor.  
The no form of the command resets to default values.

<b>Syntax Description</b>	ipv4_addr, ipv6_addr peer-group-name value	IP address of the neighbor Peer group name Weight value • Range: 1-65535 • Explicitly configuring a default value prevents the system from inheriting this parameter's group configuration
<b>Default</b>		Value is 32768 for router-originated paths and 0 for routes received through BGP
<b>Configuration Mode</b>		Config Router BGP
<b>History</b>	3.4.0000 3.6.4070	
		Added IPv6 and IPv4 support
<b>Role</b>	admin	
<b>Example</b>		switch (config router bgp 100)# neighbor 10.10.10.10 weight 100
<b>Related Commands</b>	N/A	
<b>Note</b>		<ul style="list-style-type: none"> <li>Weight values set through route map commands have precedence over neighbor weight command values.</li> <li>Other attributes are used only when all paths to the prefix have the same weight.</li> <li>A path's BGP weight is also configurable through route maps.</li> <li>When multiple paths to a destination prefix exist, the best-path selection algorithm prefers the path with the highest weight.</li> <li>Weight is the first parameter that the BGP best-path selection algorithm considers.</li> </ul>

## network

```
network <ipv4_prefix length | ipv6_prefix length> [<route-map-name>]
no network <ipv4_prefix length | ipv6_prefix length> [<route-map-name>]
```

Configures a route for advertisement to BGP peers.

The no form of the command removes the route from the BGP routes table, preventing its advertisement. The route is only advertised if the router has a gateway to the destination.

<b>Syntax Description</b>	ipv4_prefix, ipv6_prefix	A string that specific route map is assigned to the network.
	length	/24 or 255.255.255.0 format.
	route-map-name	The name of a route-map which is used to set the route's attributes when it is advertised.
<b>Default</b>	N/A	
<b>Configuration Mode</b>	Config Router BGP	
<b>History</b>	3.3.5006 3.3.5200 3.6.4070	
	Updated description, syntax description and notes Added IPv6 and IPv4 support	
<b>Role</b>	admin	
<b>Example</b>	<pre>switch (config router bgp 100)# network 10.10.10.0 /24 routemap</pre>	
<b>Related Commands</b>		
<b>Note</b>	<ul style="list-style-type: none"> <li>The parameters “ip-prefix” and “length” specify the route destination</li> <li>The configuration zeros the host portion of the specified network address (e.g. 192.0.2.4/24 is stored as 192.0.2.0/24)</li> <li>This command cannot be used with route-maps</li> </ul>	

## redistribute

```
redistribute {connected | static | ospf | ospf-internal | ospf-external} [<route-map>]
no redistribute {connected | static | ospf}
```

Enables redistribution of specified routes to the BGP domain.

The no form of the command disables route redistribution from the specified source.

<b>Syntax Description</b>	connected static ospf ospf-internal ospf-external	Redistributes the direct routes Redistributes the user-defined (static) route Redistributes all routes learned by OSPF protocol Redistributes all OSPF-learned routes which are marked as internal Redistributes all OSPF-learned routes which are marked as external
<b>Default</b>	No redistribution	
<b>Configuration Mode</b>	Config Router BGP	
<b>History</b>	3.2.1000	
<b>Role</b>	admin	
<b>Example</b>	switch (config router bgp 100)# redistribute ospf	
<b>Related Commands</b>	N/A	
<b>Note</b>	<ul style="list-style-type: none"> <li>Multiple redistribution options can be applied</li> <li>This command cannot be used with route-maps</li> </ul>	

## router-id

**router-id <ip-address> [force]**  
**no router-id [force]**

Configures a fixed router ID for BGP.

The no form of the command removes the fixed router ID and restores the system default.

<b>Syntax Description</b>	ip-address	IP Address identified the router ID
	force	Applies configuration while BGP is admin-up
<b>Default</b>	The Router ID is dynamically elected (no router-id).	<ul style="list-style-type: none"> <li>If a loopback interface is configured, the router ID is set to the IP address of the loopback interface.</li> <li>If multiple loopback interfaces are configured, the router ID is set to the IP address of the loopback interface with the highest IP address.</li> <li>If no loopback interface is configured, the router ID is set to the highest IP address on a physical interface.</li> </ul>
<b>Configuration Mode</b>	Config Router BGP	
<b>History</b>	3.3.5006	
	3.6.3004	Added “force” parameter
<b>Role</b>	admin	
<b>Example</b>	switch (config router bgp 100)# router-id 10.10.10.10	
<b>Related Commands</b>		
<b>Note</b>	The IP address configured identifies the BGP speaker. The command triggers an automatic notification and session reset for the BGP neighbors.	

## address-family

**address-family <ipv4-unicast | ipv6-unicast>**

Enables selected address family configuration mode.

<b>Syntax Description</b>	ipv4	IPv4 address family configuration mode
	ipv6	IPv6 address family configuration mode
<b>Default</b>	IPv4	
<b>Configuration Mode</b>	Config Router BGP	
<b>History</b>	3.6.4070	
<b>Role</b>	admin	
<b>Example</b>	switch (config router bgp)# address-family ipv4 switch (config router bgp)#{/td} <td data-kind="ghost"></td>	
<b>Related Commands</b>		
<b>Note</b>		

## neighbor activate

[no | disable] neighbor <ipv4\_addr | ipv6\_addr | peer\_group> activate

Enables advertisement of ipv4 or ipv6 capability and related network advertisements to specified neighbor or peer group.

The “no” form of the command disables advertisement of ipv4 or ipv6 capability and related network advertisements.

Syntax Description	ipv4_addr	Neighbor IPv4 address
	ipv6_addr	Neighbor IPv6 address
	peer_group	peer_group name
Default	N/A	
Configuration Mode	Config Router BGP	
History	3.6.4070	
	3.6.4110	Added “disable” option to the command
Role	admin	
Example	switch (config router bgp)# no neighbor 10.10.10.1 activate switch (config router bgp)#+	
Related Commands		
Note		

## neighbor default-originate

[no | disable] neighbor <ipv4\_addr | ipv6\_addr | peer\_group> default-originate  
[route\_map\_name]

Enables advertisement of the default route to a specified neighbor or peer group.  
The “no” form of the command disables advertisement of the default route.

Syntax Description	ipv4_addr	Neighbor IPv4 address
	ipv6_addr	Neighbor IPv6 address
	peer_group	Peer group's name
	route_map_name	route map name that modifies default route attributes
Default	N/A	
Configuration Mode	Config Router BGP	
History	3.6.4070	
	3.6.4110	Added “disable” option to the command
Role	admin	
Example	<pre>switch (config router bgp)# neighbor 10.10.10.1 default-originate default-attr switch (config router bgp)#+</pre>	
Related Commands		
Note		

## neighbor route-map

```
[no] neighbor <ipv4_addr | ipv6_addr | peer_group> route-map  
<route_map_name> [{in | out}]
```

Specifies a route map that will be applied to given neighbor in the given direction for specific address family.

The “no” form of the command removes the specified route map.

Syntax Description	
ipv4_addr	Neighbor IPv4 address
ipv6_addr	Neighbor IPv6 address
route_map_name	Route map name that modifies default route attributes
in/out	Specifies in which direction the route map is applied. If nothing is given - route map is applied in both directions
Default	N/A
Configuration Mode	Config Router BGP
History	3.6.4070
Role	admin
Example	<pre>switch (config router bgp)# neighbor 10.10.10.1 route-map default in switch (config router bgp)#{</pre>
Related Commands	
Note	

## network

[no] network <ipv4\_prefix length | ipv6\_prefix length> [<route\_map\_name>]

Adds the given prefix to advertisements that are sent with the specified address family.

The “no” form of the command removes the given prefix from advertisements that are sent with the specified address family.

Syntax Description	ipv4_prefix	IPv4 subnet
	ipv6_prefix	IPv6 subnet
	route_map_name	Route map name that modifies default route attributes
	length	Allowed prefix length is 24 for IPv4 and IPv6 or 255.255.0.0 for IPv4
Default	N/A	
Configuration Mode	Config Router BGP	
History	3.6.4070	
Role	admin	
Example	<pre>switch (config router bgp)# network 10.10.10.0 /24 default switch (config router bgp)#+</pre>	
Related Commands		
Note	Address family is identified by the network address itself and not by the configuration command context	

## redistribute

[no] [neighbor <peer\_group>] redistribute {connected | static}

Enables redistribution of routes to BGP in the specified address family or a peer-group in the address family.

The “no” form of the command disables the redistribution of routes to BGP.

<b>Syntax Description</b>	connected static peer_group	Redistributes direct routes Redistributes static routes Route map name that modifies default route attributes		
<b>Default</b>	N/A			
<b>Configuration Mode</b>	Config Router BGP			
<b>History</b>	3.6.4070			
<b>Role</b>	admin			
<b>Example</b>	switch (config router bgp)# redistribute connected switch (config router bgp)#{			
<b>Related Commands</b>				
<b>Note</b>				

## exit

exit

Exits address family configuration mode and returns to config router BGP mode.

**Syntax Description** N/A

**Default** N/A

**Configuration Mode** Config Router BGP

**History** 3.6.4070

**Role** admin

**Example**  
`switch (config router bgp)# exit  
switch (config router bgp)#{/code}`

**Related Commands**

**Note**

## route-map

[no] [neighbor <peer\_group>] route-map <route\_map\_name> [{in | out}]

Specifies a route map that will be applied in the given direction for specific address family.

<b>Syntax Description</b>	route_map_name	Name of a route map to apply.
	in/out	Specifies in which direction the route map is applied. If nothing is given - route map is applied in both directions
	peer_group	Peer group name
<b>Default</b>	N/A	
<b>Configuration Mode</b>	Config Router BGP	
<b>History</b>	3.6.4070	
<b>Role</b>	admin	
<b>Example</b>	switch (config router bgp)# route-map default in switch (config router bgp)#	
<b>Related Commands</b>		
<b>Note</b>		

## bgp default

[no] bgp default {ipv4-unicast | ipv6-unicast}

Enables to set address families as default for peer or peer-group activation.

<b>Syntax Description</b>	ipv4-unicast	IPv4 unicast address family, enabled by default.
	ipv6-unicast	IPv6 unicast address family, disabled by default.
<b>Default</b>	N/A	
<b>Configuration Mode</b>	Config Router BGP	
<b>History</b>	3.6.4070	
	3.6.4110	Added support for IPv6
<b>Role</b>	admin	
<b>Example</b>	switch (config router bgp)# bgp default ipv4-unicast switch (config router bgp)#	
<b>Related Commands</b>		
<b>Note</b>	This command can be used multiple times and each address family can be configured separately.	

### 6.4.7.3 Show

#### show ip bgp

**show ip bgp [vrf <vrf-name>] [<ipv4-prefix> <length> [detail | longer-prefixes [detail]]]**

**show ipv6 bgp [vrf <vrf-name>] [<ipv6\_prefix> <length> [detail | longer-prefixes [detail]]]**

Displays information about the BGP routes table (RIB).

<b>Syntax Description</b>	ipv4_prefix, ipv6_prefix	IPv4 and IPv6 subnet
	length	Netmask (e.g. /24 or 255.255.255.0).
	detail	Displays detailed information about a subset of the bgp learned routes.
	longer-prefixes	Displays the routes to the specified destination and any routes to a more specific destination. Example: If “10.20.30.0 /24 longer-prefixes” is run, all routes starting with 10.20.30 regardless of the prefix length (10.20.30.X /24, 10.20.30.X /25, etc.) are displayed – providing there are any such routes received/sent from/to that neighbor.
<b>Default</b>	N/A	
<b>Configuration Mode</b>	Any Command Mode	
<b>History</b>	3.3.5200	
<b>History</b>	3.6.4070	
<b>Role</b>	Added support for IPv4 and IPv6 admin	

---

**Example**

```
switch (config) # show ip bgp
BGP table version is 100/200, local router ID is 16.0.1.1
Status codes: * valid, > best, i - internal, m multipath
Origin codes: i - IGP, e - EGP, ? - incomplete
Network          NextHop Metric LocPrf Weight Path
20.20.20.0/24    2.2.2.2  0      2      20      e
100.100.100.0/24 2.2.2.2  0      2      50      100 e
100.100.100.0/24 2.2.2.12 0      12     50      100 e

(config) # show ip bgp 50.50.0.0 /24 detail
BGP routing table entry for 50.50.0.0/24
Paths: (2, best #1)
[5 13 22]
  2001::1 from 2003::10 (2003::9)
    Origin IGP, metric 0, localpref 0, weight 32768, valid, best
    Communities: 1:2 1:3
    Originator-ID: 9.8.7.6
    Cluster-List: 0.0.0.1 0.0.0.2 0.0.0.3
  2001::1 from 2003::10 (2003::9)
    Origin IGP, metric 0, localpref 100, valid
    Communities: 5:200 10:255 no-export

switch (config) #
```

---

**Related Commands** N/A

---

**Note**

## **show ip bgp community**

```
show ip bgp [vrf <vrf-name>] community <comm1> <comm2> ... <commn>  
[exact] [detail]
```

Displays information about the BGP routes (RIB) filtered according to communities.

---

**Related Commands** N/A

---

**Note**

---

## show ip bgp neighbors

```
show {< ip >} bgp neighbors [vrf <vrf-name>] [<ipv6_addr | ipv4_addr>]
show {< ip >} bgp neighbors [vrf <vrf-name>] <ipv6_addr | ipv4_addr> received
[<ip4_prefix | ipv6_prefix> [<mask | length>] [longer-prefixes]]
```

Displays summaries information about all BGP neighbors.

<b>Syntax Description</b>	ipv4_prefix, ipv6_prefix	Destination to aggregate
	length	Mask length (e.g. /24 or 255.255.255.254)
	ip[v6]_addr	neighbor address
	longer-prefixes	Displays information about routes with longer prefixes than given
<b>Default</b>	N/A	
<b>Configuration Mode</b>	Any Command Mode	
<b>History</b>	3.3.5200	
	3.6.4070	Added support for IPv4 and IPv6
<b>Role</b>	admin	

**Example**

```

switch (config) # show ip bgp neighbors
BGP neighbor is 9.9.9.150, remote AS 44, external link
    BGP version 4, remote router ID 170.148.0.9
    BGP State = ESTABLISHED
    Last read 0:00:00:29, last write 0:00:00:29, hold time is 90, keep-
alive interval is 30 seconds
    Configured hold time is 180, keepalive interval is 60 seconds
    Minimum holdtime from neighbor is 90 seconds

switch# show ip bgp neighbors 9.9.9.150
BGP neighbor is 9.9.9.150, remote AS 44, external link
    BGP version 4, remote router ID 170.148.0.9
    BGP State = ESTABLISHED
    Last read 0:00:00:43, last write 0:00:00:43, hold time is 90, keep-
alive interval is 30 seconds

Neighbor capabilities:
    Route refresh: advertise and received
    Graceful Restart Capability: advertise
    Address family IPv4 Unicast: advertise and received
    Address family IPv6 Unicast: advertise and received

Message statistics:
    InQ depth is 0
    OutQ depth is 0
      Sent          Rcvd
    Opens:           1          1
    Notifications:  0          0
    Updates:        4          1
    Keepalives:     2          3
    Route Refresh:  0          0
    Total:          7          5
Default minimum time between advertisement runs is 30 seconds

For address family: IPv6 Unicast
    BGP table version 5
    Output queue size : 0

      Sent          Rcvd
Prefix activity:  -----
    Prefixes Current:   18          1
    Prefixes Total:     18          1
    Implicit Withdraw:  0          0
    Explicit Withdraw:  0          0
    Used as bestpath:   n/a         1
    Used as multipath:  n/a         n/a

      Outbound      Inbound
Local Policy Denied Prefixes:  -----
    Total:            2          0

Connections established 1; dropped 0
Last reset 0:00:00:45, due to 0 (0)
Connection state is ESTABLISHED
Local host: 1.2.3.4, Local port: 179
Foreign host: 9.9.9.150, Foreign port: 54933

switch (config) # show ipv6 bgp neighbors 2001::1 received
BGP table version is 100/10, local router ID is 16.0.1.1
Status codes: * valid, > best, i - internal, m multipath
Origin codes: i - IGP, e - EGP, ? - incomplete
Network          Next Hop Metric LocPrf Weight Path
*> 100.0.20.0/24  3.5.7.5 10    100    0      5      i

```

---

**Related Commands** N/A

---

**Note**

---

## show ip bgp neighbors <ip> received

**show ip bgp neighbors <ip-address> received [<ip-address> [<mask>] [longer-prefixes]]**

Displays BGP summary information.

<b>Syntax Description</b>	ip-address longer-prefixes	Neighbor IP address Displays the routes to the specified destination and any routes to a more specific destination. (Only available if both IP and mask are specified.)
<b>Default</b>	N/A	
<b>Configuration Mode</b>	Any Command Mode	
<b>History</b>	3.3.5200	
<b>Role</b>	admin	
<b>Example</b>		
<b>Related Commands</b>	N/A	
<b>Note</b>		

## **show ip bgp paths**

**show ip bgp paths [vrf <vrf-name>] [ipv4 | ipv6]**

Displays summary of all AS paths and for prefixes for specific address family.

## show ip bgp peer-group

**show ip bgp peer-group [vrf <vrf-name>] [peer-group-name] [address-family <ipv4 | ipv6>]**

Displays information about peer groups and configuration, filtered per address family.

<b>Syntax Description</b>	peer-group-name	Displays information about a specific peer-group.
<b>Default</b>	N/A	
<b>Configuration Mode</b>	Any Command Mode	
<b>History</b>	3.4.0000	
	3.6.4070	Added support for IPv4 and IPv6
<b>Role</b>	admin	
<b>Example</b>	<pre>switch (config) # show ip bgp peer-group BGP Peer-group [grpA]: Hold time: 1, Keepalive: 60 Allow as-in: 0 Weight: 32768 Max prefix: 12000 Export local preferences: 100, Import local preferences: 100 Soft reconfiguration: set Neighbor      V      AS MsgRcvd MsgSent TblVer InQ OutQ Up/Down State/PfxRcd 3.5.7.5        0        5      0      0      0      0      0 0:00:00:42 CONNECT 100.100.100.100  0     100      0      0      0      0      0 Never IDLE  BGP Peer-group [grpB]: Hold time: 1, Keepalive: 60 Allow as-in: 0 Weight: 32768 Max prefix: 12000 Export local preferences: 100, Import local preferences: 100 Soft reconfiguration: set Neighbor      V      AS MsgRcvd MsgSent TblVer InQ OutQ Up/Down State/PfxRcd 3.4.3.7        0        7      0      0      0      0      0 0:00:00:17 ACTIVE  BGP Peer-group [tomer_group]: Hold time: 1, Keepalive: 60 Allow as-in: 0 Weight: 32768 Max prefix: 12000 Export local preferences: 100, Import local preferences: 100 Soft reconfiguration: set  Peer-groups count: 3 switch-e07c04 [standalone: master] (config) #</pre>	

---

**Related Commands** N/A

---

**Note**

---

## **show ip bgp summary**

**show ipv6 bgp summary [vrf <vrf-name>]**

Displays BGP summary for IPv6 addresses.

## show ip bgp address-family

**show ip bgp address-family [vrf <vrf-name>] <ipv4-unicast | ipv6-unicast> [active]**

Displays address-family configuration.

<b>Syntax Description</b>	active	Displays active neighbors in that address family (configured, active or dynamic)
<b>Default</b>	N/A	
<b>Configuration Mode</b>	Any Command Mode	
<b>History</b>	3.6.4070	
<b>Role</b>	admin	
<b>Example</b>	<pre>switch (config) # show ip bgp address-family ipv4 &lt;detail&gt; Address family: IPv4 Networks: &lt;list of advertised networks&gt; 1.2.3.4 /24 route-map default 2.3.4.5 /28 route-map security in advertisement interval - 10 route-map top_security out send-community - off maximum-path 20 redistribute - static ...&lt;all address family current configuration&gt; Total neighbors: 50 &lt;not brief - list of neighbors&gt; Total peer-groups: 2 &lt;not brief - list of peer-groups&gt; Peer group: groupA Peer group: groupB Total dynamic ranges: 4 &lt;not brief - list of ranges&gt; Listen peer group: groupC</pre>	
<b>Related Commands</b>	N/A	
<b>Note</b>		

## show ip bgp update-group

**show ip bgp update-group [<neighbor ip address>]**

Displays update-group information for all neighbors.

<b>Syntax Description</b>	N/A
<b>Default</b>	N/A
<b>Configuration Mode</b>	Any Command Mode
<b>History</b>	3.6.4070
<b>Role</b>	admin
<b>Example</b>	<pre>switch (config) # show ip bgp update-group BGP version 4 Address Family: IPv4 Unicast   BGP Update version : 0, messages 0/0   Update messages formatted 0, replicated 0   Number of NLRI's in the update sent: max 0, min 0   Minimum time between advertisement runs is 5 seconds   Has 1 member:     10.4.9.21  switch&gt;# switch (config)# show ip bgp update-group 2001::1  Update-group for neighbor 2001::1: ----- BGP router identifier 10.4.9.4, local AS number 101 BGP table version is 1, main routing table version 1 Neighbor V AS MsgRcvd MsgSent InQ OutQ Up/Down      State/PfxRcd 2001::1  4 7          3        9   0     0 0:00:00:48 ESTABLISHED</pre>
<b>Related Commands</b>	N/A
<b>Note</b>	

## 6.4.8 IP AS-Path Access-List

### 6.4.8.1 Commands

#### ip as-path access-list

```
ip as-path access-list <list-name> {permit | deny} <reg-exp> [any | egp | igr | incomplete]
no ip as-path access-list <list-name>
```

Creates an access list to filter BGP route updates.

The no ip as-path access-list command deletes the named access list.

<b>Syntax Description</b>	list-name	The name for the access list
	permit	Permits access for a matching condition
	deny	Denies access for a matching condition
	reg-exp	Regular expression that is used to specify a pattern to match against an input string.
	any	Any route type
	egp	External BGP routes
	igr	Internal BGP routes
	incomplete	Routes marked as “Incomplete”
<b>Default</b>	N/A	
<b>Configuration Mode</b>	Config	
<b>History</b>	3.4.0000	
<b>Role</b>	admin	
<b>Example</b>	<pre>switch (config)# ip as-path access-list mylist permit switch (config)#+</pre>	
<b>Related Commands</b>	N/A	
<b>Note</b>	If access list_name does not exist, this command creates it. If it already exists, this command appends statements to the list.	

## show ip as-path access-list

**show ip as-path access-list [list-name]**

Presents defined as-path access lists

<b>Syntax Description</b>	list-name	Displays a specific prefix-list.
<b>Default</b>	N/A	
<b>Configuration Mode</b>	Config	
<b>History</b>	3.4.0000	
<b>Role</b>	admin	
<b>Example</b>	switch (config)# show ip as-path access-list mylist	
<b>Related Commands</b>	N/A	
<b>Note</b>		

## 6.4.9 IP Community-List

### 6.4.9.1 Commands

#### ip community-list standard

```
ip community-list standard <list-name> {deny | permit} <list-of-communities>
no ip community-list standard <list-name>
```

Adds a standard entry to a community-list.

The no form of the command deletes the specified community list.

<b>Syntax Description</b>	<table border="0"> <tr> <td>list-name</td><td>The name for the community list</td></tr> <tr> <td>permit</td><td>Permits access for a matching condition.</td></tr> <tr> <td>deny</td><td>Denies access for a matching condition.</td></tr> </table>	list-name	The name for the community list	permit	Permits access for a matching condition.	deny	Denies access for a matching condition.
list-name	The name for the community list						
permit	Permits access for a matching condition.						
deny	Denies access for a matching condition.						
	<table border="0"> <tr> <td>list-of-communities</td><td>List of standard communities:           <ul style="list-style-type: none"> <li>• &lt;aa:nn&gt;</li> <li>• &lt;number&gt;</li> <li>• internet</li> <li>• local-AS</li> <li>• no-advertise</li> <li>• no-export</li> </ul> </td></tr> </table>	list-of-communities	List of standard communities: <ul style="list-style-type: none"> <li>• &lt;aa:nn&gt;</li> <li>• &lt;number&gt;</li> <li>• internet</li> <li>• local-AS</li> <li>• no-advertise</li> <li>• no-export</li> </ul>				
list-of-communities	List of standard communities: <ul style="list-style-type: none"> <li>• &lt;aa:nn&gt;</li> <li>• &lt;number&gt;</li> <li>• internet</li> <li>• local-AS</li> <li>• no-advertise</li> <li>• no-export</li> </ul>						
<b>Default</b>	N/A						
<b>Configuration Mode</b>	Config						
<b>History</b>	3.4.0000						
<b>Role</b>	admin						
<b>Example</b>	<pre>switch (config)# ip community-list standard mycommunity permit 1:2 3:4</pre>						
<b>Related Commands</b>	N/A						
<b>Note</b>	A BGP community access list filters route maps that are configured as BGP communities. The command uses regular expressions to name the communities specified by the list.						

## ip community-list expanded

```
ip community-list expanded <list-name> {deny | permit} <reg-exp>
no ip community-list expanded <list-name>
```

Adds a regular expression entry to a community-list  
The no form of the command deletes the specified community list.

Syntax Description	
list-name	Configures a named standard community list.
permit	Permits access for a matching condition.
deny	Denies access for a matching condition.
reg-exp	Regular expression that is used to specify a pattern to match against an input string.
<b>Default</b>	N/A
<b>Configuration Mode</b>	Config
<b>History</b>	3.4.0000
<b>Role</b>	admin
<b>Example</b>	<pre>switch (config)# ip community-list expanded mycommunity permit 1:[0-9]+</pre>
<b>Related Commands</b>	N/A
<b>Note</b>	A BGP community access list filters route maps that are configured as BGP communities. The command uses regular expressions to name the communities specified by the list.

## show ip community-list

**show ip community-list [community-list-name]**

Displays the defined community lists

<b>Syntax Description</b>	community-list-name	An optional parameter to display only the specified list
<b>Default</b>	N/A	
<b>Configuration Mode</b>	Config	
<b>History</b>	3.4.0000	
<b>Role</b>	admin	
<b>Example</b>	switch (config)# show ip community-list mycommunity	
<b>Related Commands</b>	N/A	
<b>Note</b>	A BGP community access list filters route maps that are configured as BGP communities. The command uses regular expressions to name the communities specified by the list.	

## 6.5 BFD Infrastructure

Many protocols uses slow Hello mechanisms and failure is detection usually seconds after the problem occurs. The BFD goal is to provide low overhead short duration detection of failures between adjacent nodes and single mechanism that can be used for liveness detection over any media.

BFD session is established by the application that uses it. There is no discovery mechanism. E.g. in OSPF BFD session is established to all neighbors that were discovered by OSPF hello protocol.

BFD supports multiple modes: one of them is Asynchronous.

In Asynchronous mode a system periodically sends BFD packets to verify connectivity. If a number of packets in a row are not received – the session is declared down.

A system can be passive or active. Active system initiates BDF sessions. Both systems can be active. (Only active mode is supported.)

### 6.5.1 Session Establishment

A session begins with exchange of control packets. When bidirectional communication is achieved - a session becomes Up.

After session becomes up - control packet rate can be incremented.

Each side informs the neighbor in what intervals it is going to send BFD packets and what minimum interval it can receive BFD packets is.

Detection time is different in both directions and depends on negotiated parameters.

In Asynchronous mode—agreed transmit interval or remote system—max between local minimum rx time and last received min transmit time.

Detection time is equal to agreed transmit interval of remote system multiplied to multiplier received from remote system.

### 6.5.2 Interaction with Protocols

BFD session can be single-hop or multi-hop:

- Single hop session traverse between two adjacent IP neighbors. BFD control packet should be encapsulated in UDP with DPORT = 3784. SPORT should be in range 49152 to 65535. Same SPORT must be used for all control BFD packets for given session and is unique between different sessions. TTL value is 255.
- Multi-hop sessions traverse between to remote ip neighbors. Control packets are encapsulated in UDP with DPORT = 4784.

If different protocols want to establish a BFD session with the same remote system for same data plane - they should share BFD session.

IPv4 and IPv6 data protocols have different BFD sessions.

In OSPF Protocol neighbor discovery protocol establishes single hop BFD sessions. For OSPF when session fails - it tears down OSPF neighbor.

BFD session is established to BGP neighbor (single hop or multiple hop).

Single hop BFD session can be established for static route next hop.

## 6.5.3 Config Commands

### protocol bfd

[no] protocol bfd

Enables bfd on a system level

The no form of the command removes bfd configuration.

<b>Syntax Description</b>	N/A
<b>Default</b>	N/A
<b>Configuration Mode</b>	Config Router BGP
<b>History</b>	3.6.4070
<b>Role</b>	admin
<b>Example</b>	<pre>switch (config router bgp)# bfd shutdown switch (config router bgp)#{/pre}</pre>
<b>Related Commands</b>	
<b>Note</b>	The command will return an error if BFD is enabled in clients already running on the system (static routes or BGP or OSPF).

## bfd shutdown

[no] bfd shutdown [vrf <vrf-name>]

Disables bfd sessions but doesn't remove the configuration  
if VRF is not given the command will be executed in active VRF.

<b>Syntax Description</b>	N/A
<b>Default</b>	N/A
<b>Configuration Mode</b>	Config Router BGP
<b>History</b>	3.6.4070
<b>Role</b>	admin
<b>Example</b>	<pre>switch (config router bgp)# bfd shutdown switch (config router bgp)#{/pre}</pre>
<b>Related Commands</b>	
<b>Note</b>	"no ip bfd shutdown" or BFD interval parameters modification are affect traffic for all protocols; OSPF, BGP, static routes. The dynamic protocols (OSPF and BGP) will restore the connection based on Hello protocol. For static routes, please execute "no ip route static bfd <ip address>"

## 6.5.4 Interface Commands

### bfd interval

**[no] bfd interval [vrf <vrf-name>] [transmit\_rate] [min\_rx] [multiplier]**

Sets the interval rates between BFD messages.

The no form of the command removes bfd interval rates.

<b>Syntax Description</b>	transmit_rate	Transfer time between two consecutive BFD messages, the actual time is negotiated between two systems. Range: 50-60000 (msec) Default: 300 (msec)
	min_rx	Minimum time between neighbor messages, the actual time is negotiated between two systems. Range: 50-60000 (msec) Default: 150 (msec)
	multiplier	Defines a time period to detect BFD failure. Range: 3-50 Default: 3
<b>Default</b>	N/A	
<b>Configuration Mode</b>	Config	
<b>History</b>	3.6.4070	
<b>Role</b>	admin	
<b>Example</b>	<pre>switch (config router bgp)# bfd shutdown switch (config router bgp)# </pre>	
<b>Related Commands</b>		
<b>Note</b>	The command is executed in Active VRF when VRF is not specified.	

## ip ospf bfd

[no] ip ospf bfd

Enables BFD on the given interface for all OSPF neighbors on a number of active sessions.

The no form of the command disables BFD on all OSPF neighbors.

<b>Syntax Description</b>	N/A
<b>Default</b>	N/A
<b>Configuration Mode</b>	Config Interface Ethernet
<b>History</b>	3.6.4070
	3.6.4110                          Added “no” form of the command.
<b>Role</b>	admin
<b>Example</b>	switch (config interface ethernet)# ip ospf bfd
<b>Related Commands</b>	N/A
<b>Note</b>	"ip ospf bfd" affects traffic, OSPF will restore the connection based on Hello protocol.

## ip route static bfd

```
ip route [vrf <vrf-name>] static bfd <gateway IP address>
no ip route [vrf <vrf-name>] static bfd <gateway IP address>
```

Configures a static bfd route inside VRF.

The no form of the command removes the static bfd route configured.

<b>Syntax Description</b>	vrf-name	VRF session name
	gateway IP address	IP address of the gateway.
<b>Default</b>	N/A	
<b>Configuration Mode</b>	Config	
<b>History</b>	3.6.4070	
<b>Role</b>	admin	
<b>Example</b>	switch (config) # ip route static bfd	
<b>Related Commands</b>	N/A	
<b>Notes</b>	When a session fails, all static routes pointing to the specified gateway are removed from routing decision.	

## show ip static route bfd

**show ip static route bfd [vrf <vrf-name> | all]**

Displays bfd static routing table of VRF instance.

<b>Syntax Description</b>	all	Displays routing tables for all VRF instances
<b>Default</b>	N/A	
<b>Configuration Mode</b>	Any Command Mode	
<b>History</b>	3.6.4070	
<b>Role</b>	admin	
<b>Example</b>	switch (config) # show ip static route bfd	
<b>Related Commands</b>	ip route	
<b>Notes</b>	<ul style="list-style-type: none"><li>If no routing-context is specified, the “routing-context” VRF is automatically displayed</li><li>If no default route exists, then the message “Route not found” is printed</li></ul>	

## show ip bfd neighbors

**show ip bfd [vrf <name>|all] neighbors [brief]<ip>]**

Displays bfd table of neighbor VRF instances.

<b>Syntax Description</b>	all	Displays tables for all VRF instances
<b>Default</b>	N/A	
<b>Configuration Mode</b>	Any Command Mode	
<b>History</b>	3.6.4110	
<b>Role</b>	admin	

## Example

```

switch (config) # show ip bgp neighbors 1000::1040
BGP neighbor: 1000::1040, remote AS: 100, link: external
  BGP version: 4, remote router ID: 2.1.1.1
  BGP State: ESTABLISHED
  Last read: 0:00:09:28, last write: 0:00:09:28, hold time is: 180, keepalive interval in seconds: 60
  BFD State: Up
  Configured hold time in seconds: 180, keepalive interval in seconds: 60
  Minimum holdtime from neighbor in seconds: 180

  Neighbor capabilities:
    Route refresh: advertise and received
    Graceful Restart Capability: advertise and received
    Address family IPv4 Unicast: advertise and received
    Address family IPv6 Unicast: n/a

  Message statistics:
    InQ depth is: 0
    OutQ depth is: 0
    -----
    Sent      Rcvd
    -----  -----
    Opens:        1      1
    Notifications: 0      0
    Updates:       4      4
    Keepalives:   1587   1593
    Route Refresh: 0      0
    Total:        1592   1598
    Default minimum time between advertisement runs in seconds: 30

    For address family: IPv4 Unicast
    BGP table version: 7
    Output queue size : 0

    -----
    Sent      Rcvd
    -----  -----
    Prefix activity:  -----
    Prefixes Current: 4      2
    Prefixes Total:    4      2
    Implicit Withdraw: 0      0
    Explicit Withdraw: 0      0
    Used as bestpath:  n/a     2
    Used as multipath: n/a    n/a

    -----
    OutboundInbound
    Local Policy Denied Prefixes:-----
    Total:          0      0

    Connections established: 1; dropped: 1
    Last reset: 0:23:01:17, due to: 0 (0)
    External BGP neighbor possible distance in hops: 1
    Connection state is: ESTABLISHED
    Local host: 1.1.1.1, Local port: 49616
    Foreign host: 1000::1040, Foreign port: 179

```

## Related Commands

### Notes

## 6.6 Policy Rules

### 6.6.1 Route Map

Route maps define conditions for redistributing routes between routing protocols. A route map clause is identified by a name, filter type (permit or deny) and a sequence number. Clauses with the same name are components of a single route map; the sequence number determines the order in which the clauses are compared to a route.



Route maps can be used only for the BGP protocol.



Route maps cannot be used for the commands “network” on page 1249 or “redistribute” on page 1250.

### 6.6.1.1 Commands

#### route-map

```
route-map <map-name> [deny | permit] [sequence-number]
no route-map <map-tag> {deny | permit} [<sequence-number>]
```

Creates a route map that can be used for importing, exporting routes and applying local policies.

<b>Syntax Description</b>	<table> <tr> <td>name</td><td>Name of the route-map</td></tr> <tr> <td>deny   permit</td><td>Configures the rule to be used</td></tr> <tr> <td>sequence-number</td><td>Sequence number for a route-map specific record</td></tr> </table>	name	Name of the route-map	deny   permit	Configures the rule to be used	sequence-number	Sequence number for a route-map specific record
name	Name of the route-map						
deny   permit	Configures the rule to be used						
sequence-number	Sequence number for a route-map specific record						
<b>Default</b>	N/A						
<b>Configuration Mode</b>	Config						
<b>History</b>	<table> <tr> <td>3.3.5006</td><td></td></tr> <tr> <td>3.3.5200</td><td>Updated notes</td></tr> </table>	3.3.5006		3.3.5200	Updated notes		
3.3.5006							
3.3.5200	Updated notes						
<b>Role</b>	admin						
<b>Example</b>	<pre>switch (config) # route-map mymap permit 1200 switch (config route-map mymap permit 1200)#</pre>						
<b>Related Commands</b>	N/A						
<b>Note</b>	<ul style="list-style-type: none"> <li>• All changes in a the route map configuration mode become pending until the end of the route-map session.</li> <li>• If not configured, deny   permit is configured as permit</li> <li>• If not configured, sequence-number default value is 10</li> </ul>						

## continue <sequence-number>

**continue <sequence-number>**  
**no continue**

Enables additional route map evaluation of routes whose parameters meet the clause's matching criteria.

The no form of the command removes this configuration from the route map clause.

<b>Syntax Description</b>	sequence-number
<b>Default</b>	N/A
<b>Configuration Mode</b>	Config Route Map
<b>History</b>	3.3.5006 3.3.5200 Updated example
<b>Role</b>	admin
<b>Example</b>	<pre>switch (config route-map mymap permit 10)# match as-number 40 switch (config route-map mymap permit 10)# set weight 7 switch (config route-map mymap permit 10)# continue 1200 switch (config route-map mymap permit 10)# exit switch (config)# show route-map test route-map test, permit, sequence 10     Match clauses:         as-number 40     Set clauses:         weight 7         continue 1200 switch (config route-map mymap permit 10)# route-map test permit 10 no continue switch (config route-map mymap permit 10)# show route-map test route-map test, permit, sequence 10     Match clauses:         as-number 40     Set clauses:         weight 7 switch (config route-map mymap permit 10)# </pre>

**Related Commands**`route-map <map-name> [deny | permit] [sequence-number]`**Note**

- A clause typically contains a match (route-map) and a set (route-map) statement. The evaluation of routes whose settings are the same as match statement parameters normally end and the clause's set statement are applied to the route. Routes that match a clause containing a continue statement are evaluated against the clause specified by the continue statement.
- When a route matches multiple route-map clauses, the filter action (deny or permit) is determined by the last clause that the route matches. The set statements in all clauses matching the route are applied to the route after the route map evaluation is complete. Multiple set statements are applied in the same order by which the route was evaluated against the clauses containing them.
- Continue cannot be set to go back to a previous clause; <sequence-number> of the continue must always be higher than the current clause's sequence number.

## abort

### abort

Discards pending changes and returns to global configuration mode.

<b>Syntax Description</b>	N/A
<b>Default</b>	N/A
<b>Configuration Mode</b>	Config Route Map
<b>History</b>	3.3.5006 3.3.5200 Updated example
<b>Role</b>	admin
<b>Example</b>	<pre>switch (config)# route-map mymap permit 10 match as-number 40 switch (config)# route-map mymap permit 10 set weight 7 switch (config)# show route-map test route-map test, permit, sequence 10   Match clauses:     as-number 40   Set clauses:     weight 7 switch (config)# route-map mymap permit 1200 switch (config route-map mymap permit 1200)# set weight 11 switch (config route-map mymap permit 1200)# abort switch (config)# show route-map mymap route-map mymap, permit, sequence 10   Match clauses:     as-number 40   Set clauses:     weight 7 switch (config)# </pre>
<b>Related Commands</b>	N/A
<b>Note</b>	

## exit

### exit

Saves pending route map clause changes to running-config and returns to global configuration mode.

<b>Syntax Description</b>	N/A
<b>Default</b>	N/A
<b>Configuration Mode</b>	Config Route Map
<b>History</b>	3.3.5006
<b>Role</b>	admin
<b>Example</b>	<pre>switch (config)# route-map mymap permit 10 match as-number 40 switch (config)# route-map mymap permit 10 set weight 7 switch (config)# show route-map test route-map test, permit, sequence 10   Match clauses:     as-number 40   Set clauses:     weight 7 switch (config)# route-map mymap permit 1200 switch (config route-map mymap permit 1200)# set weight 11 switch (config route-map mymap permit 1200)# exit switch (config)# show route-map test route-map mymap, permit, sequence 10   Match clauses:     as-number 40   Set clauses:     weight 7 route-map mymap, permit, sequence 1200   Set clauses:     weight 11 switch (config)# </pre>
<b>Related Commands</b>	N/A
<b>Note</b>	

## match as-number

```
match as-number <number>
no match as-number
```

Filters according to one of the AS numbers in the AS path of the route.  
The no form of the command removes this configuration from the route map clause.

<b>Syntax Description</b>	number	Autonomous system number to check.
<b>Default</b>	N/A	
<b>Configuration Mode</b>	Config Route Map	
<b>History</b>	3.3.5006	
<b>Role</b>	admin	
<b>Example</b>	<pre>switch (config route-map mymap permit 10)# match as-number 40 switch (config route-map mymap permit 10)# </pre>	
<b>Related Commands</b>	N/A	
<b>Note</b>	<ul style="list-style-type: none"><li>When a clause contains multiple match commands, the permit or deny filter applies to a route only if its properties are equal to corresponding parameters in each match statement.</li><li>When a route's properties do not equal the statement parameters, the route is evaluated against the next clause in the route map, as determined by sequence number.</li><li>If all clauses fail to permit or deny the route, the route is denied.</li></ul>	

## match as-path

**match as-path <as-path-list name>**  
**no match as-path**

Creates a route map clause entry that matches the route's AS path using an as-path access-list.

The no form of the command removes the match statement from the configuration mode route map clause.

<b>Syntax Description</b>	number	Autonomous system number to check.
<b>Default</b>	N/A	
<b>Configuration Mode</b>	Config Route Map	
<b>History</b>	3.3.5006	
	3.6.3004	Added note
<b>Role</b>	admin	
<b>Example</b>	switch (config route-map mymap permit 10)# match as-path my-list	
<b>Related Commands</b>	N/A	
<b>Note</b>	<ul style="list-style-type: none"> <li>• When a clause contains multiple match commands, the permit or deny filter applies to a route only if its properties are equal to corresponding parameters in each match statement</li> <li>• When a route's properties do not equal the statement parameters, the route is evaluated against the next clause in the route map, as determined by sequence number</li> <li>• If all clauses fail to permit or deny the route, the route is denied</li> <li>• An as-path-list must already exist before a node is configured to use it</li> </ul>	

## match community

**match community <list-of-communities> [exact-match]  
no match community <list-of-communities>**

Creates a route map clause entry that matches a route if it contains at least the specified communities.

The no form of the command removes the match clause.

<b>Syntax Description</b>	list of communities	List of standard communities: <ul style="list-style-type: none"> <li>• &lt;aa:nn&gt;</li> <li>• &lt;number&gt;</li> <li>• internet</li> <li>• local-AS</li> <li>• no-advertise</li> <li>• no-export</li> </ul>
	exact-match	Creates a route map clause entry that matches the route's communities exactly.
<b>Default</b>	N/A	
<b>Configuration Mode</b>	Config Route Map	
<b>History</b>	3.3.5006	
<b>Role</b>	admin	
<b>Example</b>	switch (config route-map mymap permit 10)# match community 1:100 3:52	
<b>Related Commands</b>	N/A	
<b>Note</b>	<ul style="list-style-type: none"> <li>• When a clause contains multiple match commands, the permit or deny filter applies to a route only if its properties are equal to corresponding parameters in each match statement.</li> <li>• When a route's properties do not equal the statement parameters, the route is evaluated against the next clause in the route map, as determined by sequence number.</li> <li>• If all clauses fail to permit or deny the route, the route is denied.</li> <li>• Route-map's match on a list of communities is performed with the command "match community-list" and not this command.</li> </ul>	

## match community-list

```
match community <communities-list-name> exact-match
no match community <communities-list-name> exact-match
```

Creates a route map clause entry that specifies one route filtering condition  
The no form of the command removes the match clause.

<b>Syntax Description</b>	communities-list-name	A name of an IP community list
<b>Default</b>	N/A	
<b>Configuration Mode</b>	Config Route Map	
<b>History</b>	3.3.5006	
<b>Role</b>	admin	
<b>Example</b>	<pre>switch (config route-map mymap permit 10)# match community-list COM_LIST exact-match</pre>	
<b>Related Commands</b>	N/A	
<b>Note</b>	<ul style="list-style-type: none"><li>When a clause contains multiple match commands, the permit or deny filter applies to a route only if its properties are equal to corresponding parameters in each match statement.</li><li>When a route's properties do not equal the statement parameters, the route is evaluated against the next clause in the route map, as determined by sequence number.</li><li>If all clauses fail to permit or deny the route, the route is denied.</li></ul>	

## match interface

**match interface <interface-type> <number>**  
**no match interface**

Matches the route's interface

The no form of the command removes the match clause.

<b>Syntax Description</b>	prefix-list-name	Prefix-list name.
<b>Default</b>	N/A	
<b>Configuration Mode</b>	Config Route Map	
<b>History</b>	3.3.5006	
<b>Role</b>	admin	
<b>Example</b>	switch (config route-map mymap permit 10)# match interface ethernet 1/1	
<b>Related Commands</b>	N/A	
<b>Note</b>	<ul style="list-style-type: none"><li>When a clause contains multiple match commands, the permit or deny filter applies to a route only if its properties are equal to corresponding parameters in each match statement.</li><li>When a route's properties do not equal the statement parameters, the route is evaluated against the next clause in the route map, as determined by sequence number.</li><li>If all clauses fail to permit or deny the route, the route is denied.</li></ul>	

## match ip address

```
match ip address <prefix-list-name>
no match ip address
```

Filters according to IPv4 prefix list.

The no form of the command removes this configuration from the route map clause.

<b>Syntax Description</b>	prefix-list-name	Prefix-list name.
<b>Default</b>	N/A	
<b>Configuration Mode</b>	Config Route Map	
<b>History</b>	3.3.5006	
<b>Role</b>	admin	
<b>Example</b>	switch (config route-map mymap permit 10)# match ip address listSmallRoutes	
<b>Related Commands</b>	N/A	
<b>Note</b>	<ul style="list-style-type: none"><li>When a clause contains multiple match commands, the permit or deny filter applies to a route only if its properties are equal to corresponding parameters in each match statement.</li><li>When a route's properties do not equal the statement parameters, the route is evaluated against the next clause in the route map, as determined by sequence number.</li><li>If all clauses fail to permit or deny the route, the route is denied.</li><li>The prefix-list-name should point to an existing IP prefix-list. If it is not found, no route is considered as a match for this clause.</li></ul>	

## match ip next-hop

```
match ip next-hop <ipv4/ipv6>
no match ip next-hop
```

Configures a route's entry next-hop match.

The no form of the command removes a route-map's entry next-hop match.

<b>Syntax Description</b>	ipv4/ipv6	Next hop IP address: A.B.C.D (e.g. 10.0.13.86).
<b>Default</b>	N/A	
<b>Configuration Mode</b>	Config Route Map	
<b>History</b>	3.3.5200	
	3.6.4070	Added support for IPv4 and IPv6
<b>Role</b>	admin	
<b>Example</b>	<pre>switch (config route-map mymap permit 10)# match ip next-hop 10.10.10.10</pre>	
<b>Related Commands</b>	N/A	
<b>Note</b>	<ul style="list-style-type: none"><li>When a clause contains multiple match commands, the permit or deny filter applies to a route only if its properties are equal to corresponding parameters in each match statement.</li><li>When a route's properties do not equal the statement parameters, the route is evaluated against the next clause in the route map, as determined by sequence number.</li><li>If all clauses fail to permit or deny the route, the route is denied.</li></ul>	

## match local-preference

**match local-preference <value>**  
**no match local-preference**

Configures a route's entry local-preference match.

The no form of the command removes a route-map's entry local-preference match.

Syntax Description	value	Range: 1-2147483647.
<b>Default</b>	N/A	
<b>Configuration Mode</b>	Config Route Map	
<b>History</b>	3.3.5200	
	3.4.0000	Updated value range
<b>Role</b>	admin	
<b>Example</b>	switch (config route-map mymap permit 10)# match local-preference 10	
<b>Related Commands</b>	N/A	
<b>Note</b>	<ul style="list-style-type: none"><li>When a clause contains multiple match commands, the permit or deny filter applies to a route only if its properties are equal to corresponding parameters in each match statement.</li><li>When a route's properties do not equal the statement parameters, the route is evaluated against the next clause in the route map, as determined by sequence number.</li><li>If all clauses fail to permit or deny the route, the route is denied.</li></ul>	

## match metric

**match metric <value>**  
**no match metric**

Configures a route's entry metric match.

The no form of the command removes a route-map's entry metric match.

Syntax Description	value	Range: 1-2147483647.
<b>Default</b>	N/A	
<b>Configuration Mode</b>	Config Route Map	
<b>History</b>	3.3.5200	
	3.4.0000	Updated value range
<b>Role</b>	admin	
<b>Example</b>	switch (config route-map mymap permit 10)# match metric 10	
<b>Related Commands</b>	N/A	
<b>Note</b>	<ul style="list-style-type: none"><li>When a clause contains multiple match commands, the permit or deny filter applies to a route only if its properties are equal to corresponding parameters in each match statement.</li><li>When a route's properties do not equal the statement parameters, the route is evaluated against the next clause in the route map, as determined by sequence number.</li><li>If all clauses fail to permit or deny the route, the route is denied.</li></ul>	

## set as-path prepend

```
set as-path prepend <value1> <value2> ... <valuen>  
no set as-path prepend
```

Modifies as-path on affected routes

The no form of the command removes the set statement from the route map.

<b>Syntax Description</b>	value	BGP AS number that is prepended to as-path. Range: 1-4294967295.
<b>Default</b>	N/A	
<b>Configuration Mode</b>	Config Route Map	
<b>History</b>	3.4.0000	
<b>Role</b>	admin	
<b>Example</b>		switch (config route-map mymap permit 10)# set as-path prepend 5 10
<b>Related Commands</b>	N/A	
<b>Note</b>		

## set as-path tag

```
set as-path tag <value>
no set as-path tag
```

Configures a route's entry AS-path tag parameter.

The no form of the command removes a route-map's entry AS path tag setting.

Syntax Description	value	Range: 1-2147483648.
<b>Default</b>	N/A	
<b>Configuration Mode</b>	Config Route Map	
<b>History</b>	3.3.5200	
<b>Role</b>	admin	
<b>Example</b>	switch (config route-map mymap permit 10)# set as-path tag 1	
<b>Related Commands</b>	N/A	
<b>Note</b>		

## set community

```
set community {<list of communities> | none}
no set community {<list of communities> | none}
```

Sets the community attribute of a distributed route

The no form of the command removes the set statement from the clause.

<b>Syntax Description</b>	list of communities	List of standard communities: <ul style="list-style-type: none"><li>• &lt;aa:nn&gt;</li><li>• &lt;number&gt;</li><li>• internet</li><li>• local-AS</li><li>• no-advertise</li><li>• no-export</li></ul>
<b>Default</b>	N/A	
<b>Configuration Mode</b>	Config Route Map	
<b>History</b>	3.3.5200	
<b>Role</b>	admin	
<b>Example</b>	switch (config route-map mymap permit 10)# set community 1:2 3:4	
<b>Related Commands</b>	N/A	
<b>Note</b>		

## set community additive

```
set community <list-of-communities> additive
no set community <list-of-communities> additive
```

Adds the matching communities

The no form of the command removes the set statement from the clause.

<b>Syntax Description</b>	list-of-communities	List of standard communities: <ul style="list-style-type: none"><li>• &lt;aa:nn&gt;</li><li>• &lt;number&gt;</li><li>• internet</li><li>• local-AS</li><li>• no-advertise</li><li>• no-export</li></ul>
<b>Default</b>	N/A	
<b>Configuration Mode</b>	Config Route Map	
<b>History</b>	3.3.5200	
<b>Role</b>	admin	
<b>Example</b>	switch (config route-map mymap permit 10)# set community none	
<b>Related Commands</b>	N/A	
<b>Note</b>		

## set community none

**set community none**  
**no set community none**

Sets the community attribute of a distributed route to be empty  
The no form of the command removes the set statement from the clause.

<b>Default</b>	N/A
<b>Configuration Mode</b>	Config Route Map
<b>History</b>	3.3.5200
<b>Role</b>	admin
<b>Example</b>	switch (config route-map mymap permit 10)# set community none
<b>Related Commands</b>	N/A
<b>Note</b>	

## set community delete

```
set community <list of communities> delete
no set community <list of communities> delete
```

Deletes matching communities.

The no form of the command removes the set statement from the clause.

<b>Syntax Description</b>	list of communities	List of standard communities: <ul style="list-style-type: none"><li>• &lt;aa:nn&gt;</li><li>• &lt;number&gt;</li><li>• internet</li><li>• local-AS</li><li>• no-advertise</li><li>• no-export</li></ul>
<b>Default</b>	N/A	
<b>Configuration Mode</b>	Config Route Map	
<b>History</b>	3.3.5200	
<b>Role</b>	admin	
<b>Example</b>		<pre>switch-e07c04 [standalone: master] (config) # route-map test_route_map switch-e07c04 [standalone: master] (config route-map test_route_map permit 10) # set community 400:1 delete</pre>
<b>Related Commands</b>	N/A	
<b>Note</b>		

## set community-list

```
set community-list <community-list-name>
no set community <list of communities>
```

Configures a named standard community list.  
The no form of the command removes the set statement from the clause.

<b>Syntax Description</b>	<community-list-name>	Name of community list
<b>Default</b>	N/A	
<b>Configuration Mode</b>	Config Route Map	
<b>History</b>	3.3.5200	
	3.6.3004	Added note
<b>Role</b>	admin	
<b>Example</b>	switch (config route-map mymap permit 10)# set community internet 1:3 additive	
<b>Related Commands</b>	N/A	
<b>Note</b>	A community-list must already exist before a node is configured to use it	

## set community-list additive

```
set community-list <community-list-name> additive
no set community <list of communities> additive
```

Adds to existing communities using the communities found in the community list.  
The no form of the command removes the set statement from the clause.

<b>Syntax Description</b>	<community-list-name>	Name of community list
<b>Default</b>	N/A	
<b>Configuration Mode</b>	Config Route Map	
<b>History</b>	3.3.5200	
<b>Role</b>	admin	
<b>Example</b>	switch (config route-map mymap permit 10)# set community-list mycommunity additive	
<b>Related Commands</b>	N/A	
<b>Note</b>		

## set community-list delete

```
set community-list <community-list-name> delete
no set community-list
```

Deletes the matching community list permit entries from the route community list  
The no form of the command removes the set statement from the clause.

Syntax Description	community-list-name	Name of community list
<b>Default</b>	N/A	
<b>Configuration Mode</b>	Config Route Map	
<b>History</b>	3.3.5200	
<b>Role</b>	admin	
<b>Example</b>	switch (config route-map mymap permit 10)# set community-list mycommunity delete	
<b>Related Commands</b>	N/A	
<b>Note</b>		

## set ip next-hop

```
set ip next-hop <ipv4/ipv6>
no set ip next-hop
```

Configures a route's entry next-hop parameter.

The no form of the command removes a route-map's entry next-hop setting.

<b>Syntax Description</b>	ipv4/ipv6	Route next-hop IP: A.B.C.D (e.g. 10.0.13.86).
<b>Default</b>	N/A	
<b>Configuration Mode</b>	Config Route Map	
<b>History</b>	3.3.5200	
	3.6.4070	Added support for IPv4 and IPv6
<b>Role</b>	admin	
<b>Example</b>	switch (config route-map mymap permit 10)# set ip next-hop 10.10.10.10	
<b>Related Commands</b>	N/A	
<b>Note</b>		

## set local-preference

```
set local-preference <value>
no set local-preference
```

Configures a route's entry local-preference parameter.  
The no form of the command removes a route-map's entry local-pref setting.

Syntax Description	value	Route local-pref: 1-2147483648.
<b>Default</b>	N/A	
<b>Configuration Mode</b>	Config Route Map	
<b>History</b>	3.3.5200	
<b>Role</b>	admin	
<b>Example</b>		switch (config route-map mymap permit 10)# set local-preference 10
<b>Related Commands</b>	N/A	
<b>Note</b>		

## set metric

**set metric <value>**  
**no set metric**

Configures a route's entry metric parameter.  
The no form of the command removes a route-map's entry metric setting.

Syntax Description	value	Route metric: 1-2147483647.
<b>Default</b>	N/A	
<b>Configuration Mode</b>	Config Route Map	
<b>History</b>	3.3.5200	
<b>Role</b>	admin	
<b>Example</b>		switch (config route-map mymap permit 10)# set metric 10
<b>Related Commands</b>		N/A
<b>Note</b>		

## set origin

```
set origin {egp | igp | incomplete}  
no set origin
```

Configures a route's entry origin parameter.

The no form of the command removes a route-map's entry origin setting.

Syntax Description	egp	Set a route's entry origin parameter to external.
	igp	Set a route's entry origin parameter to internal.
	incomplete	Set a route's entry origin parameter to incomplete.
Default	N/A	
Configuration Mode	Config Route Map	
History	3.3.5200	
Role	admin	
Example	switch (config route-map mymap permit 10)# set origin egp	
Related Commands	N/A	
Note		

## set tag

```
set tag <value>
no set tag
```

Configures a route's entry tag parameter.  
The no form of the command removes a route-map's entry tag setting.

Syntax Description	value	Range: 1-2147483647.
<b>Default</b>	N/A	
<b>Configuration Mode</b>	Config Route Map	
<b>History</b>	3.3.5200	
	3.4.0000	Updated parameter range
<b>Role</b>	admin	
<b>Example</b>	switch (config route-map mymap permit 10)# set tag 10	
<b>Related Commands</b>	N/A	
<b>Note</b>		

## set weight

**set weight <number>**  
**no set weight**

Configures modifications to redistributed routes.

The no form of the command removes this configuration from the route map clause.

Syntax Description	number	Value of the weight to set. Range: 1-65535.
<b>Default</b>	N/A	
<b>Configuration Mode</b>	Config Route Map	
<b>History</b>	3.3.5006	
	3.4.0000	Updated parameter range
<b>Role</b>	admin	
<b>Example</b>	switch (config route-map mymap permit 10)# set weight 7	
<b>Related Commands</b>	route-map <map-name> [deny   permit] [sequence-number]	
<b>Note</b>		

## show route-map

**show route-map [<name>]**

Displays route map configuration.

<b>Syntax Description</b>	N/A
<b>Default</b>	N/A
<b>Configuration Mode</b>	Any Command Mode
<b>History</b>	3.3.5006
<b>Role</b>	admin
<b>Example</b>	<pre>switch (config)# show route-map mymap route-map mymap, permit, sequence 1200   Set clauses:     continue 1800 switch (config)#+</pre>
<b>Related Commands</b>	N/A
<b>Note</b>	

## 6.6.2 IP Prefix-List

Prefix-list is a list of entries, each of which can match one or more IP prefixes. A prefix-list is usually used to match a specific IP prefix, mostly in relation to IP route destinations.

The prefix is considered to match the list if one of the entries match the prefix; the entry itself can be marked as a “permit” entry or a “deny” entry, which can be used by the matching code to decide if the route is to be accepted or not.

The prefix is matched to the prefix-list entries in the order of the sequence number of the entries in the list.

### 6.6.2.1 Commands

#### ip prefix-list

```
ipv6 prefix-list <list-name> [seq <number>] {permit | deny} <ipv6> <length> [eq
<length> | le <length> | ge <length> [le <length>]]]
no ipv6 prefix-list <list-name> [seq <number>]
```

The command creates or updates IPv6 prefix-list.

The no form of the command deletes the prefix-list or a prefix-list entry

<b>Syntax Description</b>	list-name	String
	seq <number>	Sequence number assigned to entry. Range: 0-65535.
	permit	Permits access for a matching condition.
	deny	Denies access for a matching condition.
	ipv6	IPv6 address
	length	Prefix length
	eq   ge   le <mask>	<ul style="list-style-type: none"> <li>• eq: Equal to a specified prefix length</li> <li>• ge: Greater than or equal to a specified prefix length</li> <li>• le: Less than or equal to a specified prefix length</li> </ul>
<b>Default</b>	Sequence value = 10	
<b>Configuration Mode</b>	Config	
<b>History</b>	3.3.5200	
	3.6.4070	Added support for IPv6
<b>Role</b>	admin	
<b>Example</b>	<pre>switch (config)# ipv6 prefix-list a-list permit 2001::0 /64 eq 32 switch (config)#{/pre} </pre>	
<b>Related Commands</b>	N/A	
<b>Note</b>		

## show ipv6 prefix-list

**show ipv6 prefix-list [<name>]**

Displays IPv6 prefix-lists.

<b>Syntax Description</b>	name	Displays a specific prefix-list.
<b>Default</b>	N/A	
<b>Configuration Mode</b>	Any Command Mode	
<b>History</b>	3.3.5200	
	3.6.4070	Added support for IPv6
<b>Role</b>	admin	
<b>Example</b>	<pre>switch (config)# show ipv6 prefix-list prefix-list: a-list count: 1, range entries: 1, sequences: 10 - 10 seq 10 permit 2001::0 /64 ge eq 32 (hit count: 0, refcount: 0)  switch (config)#+</pre>	
<b>Related Commands</b>	N/A	
<b>Note</b>		

## 6.7 Multicast (IGMP and PIM)

Protocol independent multicast (PIM) is a collection of protocols that deal with efficient delivery of IP multicast (MC) data. Those protocols are published in the series of RFCs and define different ways and aspects of multicast data distribution. PIM protocol family includes PIM dense mode (PIM-DM), Bootstrap router (BSR) protocol, and PIM sparse mode (PIM-SM) and Bidirectional PIM (PIM-BIDIR)—both of which are not supported on MLNX-OS®.

PIM builds and maintains multicast routing tables based on the unicast routing information provided by unicast routing tables that can be maintained statically or dynamically by IP routing protocols like OSPF and BGP.

### 6.7.1 Basic PIM-SM

PIM relies on the underlying topology gathering protocols that collect unicast routing information and build multicast routing information base (MRIB). The primary role of MRIB is to determine the next hop for PIM messages. MC data flows along with the reverse path of the PIM control.

MC tree construction contains three phases:

1. Construction of a shared distribution tree. This tree is built around a special designated router (DR) called the rendezvous point (RP).
2. Establishing a native forwarding path from MC sources to the RP
3. Building an optimized MC distribution tree from each MC source to all MC targets bypassing the RP

The first stage of the multicast tree establishment starts when the MC receiver expresses desire to start receiving MC data. It can happen as a result of using one of the L2 protocols like MLD or IGMP, or by static configuration. When such request is received by the last hop router (a designated router) this router starts to build a distribution path from the RP. It starts to send periodic “Join” messages to the nearest PIM neighbor router towards the RP. The next router continues to do the same. Eventually the process converges when Join messages reach RP or a router that has already created that distribution tree. Usually that tree is called a shared tree because it is created for any source for specific MC group G and is noted as (\*,G).

At that stage, MC senders can start sending MC data. The DR next to the MC source extracts the packets from the data flow and tunnels them to the RP. The RP decapsulates the packets and distributes them to all MC receivers along with the share tree.

On the second stage the RP switches from tunneling of multicast packets from MC sources to forwarding native traffic. When the RP identifies that a new MC source started to send packets, it initiates an establishment of a native forwarding path from the DR of that source to itself. For this purpose it starts to send Join messages towards MC source to nearest neighbor to that source according the MRIB. This is a source specific Join and is noted as (S,G). When data path is established up to the DR, the DR switches from tunneling MC packets to their native forwarding, so the RP does not need to decapsulate MC packets anymore, but still continue to distribute the packets along with shared tree.

On the third phase multicast receivers will try to switch from shared tree to source specific tree by creating a direct distribution path from a multicast source. When last hop router of the multicast receiver identifies multicast traffic coming from any multicast source it will start to send

Join messages towards the source with purpose to create a direct source specific path to that source. Once such path will be established and Designated router that is attached to the source L2 network will start to distribute the multicast traffic directly bypassing shared tree, the last hop router will detach its receivers from shared tree for that data and will switch to the shortest path tree distribution.

### 6.7.2 Source-Specific Multicast (SSM)

Source-Specific Multicast (SSM) is a method of delivering multicast packets in which the only packets that are delivered to a receiver are those originating from a specific source address requested by the receiver. By so limiting the source, SSM reduces demands on the network and improves security.

SSM requires that the receiver specify the source address and explicitly excludes the use of the (\*,G) join for all multicast groups in RFC 3376, which is possible only in IPv4's IGMPv3 and IPv6's MLDv2.

Source-specific multicast is best understood in contrast to any-source multicast (ASM). In the ASM service model a receiver expresses interest in traffic to a multicast address. The multicast network must discover all multicast sources sending to that address, and route data from all sources to all interested receivers.

This behavior is particularly well suited for groupware applications where all participants in the group want to be aware of all other participants, and the list of participants is not known in advance.

The source discovery burden on the network can become significant when the number of sources is large.

In the SSM service model, in addition to the receiver expressing interest in traffic to a multicast address, the receiver expresses interest in receiving traffic from only one specific source sending to that multicast address. This relieves the network of discovering many multicast sources and reduces the amount of multicast routing information that the network must maintain.

SSM requires support in last-hop routers and in the receiver's operating system. SSM support is not required in other network components, including routers and even the sending host. Interest in multicast traffic from a specific source is conveyed from hosts to routers using IGMPv3 as specified in RFC 4607.

SSM destination addresses must be in the ranges 232.0.0.0/8 for IPv4 or FF3x::/96 for IPv6.

Source-specific multicast delivery semantics are provided for a datagram sent to an SSM address. That is, a datagram with source IP address S and SSM destination address G is delivered to each upper-layer "socket" that has specifically requested the reception of datagrams sent to address G by source S, and only to those sockets.

### 6.7.3 Bootstrap Router

For correct operation each PIM router requires a capability to map a multicast group that it needs to serve to a Rendezvous point for that group. This mapping can be done manually or the mapping can be distributed dynamically in the network. BSR protocol serves for this purpose.

This protocol introduces new role in the multicast network – Bootstrap router. That router is responsible to flood multicast group to RP mapping through the multicast routing domain. Boot-

strap router is elected dynamically among bootstrap router candidates (C-BSR) and once elected will collect from Rendezvous point candidate (C-RP) mapping information and distribute it in the domain.

Bootstrap activity contains 4 steps. First each C-BSR configured in the network originates floods into the network bootstrap messages that express the router desire to become BSR and also its BSR priority. Any C-BSR that receives that information and has lower priority will suspend itself, so eventually only one router will send BSR messages and become BSR.

When BSR is elected all RP candidates start to advertise to BSR a list of groups that this RP can serve. On the next step, after BSR learns the group mapping proposals, it forms a final group to RP mapping in the domain and starts to distribute it among PIM routers in the multicast routing domain. When PIM router receives BSR message with the group to RP mapping, it installs that mapping in the router local cache and uses that information to create multicast distribution trees.

## 6.7.4 Configuring Multicast

### Precondition steps:

- Step 1.** Enable IP routing functionality. Run:

```
switch (config)# ip routing
```

- Step 2.** Enable the desired VLAN. Run:

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

- Step 3.** Add this VLAN to the desired interface. Run:

```
switch (config)# interface ethernet 1/1
switch (config ethernet 1/1)#switchport access vlan 10
```

- Step 4.** Create a VLAN interface. Run:

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

- Step 5.** Apply IP address to the VLAN interface. Run:

```
switch (config interface vlan 10)# ip address 10.10.10.10 /24
```

- Step 6.** Enable the interface. Run:

```
switch (config interface vlan 10)# no shutdown
```

### 6.7.4.1 Configuring IGMP

IGMP is enabled when IP multicast is enabled and static multicast or PIM is enabled on the interface.

### 6.7.4.2 Verifying IGMP

- Step 1.** Display a brief IGMP interface status. Run:

```
switch (config)# show ip igmp interface brief
IGMP Interfaces for VRF "default", Count: 1
Interface          IP Address      IGMP Querier    Membership   Version
VLAN10            10.10.10.1    10.10.10.1      5           v2
```

- Step 2.** Display detailed IGMP interface status. Run:

```
switch (config)#show ip igmp interface vlan 10
IGMP Interfaces for VRF "default"

VLAN10
  Interface status: protocol-up/admin-up/link-up
  IP address: 10.10.10.1, IP Subnet: 10.10.10.0/24
  Active Querier: 10.10.10.1
  Membership count: 5
  Route-queue depth: 0
  IGMP Version: 2
  IGMP query interval: 125 secs, configured value: 125 secs
  IGMP max response time: 10 secs, configured value: 10 secs
  IGMP startup query interval: 125 secs, configured value: 125 secs
  IGMP startup query count: 2
  IGMP group timeout: 260 secs, configured value: 260 secs
  IGMP querier timeout: 260 secs configured value: 260 secs
  IGMP last member mrt: 25 secs configured value: 25
  IGMP robustness variable: 2
  IGMP interface statistics:
    General (sent/received):
    v1/v2-reports: 0/10
    v2-queries: 271/0,v2-leaves: 0/0
    v3-queries: 0/0,
    v3-reports: 0/0
switch (config)#

```

- Step 3.** Display the list of IGMP groups and their status. Run:

```
switch (config)#show ip igmp groups
IGMP Connected Group Membership for VRF "default", - 2 total entries
Type: S - Static, D - Dynamic, L - Local, T - SSM Translated
Group Address Type      Interface Uptime           Expires        Last
Reporter
  226.0.1.0    D      vlan10    [0d 00:00:07.46]  [0d 00:04:05.08] 10.10.10.2
  226.0.1.1    D      vlan10    [0d 00:00:07.47]  [0d 00:04:05.08]
10.10.10.2
switch (config)#

```

#### 6.7.4.3 Configuring PIM

Prerequisites:

- Step 1.** If not enabled, enable IP routing. Run:

```
switch (config)# ip routing
```

- Step 2.** Globally enable multicast routing. Run:

```
switch (config)# ip multicast-routing
```

➤ **To configure PIM:**

- Step 1.** Enable PIM. Run:

```
switch (config)# protocol pim
```

- Step 2.** Globally enable Bidirectional PIM (BIDIR mode). Run:

```
switch (config)# no ip pim bidir shutdown
```

## 6.7.5 Commands

### 6.7.5.1 PIM

#### protocol pim

**protocol pim**  
**no protocol pim**

Enables protocol independent multicast (PIM).

The no form of the command hides all PIM commands and deletes all PIM configurations.

<b>Syntax Description</b>	N/A
<b>Default</b>	Disabled
<b>Configuration Mode</b>	Config
<b>History</b>	3.3.5006
<b>Role</b>	admin
<b>Example</b>	switch (config) # protocol pim
<b>Related Commands</b>	N/A
<b>Note</b>	

## ip pim bidir shutdown

```
ip pim bidir shutdown
no ip pim bidir shutdown
```

Disables PIM bidir.

The no form of the command enables PIM bidir.

<b>Syntax Description</b>	N/A
<b>Default</b>	Disabled
<b>Configuration Mode</b>	Config
<b>History</b>	3.3.5006
<b>Role</b>	admin
<b>Example</b>	switch (config) # no ip pim bidir shutdown
<b>Related Commands</b>	N/A
<b>Note</b>	

## ip pim rp-address

```
ip pim rp-address <rp-address> [group-list <ip-address> <prefix>] [override]
bidir
no ip pim rp-address <rp-address> [group-list <ip-address> <prefix>]
```

Configures a static IP address of a rendezvous point for a multicast group range or adds new multicast range to existing RP.

The no form of the command removes the rendezvous point for a multicast group range or removes all configuration of the RP.

<b>Syntax Description</b>	rp-address	The static IP address of rendezvous point.
	ip-address	IP address of the group-range (coupled with the prefix parameter).
	prefix	Network prefix (in the format of /24, or 255.255.255.0 for example) of group range.
	override	Specifies that this configuration overrides dynamic configuration learned by BSR.
	bidir	Specifies that the group range uses a bidirectional PIM.
<b>Default</b>	N/A	
<b>Configuration Mode</b>	Config	
<b>History</b>	3.3.5006	
<b>Role</b>	admin	
<b>Example</b>	switch (config) # ip pim rp-address 10.10.10.10 bidir	
<b>Related Commands</b>	N/A	
<b>Note</b>		

## ip pim bsr-candidate

```
ip pim bsr-candidate {vlan <vlan-id> | loopback <number> | ethernet <port>}  
[hash-len <hash-length>] [priority <priority>] [interval <interval>]  
no ip pim bsr-candidate {vlan <vlan-id> | loopback <number> | ethernet <port>}  
[hash-len <hash-length>] [priority <priority>] [interval <interval>]
```

Configures the switch as a candidate BSR router (C-BSR).

The no form of the command removes BSR-candidate configuration or restores default parameters values.

<b>Syntax Description</b>	vlan <vlan-id>	The VLAN ID. Range is 1-4094.
	loopback <number>	Loopback interface number.
	ethernet <port>	Ethernet interface.
	hash-len	Specifies the hash mask length used in BSR messages. Range: 0-32.
	priority	BSR priority rating. Larger numbers denote higher priority. Range: 0-255.
	interval	Period between the transmission of BSMs (seconds). Range:10-536870906.
<b>Default</b>	The interface is not BSR candidate by default. priority: 64 interval: 60 hash-len: 30	
<b>Configuration Mode</b>	Config Config Interface Ethernet configured as a router port interface Config Interface Loopback Config Interface Port Channel configured as a router port interface Config Interface VLAN	
<b>History</b>	3.3.5006	
<b>Role</b>	admin	
<b>Example</b>	switch (config) # ip pim bsr-candidate vlan 10 priority 100	

**Related Commands**

ip pim sparse-mode

**Note**

- IP PIM sparse-mode must be enabled on the interface.
- A BSR is a PIM router within the PIM domain through which dynamic RP selection is implemented. The BSR selects RPs from a list of candidate RPs and exchanges bootstrap messages (BSM) with all routers in the domain. The BSR is elected from one of the C-BSRs through an exchange of BSMs. A subset of PIM routers within the domain are configured as candidate Bootstrap routers (C-BSRs). Through the exchange of Bootstrap messages (BSMs), the C-BSRs elect the BSR, which then uses BSMs to inform all domain routers of its status.
- Command parameters specify the switch's BSR address, the interval between BSM transmissions, hash length used for RP calculations and the priority assigned to the switch when electing a BSR.
- Entering an ip pim bsr-candidate command replaces any previously configured bsr-candidate command. If the new command does not specify a priority or interval, the previously configured values persist in running-config.

## ip pim bsr-holdtime

```
ip pim bsr-holdtime <period>
no ip pim bsr-holdtime
```

Configures the timeout period an elected BSR remains valid after receiving a BSM.  
The no form of the command resets the parameters to their default.

<b>Syntax Description</b>	period	In seconds. Range: 12-1073741823 (1.073 billion).
<b>Default</b>	period = 2*(BSR candidate interval) + 10	
<b>Configuration Mode</b>	Config	
<b>History</b>	3.3.5006	
<b>Role</b>	admin	
<b>Example</b>	switch (config) # ip pim bsr-holdtime 30	
<b>Related Commands</b>		
<b>Note</b>		

## ip pim rp-candidate

```
ip pim rp-candidate {vlan <vlan-id> | loopback <number> | ethernet <slot/
port>} group-list <ip-address> <prefix> [bidir] [priority <priority>] [interval
<interval>]
no ip pim rp-candidate {vlan <vlan-id> | loopback <number> | ethernet <slot/
port>} group-list <ip-address> <prefix> [bidir] [priority <priority>] [interval
<interval>]
```

Configures the switch as a candidate rendezvous point (C-RP).  
The no form of the command removes the ip pim rp-candidate from running-config command for the specified multicast group.

<b>Syntax Description</b>	ethernet <slot/port>	Ethernet interface.
	port-channel <number>	LAG interface.
	vlan <vlan-id>	VLAN ID. Range: 1-4094.
	loopback <number>	Loopback interface number.
	ip-address	The group IP address.
	prefix	Network prefix (for example /24, or 255.255.255.0).
	priority	RP priority rating. Range: 0-255, where smaller numbers mean higher priority.
	interval	RP-advertisements message transmission interval. Range: 0-16383.
<b>Default</b>	The RP priority is 192. The BSR message interval is 60 seconds.	
<b>Configuration Mode</b>	Config Config Interface Ethernet configured as a router port interface Config Interface Loopback Config Interface Port Channel configured as a router port interface Config Interface VLAN	
<b>History</b>	3.3.5006	
<b>Role</b>	admin	
<b>Example</b>	<pre>switch (config) # ip pim rp-candidate vlan 19 group-list 225.6.5.0 /25 priority 20 interval 30 bidir</pre>	

<b>Related Commands</b>	N/A
<b>Note</b>	<ul style="list-style-type: none"><li>The BSR selects a multicast group's dynamic RP set from the list of C-RPs in the PIM domain. The command specifies the interface (used to derive the RP address), C-RP advertisement interval, and priority rating. The BSR selects the RP set by comparing C-RP priority ratings. The C-RP advertisement interval specifies the period between successive C-RP advertisement message transmissions to the BSR.</li><li>Running-config supports multiple multicast groups through multiple ip pim rp-candidate statements:</li><li>All commands must specify the same interface. Issuing a command with an interface that differs from existing commands removes all existing commands from running-config.</li><li>Running-config stores the interval and priority setting in a separate statement that applies to all rp-candidate statements. When a command specifies an interval that differs from the previously configured value, the new value replaces the old value and applies to all configured rp-candidate statements. The default interval value is 60 seconds.</li><li>When the no commands do not specify a multicast group, all rp-candidate statements are removed from running-config. The no ip pim rp-candidate interval commands restore the interval setting to the default value of 60 seconds.</li><li>When setting a priority, all previous rp-candidates within all interfaces and groups are configured to this priority.</li></ul>

## ip pim sparse-mode

**ip pim sparse-mode**  
**no ip pim sparse-mode**

Sets PIM sparse mode on this interface.

The no form of the command disables the sparse-mode on the interface and deletes all interfaces configuration.

<b>Syntax Description</b>	N/A
<b>Default</b>	Disabled
<b>Configuration Mode</b>	Config Interface VLAN Config Interface Ethernet configured as a router port interface Config Interface Port Channel configured as a router port interface
<b>History</b>	3.3.5006
<b>Role</b>	admin
<b>Example</b>	switch (config interface vlan 10) # ip pim sparse-mode
<b>Related Commands</b>	N/A
<b>Note</b>	

## ip pim dr-priority

**ip pim dr-priority <priority>**  
**no ip pim dr-priority**

Configures the designated router (DR) priority of PIM Hello messages.  
The no form of the command resets this parameter to its default.

<b>Syntax Description</b>	priority	The designated router priority of the PIM Hello messages. Range is 1-4294967295.
<b>Default</b>	1	
<b>Configuration Mode</b>	Config Interface VLAN Config Interface Ethernet configured as a router port interface Config Interface Port Channel configured as a router port interface	
<b>History</b>	3.3.5006	
<b>Role</b>	admin	
<b>Example</b>	switch (config interface vlan 10) # ip pim dr-priority 5	
<b>Related Commands</b>	ip pim sparse-mode	
<b>Note</b>	The command “ip pim sparse-mode” must be run prior to using this command.	

## ip pim hello-interval

```
ip pim hello-interval <interval>
no ip pim hello-interval
```

Configures PIM Hello interval in milliseconds.  
The no form of the command resets this parameter to its default.

<b>Syntax Description</b>	interval	PIM Hello interval in seconds . Range:1-18000.
<b>Default</b>	30 seconds	
<b>Configuration Mode</b>	Config Interface VLAN Config Interface Ethernet configured as a router port interface Config Interface Port Channel configured as a router port interface	
<b>History</b>	3.3.5006	
	3.6.4006	Updated range
<b>Role</b>	admin	
<b>Example</b>	switch (config interface vlan 10) # ip pim hello-interval 70000	
<b>Related Commands</b>	ip pim sparse-mode	
<b>Note</b>	The command “ip pim sparse-mode” must be run prior to using this command.	

## ip pim join-prune-interval

```
ip pim join-prune-interval <period>
no ip pim join-prune-interval
```

Configures the period between Join/Prune messages that the configuration mode interface originates and sends to the upstream RPF neighbor.  
The no form of the command resets this parameter to its default.

<b>Syntax Description</b>	period	Range: 1-18000 seconds.
<b>Default</b>	60 seconds	
<b>Configuration Mode</b>	Config Interface VLAN Config Interface Ethernet configured as a router port interface Config Interface Port Channel configured as a router port interface	
<b>History</b>	3.3.5200	
	3.6.4006	Updated range
<b>Role</b>	admin	
<b>Example</b>	switch (config interface vlan 10) # ip pim join-prune-interval 60	
<b>Related Commands</b>		
<b>Note</b>		

## ip pim ssm range

```
ip pim ssm range {standard | group-list {<group-range>|<address> <prefix>}}
no ip pim ssm range {standard | group-list {<group-range>|<address> <prefix>}}
```

Enables one or more ranges for SSM operation.

The no form of the command disables range for SSM operation.

<b>Syntax Description</b>	standard	set the SSM operation to standard SSM range 232.0.0.0/8
	<group-range>	user-defined multicast range for SSM operation. Example 233.0.0.0/8
	<ip-address>	group range ip-address. Example: 233.0.0.0
	<prefix>	group range prefix. Example /8 or 255.0.0.0
<b>Default</b>	Void	
<b>Configuration Mode</b>	Config	
<b>History</b>	3.6.4006	
<b>Role</b>	admin	
<b>Example</b>	switch (config) # ip pim ssm range group-list 234.0.0.0/8	
<b>Related Commands</b>		
<b>Note</b>	Standard and group-list configurations are mutually exclusive: It is necessary to delete standard SSM configuration in order to add group-list and it is necessary to delete all existing group-list configuration in order to configure standard SSM configuration.	

## ip pim border

**ip pim border**  
**no ip pim border**

Configures an interface on an IPv4 PIM border.

The no form of the command removes the interface from being a PIM border.

<b>Syntax Description</b>	N/A
<b>Default</b>	Disabled
<b>Configuration Mode</b>	Config Interface VLAN Config Interface Ethernet configured as a router port interface Config Interface Port Channel configured as a router port interface
<b>History</b>	3.3.5006
<b>Role</b>	admin
<b>Example</b>	<pre>switch (config interface vlan 10) # ip pim border</pre>
<b>Related Commands</b>	
<b>Note</b>	PIM border blocks PIM control traffic, but sends and receives all multicast traffic.

## ip pim bsr-border

**ip pim bsr-border**  
**no ip pim bsr-border**

Prevents the switch from sending bootstrap router messages (BSMs) over the configuration mode interface.

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

<b>Syntax Description</b>	N/A
<b>Default</b>	no pim bsr-border
<b>Configuration Mode</b>	Config Interface VLAN Config Interface Ethernet configured as a router port interface Config Interface Port Channel configured as a router port interface
<b>History</b>	3.3.5200
<b>Role</b>	admin
<b>Example</b>	<pre>switch (config interface vlan 10) # ip pim bsr-border</pre>
<b>Related Commands</b>	
<b>Note</b>	

## ip pim multipath rp

```
ip pim multipath rp
no ip pim multipath rp
```

Enables PIM load-sharing for Rendezvous Points (RPs).  
The no form of the command disables PIM load-sharing for RPs.

<b>Syntax Description</b>	N/A
<b>Default</b>	Disabled
<b>Configuration Mode</b>	Config
<b>History</b>	3.4.2008
<b>Role</b>	admin
<b>Example</b>	switch (config) # ip pim multipath rp
<b>Related Commands</b>	N/A
<b>Note</b>	

## show ip pim protocol

### show ip pim protocol

Displays PIM protocol information (counters).

<b>Syntax Description</b>	N/A
<b>Default</b>	N/A
<b>Configuration Mode</b>	Any Command Mode
<b>History</b>	3.3.5200
<b>Role</b>	admin
<b>Example</b>	<pre>switch (config) # show ip pim protocol PIM Control Counters       Received    Sent    Invalid Assert          0       0       0 Bootstrap Router 0       0       0 CRP Advertisement 0       0       0 Graft           0       0       0 Grapt Ack       0       0       0 Hello            0       0       0 J/P              0       0       0 Register         0       0       0 Register Stop    0       0       0 State Refresh    0       0       0 switch (config) #</pre>
<b>Related Commands</b>	
<b>Note</b>	

## show ip pim bsr

### show ip pim bsr

Displays PIM BSR information.

<b>Syntax Description</b>	N/A
<b>Default</b>	N/A
<b>Configuration Mode</b>	Any Command Mode
<b>History</b>	3.3.5006
<b>Role</b>	admin
<b>Example</b>	<pre>arc-switch14 [standalone: master] (config) # show ip pim bsr PIMv2 Bootstrap information     BSR address: 4.4.4.14     Uptime:      00:00:30, BSR Priority: 0, Hash mask length: 30     Expires:     00:00:57 This system is a candidate BSR     Candidate BSR address: 4.4.4.14, priority: 0, hash mask length: 30                                 interval: 60, holdtime: 130</pre>
<b>Related Commands</b>	
<b>Note</b>	

## show ip pim neighbor

**show ip pim neighbor [vlan <vlan-id> | <other interfaces> | <ip-addr>]**

Displays information about IPv4 PIM neighbors.

<b>Syntax Description</b>	vlan <vlan-id>	Filters the output per specific VLAN ID.
	neighbor-addr	Filters the output per specific neighbor IP address.
<b>Default</b>	N/A	
<b>Configuration Mode</b>	Any Command Mode	
<b>History</b>	3.3.5006	
<b>Role</b>	admin	
<b>Example</b>	<pre>switch (config) # show ip pim neighbor PIM Neighbor Status for VRF "default" Neighbor           Interface          Uptime   Expires  Ver    DR Prio Mode 5.5.5.1            VLAN5             10:36:45 00:01:43  1 9.9.9.1            VLAN9             10:36:42 00:01:43  1 switch (config) #</pre>	
<b>Related Commands</b>		
<b>Note</b>		

## show ip pim rp

**show ip pim rp <rp-address>**

Displays information about the rendezvous points (RPs) for PIM.

<b>Syntax Description</b>	rp-address	A rendezvous points address.
<b>Default</b>	N/A	
<b>Configuration Mode</b>	Any Command Mode	
<b>History</b>	3.3.5006	
<b>Role</b>	admin	
<b>Example</b>	<pre>switch(config)# show ip pim rp PIM RP Status Information for VRF "default" BSR: 10.10.10.10, expires: 00:01:16,       priority: 255, hash-length: 0 RP: 11.11.11.11, expires: 00:01:36       priority: 0, RP-source: 10.10.10.10, group ranges:       225.10.0.0/24 RP: 8.8.8.2, expires: 00:01:36       priority: 0, RP-source: 10.10.10.10, group ranges:       225.12.0.0/24 switch(config)#</pre>	
<b>Related Commands</b>		
<b>Note</b>		

## show ip pim rp-hash

**show ip pim rp-hash <group>**

Displays the hashed value of the group (RP address according the group address).

<b>Syntax Description</b>	group	Filters the output per a specific IP Multicast group address.
<b>Default</b>	N/A	
<b>Configuration Mode</b>	Any Command Mode	
<b>History</b>	3.3.5006	
<b>Role</b>	admin	
<b>Example</b>	<pre>switch (config) # show ip pim rp-hash 225.7.6.2 RP 20.20.20.49, v2 Info Source: 20.20.20.49, via bootstrap, priority 60, holdtime 57 Expires: 00:00:53 PIMv2 Hash Value (mask 255.255.255.252) switch (config)#</pre>	
<b>Related Commands</b>		
<b>Note</b>		

## show ip pim rp-candidate

### show ip pim rp-candidate

Displays information about RP candidate status.

**Syntax Description** N/A

**Default** N/A

**Configuration Mode** Any Command Mode

**History** 3.3.5006

**Role** admin

**Example**

```
switch (config)# show ip pim rp-candidate

Next Candidate-RP-Advertisement in 00:11:22/00:60:00
RP: 10.10.10.10
group prefixes priority
224.0.0.0/4    190
225.0.0.0/4    191
switch (config)#

```

**Related Commands**

**Note**

## show ip pim interface

**show ip pim interface {[vlan <vlan id> | ethernet <port>] [df] | brief}**

Displays information about the enabled interfaces for PIM.

<b>Syntax Description</b>	vlan <vlan-id>	Filters the output for specific interface.
	ethernet <port>	Ethernet interface.
	df	Displays information about elected designated forwarders.
	brief	Displays a summary of information for all interfaces.
<b>Default</b>	N/A	
<b>Configuration Mode</b>	Any Command Mode	
<b>History</b>	3.3.5006	
<b>Role</b>	admin	
<b>Example</b>	<pre># arc-switch55 [standalone: master] (config) # show ip pim interface vlan 2919 Interface Vlan2919 address is 70.28.23.80 PIM: enabled PIM version: 2, mode: sparse PIM DR: 70.28.23.80 (this system) PIM DR Priority: 1 PIM configured DR priority: PIM neighbor count: 1 PIM neighbor holdtime: 105 secs PIM Hello Interval: 30 seconds, next hello sent in: 00:00:28 PIM Hello Generation ID: 61345 PIM Join-Prune Interval: 60 seconds PIM domain border: no PIM Interface Statistics:     General (sent/received):         Hellos: 36/37, JPs: 0/0, Asserts: 0/0         Grafts: 0/0, Graft-Acks: 0/0         DF-Offers: 0/0, DF-Winners: 0/0, DF-Backoffs: 0/0, DF- Passes: 0/0     Errors:         Checksum errors: 0, Invalid packet types/DF subtypes: 0/0         Authentication failed: 0         Packets from non-neighbors: 1         JPs received on RPF-interface: 0         (*,G) Joins received with no/wrong RP: 0/0         (*,G)/(S,G) JPs received for SSM/Bidir groups: 0/0</pre>	

### Related Commands

#### Note

## show ip pim upstream joins

### show ip pim upstream joins

Displays information about any PIM joins/prunes which are currently being sent to upstream PIM routers

<b>Syntax Description</b>	N/A
<b>Default</b>	N/A
<b>Configuration Mode</b>	Any Command Mode
<b>History</b>	3.3.5006
<b>Role</b>	admin
<b>Example</b>	<pre>switch (config) # show ip pim upstream joins Neighbor address: 159.135.45.26 via interface: 159.135.45.34 next message in 43 seconds       Group: 224.0.10.0       Joins:             22.74.49.25       Prunes:             No prunes included switch (config) #</pre>
<b>Related Commands</b>	
<b>Note</b>	Should contain the following information: neighbor address, interface address, group range, Joins, Prunes.

### 6.7.5.2 Multicast

#### ip multicast-routing

```
ip multicast-routing
no ip multicast-routing
```

Allows the switch to forward multicast packets.  
The no form of the command disables multicast routing.

<b>Syntax Description</b>	N/A
<b>Default</b>	Disabled
<b>Configuration Mode</b>	Config
<b>History</b>	3.3.5006
<b>Role</b>	admin
<b>Example</b>	switch (config)# ip multicast-routing
<b>Related Commands</b>	N/A
<b>Note</b>	

## ip mroute

```
ip mroute {<ip-addr> <ip-mask> <next-hop>} [pref]  
no ip mroute {<ip-addr> <ip-mask>}
```

Configure multicast reverse path forwarding (RPF) static routes.  
The no form of the command deletes the static multicast route.

Syntax Description	ip-addr	Unicast IP address.
	ip-mask	Network mask in a dotted format (e.g. 255.255.255.0) or /24 format.
	next-hop	Next hop IP address.
	preference	Route preference. Range: 1-255.
Default	Preference is 1	
Configuration Mode	Config	
History	3.3.5006	
Role	admin	
Example	arc-switch14 [standalone: master] (config) # ip mroute 16.16.0.0 /16 3.3.3.1	
Related Commands	N/A	
Note		

## ip multicast ttl-threshold

```
ip multicast ttl-threshold <ttl-value>
no ip multicast ttl-threshold
```

Configures the time-to-live (TTL) threshold of packets being forwarded out of an interface.

The no form of the command removes RPF static routes.

<b>Syntax Description</b>	ttl-value	Range: 0-225.
<b>Default</b>	0 – all packets are forwarded	
<b>Configuration Mode</b>	Config Interface VLAN Config Interface Ethernet configured as a router port interface Config Interface Port Channel configured as a router port interface	
<b>History</b>	3.3.5006	
<b>Role</b>	admin	
<b>Example</b>	switch (config interface vlan 10)# ip multicast ttl-threshold 10	
<b>Related Commands</b>	N/A	
<b>Note</b>		

## show ip mroute

**show ip mroute [summary | <group> [<prefix> [<source>]]]**

Displays information about IPv4 multicast routes.

<b>Syntax Description</b>	source group prefix summary	Source IP address. IP address of multicast group. Network prefix of multicast group (in the format of /24, or 255.255.255.0 for example). Displays a summary of the multicast routes.
<b>Default</b>	N/A	
<b>Configuration Mode</b>	Any Command Mode	
<b>History</b>	3.2.1000 3.5.1000	Added new F flag and updated Example
<b>Role</b>	admin	
<b>Example</b>	<pre>switch (config) # show ip mroute IP Multicast Routing Table Flags: B - Bidir Group, L - Local, P - Pruned, R - RP-bit set, T - SPT-bit set       J - Join SPT, F - Failed to install in H/W Timers: Uptime/Expires Interface state: Interface, State/Mode  (*, 234.10.0.0/16), 00D 01:06:04, RP 10.10.10.10, flags: BR Bidir-Upstream: Eth1/10 Outgoing interface list:     Eth1/10, Forwarding/Sparse, 00D 01:06:04/00D 00:00:00  F(*, 234.8.0.0/16), 00D 01:06:03, RP 10.10.10.10, flags: BR Bidir-Upstream: Eth1/10 Outgoing interface list:     Eth1/10, Forwarding/Sparse, 00D 01:06:04/00D 00:00:00</pre>	
<b>Related Commands</b>	N/A	
<b>Note</b>		

### 6.7.5.3 IGMP

#### ip igmp last-member-query-count

```
ip igmp last-member-query-count <count>
no ip igmp last-member-query-count
```

Configures the number of query messages the switch sends in response to a group-specific or group-source-specific leave message.

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

<b>Syntax Description</b>	Count	Range:1-7.
<b>Default</b>	2	
<b>Configuration Mode</b>	Config Interface VLAN Config Interface Ethernet configured as a router port interface Config Interface Port Channel configured as a router port interface	
<b>History</b>	3.3.5006	
<b>Role</b>	admin	
<b>Example</b>	switch (config interface vlan 10)# ip igmp last-member-query-count 7	
<b>Related Commands</b>	N/A	
<b>Note</b>	This parameter reflects expected packet loss on a congested network.	

## ip igmp last-member-query-response-time

```
ip igmp last-member-query-response-time <interval>
no ip igmp last-member-query-response-time
```

Configures the IGMP last member query response time in seconds.  
The no form of the command resets this parameter to its default.

<b>Syntax Description</b>	interval	IGMP last member query response time. Range:1-25 seconds.
<b>Default</b>	1	
<b>Configuration Mode</b>	Config Interface VLAN Config Interface Ethernet configured as a router port interface Config Interface Port Channel configured as a router port interface	
<b>History</b>	3.3.5006	
<b>Role</b>	admin	
<b>Example</b>	switch (config interface vlan 10)# ip igmp last-member-query-response-time 10	
<b>Related Commands</b>	N/A	
<b>Note</b>		

## ip igmp startup-query-count

```
ip igmp startup-query-count <count>
no ip startup-query-count
```

Configures the number of query messages an interface sends during startup.  
The no form of the command resets this parameter to its default.

<b>Syntax Description</b>	count	Range: 1-65535.
<b>Default</b>	2	
<b>Configuration Mode</b>	Config Interface VLAN Config Interface Ethernet configured as a router port interface Config Interface Port Channel configured as a router port interface	
<b>History</b>	3.3.5006	
<b>Role</b>	admin	
<b>Example</b>	switch (config interface vlan 10)# ip igmp startup-query-count 10	
<b>Related Commands</b>	N/A	
<b>Note</b>		

## ip igmp startup-query-interval

```
ip igmp startup-query-interval <interval>
no ip startup-query-interval
```

Configures the IGMP startup query interval in seconds.  
The no form of the command resets this parameter to its default.

<b>Syntax Description</b>	interval	Range: 1-1800 seconds.
<b>Default</b>	30	
<b>Configuration Mode</b>	Config Interface VLAN Config Interface Ethernet configured as a router port interface Config Interface Port Channel configured as a router port interface	
<b>History</b>	3.3.5006	
<b>Role</b>	admin	
<b>Example</b>	switch (config interface vlan 10)# ip igmp startup-query-interval 10	
<b>Related Commands</b>	N/A	
<b>Note</b>		

## ip igmp query-interval

```
ip igmp query-interval <interval>
no ip igmp query-interval
```

Configures the IGMP query interval in seconds.

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

<b>Syntax Description</b>	interval	The IGMP query interval. Range: 1-1800 seconds.
<b>Default</b>	125	
<b>Configuration Mode</b>	Config Interface VLAN	
<b>History</b>	3.3.5006	
<b>Role</b>	admin	
<b>Example</b>	switch (config interface vlan 10)# ip igmp query-interval 60	
<b>Related Commands</b>	N/A	
<b>Note</b>		

## ip igmp query-max-response-time

```
ip igmp query-max-response-time <time>
no ip igmp query-max-response-time
```

Configures the IGMP max response time in seconds.  
The no form of the command resets this parameter to its default.

Syntax Description	time	The IGMP max response time. Range: 1-25 seconds.
<b>Default</b>	10	
<b>Configuration Mode</b>	Config Interface VLAN	
<b>History</b>	3.3.5006	
<b>Role</b>	admin	
<b>Example</b>		switch (config interface vlan 10)# ip igmp query-max-response-time 20
<b>Related Commands</b>	N/A	
<b>Note</b>		

## ip igmp robustness-variable

```
ip igmp robustness-variable <count>
no ip igmp robustness-variable
```

Configures the IGMP robustness variable.

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

Syntax Description	count	IGMP robustness variable. Range: 1-7.
Default	2	
Configuration Mode	Config Interface VLAN Config Interface Ethernet configured as a router port interface Config Interface Port Channel configured as a router port interface	
History	3.3.5006	
Role	admin	
Example		switch (config interface vlan 10)# ip igmp robustness-variable 4
Related Commands	N/A	
Note		<ul style="list-style-type: none"><li>• The robustness variable can be increased to increase the number of times that packets are resent.</li><li>• This parameter reflects expected packet loss on a congested network.</li></ul>

## ip igmp static-oif

```
ip igmp static-oif <group>
no ip igmp static-oif
```

Statically binds an IP interface to a multicast group.  
The no form of the command deletes the static multicast address from the interface.

<b>Syntax Description</b>	group	Multicast IP address.
<b>Default</b>	no ip igmp static-oif	
<b>Configuration Mode</b>	Config Interface VLAN Config Interface Ethernet configured as a router port interface Config Interface Port Channel configured as a router port interface	
<b>History</b>	3.3.5006	
<b>Role</b>	admin	
<b>Example</b>	switch (config interface vlan 10)# ip igmp static-oif 10.10.10.5	
<b>Related Commands</b>	N/A	
<b>Note</b>	PIM must be enabled in order to configure the route in the hardware.	

## clear ip igmp groups

**clear ip igmp groups {all | <group-address> <mask>}**

Clears IGMP group information.

<b>Syntax Description</b>	all	Clears all IGMP groups.
	group-address	Clears a specific group.
<b>Default</b>	no ip igmp static-oif	
<b>Configuration Mode</b>	Config	
<b>History</b>	3.3.5200	
<b>Role</b>	admin	
<b>Example</b>	switch (config)# clear ip igmp groups all switch (config)#	
<b>Related Commands</b>	N/A	
<b>Note</b>		

## debug ethernet ip igmp-l3

```
debug ethernet ip igmp-l3 {all | control-plane | data-path | fail-all | init-shut |
management | memory | packet-dump | resources}
no debug ethernet ip igmp-l3 {all | control-plane | data-path | fail-all | init-shut |
management | memory | packet-dump | resources}
```

Configures the trace level for IGMP.

The no form of the command removes the trace level for IGMP.

<b>Syntax Description</b>	<table border="0"> <tr> <td>all</td><td>Enable track traces.</td></tr> <tr> <td>control-plane</td><td>Control plane traces.</td></tr> <tr> <td>data-path</td><td>IP packet dump trace.</td></tr> <tr> <td>fail-all</td><td>All failures including Packet Validation Trace.</td></tr> <tr> <td>init-shut</td><td>Init and shutdown messages.</td></tr> <tr> <td>management</td><td>Management messages.</td></tr> <tr> <td>memory</td><td>Memory related messages.</td></tr> <tr> <td>packet-dump</td><td>Packet dump messages.</td></tr> <tr> <td>resources</td><td>OS Resource trace.</td></tr> </table>	all	Enable track traces.	control-plane	Control plane traces.	data-path	IP packet dump trace.	fail-all	All failures including Packet Validation Trace.	init-shut	Init and shutdown messages.	management	Management messages.	memory	Memory related messages.	packet-dump	Packet dump messages.	resources	OS Resource trace.
all	Enable track traces.																		
control-plane	Control plane traces.																		
data-path	IP packet dump trace.																		
fail-all	All failures including Packet Validation Trace.																		
init-shut	Init and shutdown messages.																		
management	Management messages.																		
memory	Memory related messages.																		
packet-dump	Packet dump messages.																		
resources	OS Resource trace.																		
<b>Default</b>	N/A																		
<b>Configuration Mode</b>	Config																		
<b>History</b>	3.3.5200																		
<b>Role</b>	admin																		
<b>Example</b>	<code>switch (config)# debug ethernet ip igmp-l3 all</code>																		
<b>Related Commands</b>																			
<b>Note</b>																			

## show ip igmp groups

**show ip igmp groups [<group>] [vlan <vlan-id>]**

Displays information about IGMP-attached group membership.

<b>Syntax Description</b>	group vlan <vlan-id>	Filters the output to a specific IP multicast group address. Filters the output to a specific VLAN ID.
<b>Default</b>	N/A	
<b>Configuration Mode</b>	Any Command Mode	
<b>History</b>		
<b>Role</b>	admin	
<b>Example</b>	<pre>switch (config)# show ip igmp groups IGMP Connected Group Membership for VRF "default" Type: S - Static, D - Dynamic, L - Local, T - SSM Translated  Group Address Type Interface Uptime Expires Last Reporter 225.7.6.0 S vlan19 [0d 00:12:12.14] [0d 00:00:00.00] 0.0.0.0 225.7.10.1 D vlan19 [0d 00:00:01.18] [0d 00:04:08.81] 19.19.19.1 225.7.7.7 S vlan19 [0d 00:12:12.15] [0d 00:00:00.00] 0.0.0.0 225.7.7.7 S vlan21 [0d 00:12:12.15] [0d 00:00:00.00] 0.0.0.0</pre>	
<b>Related Commands</b>	N/A	
<b>Note</b>		

## show ip igmp interface

**show ip igmp interface [vlan <vlan-id> | brief]**

Displays IGMP brief configuration and status.

<b>Syntax Description</b>	brief	Displays brief output information.
	vlan <vlan-id>	Filters the output to a specific VLAN ID.
<b>Default</b>	N/A	
<b>Configuration Mode</b>	Any Command Mode	
<b>History</b>		
<b>Role</b>	admin	

---

**Example**

```
switch(config)#show ip igmp interface
IGMP Interfaces for VRF "default"

VLAN5
Interface status: protocol-down/admin-up/link-down
IP address: 5.5.5.49, IP Subnet: 5.5.5.0/24
Active Querier: 5.5.5.48
Membership count: 0
Route-queue depth: 0
IGMP Version: 2
IGMP query interval: 125 secs, configured value: 125 secs
IGMP max response time: 100 secs, configured value: 100 secs
IGMP startup query interval: 125 secs, configured value: 125 secs
IGMP startup query count: 2
IGMP group timeout: 350 secs, configured value: 350 secs
IGMP querier timeout: 350 secs configured value: 350 secs
IGMP last member mrt: 10 secs configured value: 10
IGMP robustness variable: 2
IGMP interface statistics:
General (sent/received):
v1/v2-reports: 0/0
v2-queries: 3/1,v2-leaves: 0/0
v3-queries: 0/0,
v3-reports: 0/0

VLAN19
Interface status: protocol-up/admin-up/link-up
IP address: 19.19.19.49, IP Subnet: 19.19.19.0/24
Active Querier: 19.19.19.49
Membership count: 3
Route-queue depth: 0
IGMP Version: 2
IGMP query interval: 125 secs, configured value: 125 secs
IGMP max response time: 10 secs, configured value: 10 secs
IGMP startup query interval: 125 secs, configured value: 125 secs
IGMP startup query count: 2
IGMP group timeout: 260 secs, configured value: 260 secs
IGMP querier timeout: 260 secs configured value: 260 secs
IGMP last member mrt: 1 secs configured value: 1
IGMP robustness variable: 2
IGMP interface statistics:
General (sent/received):
v1/v2-reports: 0/5
v2-queries: 14/0,v2-leaves: 0/1
v3-queries: 0/0,
v3-reports: 0/0
```

---

**Related Commands**

N/A

---

**Note**

## 6.8 VRRP

The Virtual Router Redundancy Protocol (VRRP) is a computer networking protocol that provides for automatic assignment of available IP routers to participating hosts. This increases the availability and reliability of routing paths via automatic default gateway selections on an IP sub-network.

The protocol achieves this by creating virtual routers, which are an abstract representation of multiple routers (that is, a master and backup routers, acting as a group). The default gateway of a participating host is assigned to the virtual router instead of a physical router. If the physical router that is routing packets on behalf of the virtual router fails, another physical router is selected to automatically replace it. The physical router that is forwarding packets at any given time is called the master router.

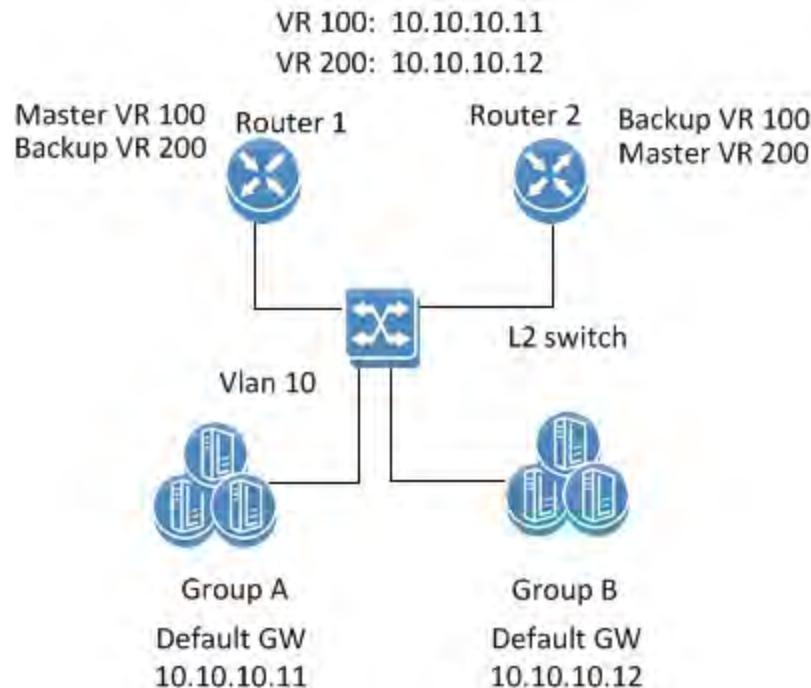
VRRP provides information on the state of a router, not the routes processed and exchanged by that router. Each VRRP instance is limited, in scope, to a single subnet. It does not advertise IP routes beyond that subnet or affect the routing table in any way.

Routers have a priority of between 1-255 and the router with the highest priority becomes the master. The configurable priority value ranges from 1-254, the router which owns the interface IP address as one of its associated IP addresses has the priority value 255. When a planned withdrawal of a master router is to take place, its priority can be lowered, which means a backup router will preempt the master router status rather than having to wait for the hold time to expire.

### 6.8.1 Load Balancing

To create load balancing between routers participating in the same VR, it is recommended to create 2 (or more) VRs. Each router will be a master in one of the VRs, and a backup to the other VR(s). A group of hosts should be configured with Router 1's virtual address as the default gateway, while the second group should be configured with Router 2's virtual address.

**Figure 40: Common VRRP Configuration with Load Balancing**



## 6.8.2 Configuring VRRP

➤ *To configure VRRP:*

Precondition steps:

**Step 1.** Enable IP routing functionality. Run:

```
switch (config)# ip routing
```

**Step 2.** Enable the desired VLAN. Run:

```
switch (config)# vlan 20
```



The VLAN cannot be the same one configured for the MLAG IPL, if MLAG is used.

**Step 3.** Add this VLAN to the desired interface. Run:

```
switch (config)# interface ethernet 1/1
switch (config ethernet 1/1)# switchport access vlan 20
```

**Step 4.** Create a VLAN interface. Run:

```
switch (config)# interface vlan 20
```

**Step 5.** Apply IP address to the VLAN interface.

On one of the switches, run:

```
switch (config interface vlan 20)# ip address 20.20.20.20 /24
```

On the other switch, run:

```
switch (config interface vlan 20)# ip address 20.20.20.30 /24
```

**Step 6.** Enable the interface. Run:

```
switch (config interface vlan 20)# no shutdown
```

#### Configure VRRP:

This is the same configuration on both switches

**Step 1.** Enable VRRP protocol globally. Run:

```
switch (config)# protocol vrrp
```

**Step 2.** Create a virtual router group for an IP interface. Up to 255 VRRP IDs are supported. Run:

```
switch (config interface vlan 20)# vrrp 100
```

**Step 3.** Set the VIP address. Run:

```
switch (config interface vlan 20 vrrp 100)# address 20.20.20.40
```

**Step 4.** Influence the election of the master in the VR cluster make sure that the priority of the desired master is the highest. Note that the higher IP address is selected in case the priority of the routers in the VR are the same. Select the priority. Run:

```
switch (config interface vlan 20 vrrp 100)# priority 200
```

**Step 5.** The advertisement interval should be the same for all the routers within the VR. Modify the interval. Run:

```
switch (config interface vlan 20 vrrp 100)# advertisement-interval 2
```

**Step 6.** The authentication text should be the same for all the routers within the VR. Configure the authentication text. Run:

```
switch (config interface vlan 20 vrrp 100)# authentication text my-password
```

**Step 7.** Use the preempt command to enable a high-priority backup virtual router to preempt the low-priority master virtual router. Run:

```
switch (config interface vlan 20 vrrp 100)# preempt
```

**Step 8.** Disable VRRP. Run:

```
switch (config interface vlan 20 vrrp 100)# shutdown
```



The configuration will not be deleted, only the VRRP state machine will be stopped.

### 6.8.3 Verifying VRRP

**Step 1.** Display VRRP brief status. Run:

```
switch(config)# show vrrp
Interface  VR  Pri  Time   Pre   State VR   IP addr
-----
Vlan20     1   200  2s      Y     Init    20.20.20.20
...
switch(config)#

```

**Step 2.** Display VRRP detailed status. Run:

```
switch (config)# show vrrp detail

VRRP Admin State : Enabled

Vlan20 - Group 1 (IPV4)

Instance Admin State : Enabled
State : Backup
Virtual IP Address : 20.20.20.40
Priority : 200
Advertisement interval (sec) : 2
Preemption : Enabled
Virtual MAC address : AA:BB:CC:DD:EE:FF
switch (config)#

```

**Step 3.** Display VRRP statistic counters. Run:

```
switch (config)# show vrrp statistics
Ethernet1/5 - Group 1 (IPV4)
Invalid packets:          0
Too short:                0
Transitions to Master    6
Total received:           155
Bad TTL:                  0
Failed authentication:    0
Unknown authentication:   0
Conflicting authentication: 0
Conflicting Advertise time: 0
Conflicting Addresses:    0
Received with zero priority: 3
Sent with zero priority:   3
switch (config)#

```

## 6.8.4 Commands

### protocol vrrp

**protocol vrrp**  
**no protocol vrrp**

Enables VRRP globally and unhides VRRP related commands.  
The no form of the command deletes all the VRRP configuration and hides VRRP related commands.

<b>Syntax Description</b>	N/A
<b>Default</b>	no feature vrrp
<b>Configuration Mode</b>	Config
<b>History</b>	3.3.4500
<b>Role</b>	admin
<b>Example</b>	switch (config)# protocol vrrp
<b>Related Commands</b>	
<b>Note</b>	

**vrrp**

**vrrp <number>**  
**no vrrp <number>**

Creates a virtual router group on this interface and enters a new configuration mode.  
The no form of the command deletes the VRRP instance and the related configuration.

<b>Syntax Description</b>	number	A VRRP instance number. Range is 1-255.
<b>Default</b>	N/A	
<b>Configuration Mode</b>	Config Interface VLAN	
<b>History</b>	3.3.4500	
<b>Role</b>	admin	
<b>Example</b>	<pre>switch (config interface vlan 10)# switch (config interface vlan 10 vrrp 10)#</pre>	
<b>Related Commands</b>		
<b>Note</b>	A maximum total of 255 VRRP instances are supported per switch system.	

## address

```
address <ip-address> [secondary]
no address [<ip-address> [secondary]]
```

Sets virtual router IP address (primary and secondary).  
The no form of the command deletes the IP address from the VRRP interface.

<b>Syntax Description</b>	ip-address secondary	The virtual IP address. A secondary IP address for the virtual router.
<b>Default</b>	N/A	
<b>Configuration Mode</b>	Config VRRP Interface	
<b>History</b>	3.3.4500	
<b>Role</b>	admin	
<b>Example</b>		<pre>switch (config vrrp 100)# address 10.10.10.10 switch (config vrrp 100)# address 10.10.10.11 secondary switch (config vrrp 100)# address 10.10.10.12 secondary</pre>
<b>Related Commands</b>		
<b>Note</b>	<ul style="list-style-type: none"><li>This command is the enabler of the protocol. Therefore, set all the protocol parameters initially and only then set the ip-address.</li><li>There are up to 10 IP addresses associated with the VRRP instance. One primary and up to 10 secondary ip-addresses.</li><li>If the configured IP address is the same as the interface IP address, this switch automatically owns the IP address (priority 255).</li></ul>	

## shutdown

**shutdown**  
**no shutdown**

Disables the virtual router.

The no form of the command enables the virtual router (stops the VRRP state machine).

<b>Syntax Description</b>	N/A
<b>Default</b>	Enabled (no shutdown)
<b>Configuration Mode</b>	Config VRRP Interface
<b>History</b>	3.3.4500
<b>Role</b>	admin
<b>Example</b>	switch (config vrrp 100)# shutdown
<b>Related Commands</b>	
<b>Note</b>	

## priority

**priority <level>**  
**no priority**

Sets the priority of the virtual router.

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

<b>Syntax Description</b>	level	The virtual router priority level. Range is 1-254.
<b>Default</b>	100	
<b>Configuration Mode</b>	Config VRRP Interface	
<b>History</b>	3.3.4500	
<b>Role</b>	admin	
<b>Example</b>	switch (config vrrp 100)# priority 200	
<b>Related Commands</b>		
<b>Note</b>	<ul style="list-style-type: none"><li>The higher IP address will be selected as master, in case the priority of the routers in the VR are the same.</li><li>To influence the election of the master in the VR cluster make sure that the priority of the desired master is the higher.</li></ul>	

## preempt

**preempt**  
**no preempt**

Sets virtual router preemption mode.

The no form of the command disables the virtual router preemption.

<b>Syntax Description</b>	N/A
<b>Default</b>	Enabled (preempt)
<b>Configuration Mode</b>	Config VRRP Interface
<b>History</b>	3.3.4500
<b>Role</b>	admin
<b>Example</b>	switch (config vrrp 100)# preempt
<b>Related Commands</b>	
<b>Note</b>	To set this router as backup for the current virtual router master, preempt must be enabled.

## authentication text

**authentication text <password>**  
**no authentication text**

Sets virtual router authentication password and enables authentication.  
The no form of the command disables the authentication mechanism.

<b>Syntax Description</b>	password	The virtual router authentication password. The password string must be up to 8 alphanumeric characters.		
<b>Default</b>	Disabled			
<b>Configuration Mode</b>	Config VRRP Interface			
<b>History</b>	3.3.4500			
<b>Role</b>	admin			
<b>Example</b>	switch (config vrrp 100)# authentication text mypassword			
<b>Related Commands</b>				
<b>Note</b>				

## advertisement-interval

**advertisement-interval <seconds>**  
**no advertisement-interval**

Sets the virtual router advertisement-interval.  
The no form of the command resets the parameter to its default.

<b>Syntax Description</b>	seconds	The virtual router advertisement-interval in seconds. Range: 1-255.
<b>Default</b>	1	
<b>Configuration Mode</b>	Config VRRP Interface	
<b>History</b>	3.3.4500	
<b>Role</b>	admin	
<b>Example</b>	switch (config vrrp 100)# advertisement-interval 10	
<b>Related Commands</b>		
<b>Note</b>		

## show vrrp

**show vrrp [interface <type> <number>] [vr <id>]**

Displays VRRP brief configuration and status.

<b>Syntax Description</b>	interface <type> <number> vr <id>	Filters the output to a specific interface type and number. Filters the output to a specific virtual router. Range: 1-10.
<b>Default</b>	N/A	
<b>Configuration Mode</b>	Any Command Mode	
<b>History</b>	3.3.4500	
<b>Role</b>	admin	
<b>Example</b>	<pre>switch(config)# show vrrp Interface  VR Pri Time Pre State VR  IP addr ----- Eth1/5      1 200 2s   Y    Init      192.0.1.10 ... switch(config)#+</pre>	
<b>Related Commands</b>		
<b>Note</b>		

## show vrrp detail

**show vrrp detail [interface <type> <number>] [vr <id>]**

Displays detailed VRRP configuration and status.

<b>Syntax Description</b>	interface <type> <number>	Filters the output to a specific interface type and number		
	vr <id>	Filters the output to a specific virtual router. Range: 1-255		
<b>Default</b>	N/A			
<b>Configuration Mode</b>	Any Command Mode			
<b>History</b>	3.3.4500			
	3.6.5000	Updated Example		
<b>Role</b>	admin			
<b>Example</b>	<pre>switch (config)# show vrrp detail VRRP Admin State: Enabled  Vlan3200 - Vrrp 110 (IPV4):   Instance Admin State: Enabled   State: Init   Virtual IP Address: 33.0.0.2   Priority: 100   Advertisement interval(sec): 2   Preemption: Enabled   Virtual MAC address: 00:00:5E:00:01:6E   Master router: 33.0.0.1   Master priority: 100   Master advertisement interval: 2   Associated IP Addresses:     33.0.0.3     33.0.0.4</pre>			
<b>Related Commands</b>				
<b>Note</b>				

## show vrrp statistics

**show vrrp statistics [interface <type <number>] [vr <id>] [all]**

Displays VRRP counters.

<b>Syntax Description</b>	interface <type> <number>	Filters the output to a specific interface type and number
	vr <id>	Filters the output to a specific virtual router Range: 1-255
<b>Default</b>	N/A	
<b>Configuration Mode</b>	Any Command Mode	
<b>History</b>	3.3.4500	
	3.6.5000	Updated Example
<b>Role</b>	admin	
<b>Example</b>	<pre>switch (config)# show vrrp statistics VRRP Instance 100:     Invalid packets:          0     Too short:                0     Transitions to Master:    0     Total received:           0     Bad TTL:                  0     Failed authentication:    0     Unknown authentication:   0     Conflicting authentication: 0     Conflicting Advertise time: 0     Conflicting Addresses:    0     Received with zero priority: 0     Sent with zero priority: 0</pre>	

### Related Commands

### Note

## 6.9 MAGP

Multi-active gateway protocol (MAGP) is aimed to solve the default gateway problem when a host is connected to a set of switch routers (SRs) via MLAG.

The network functionality in that case requires that each SR is an active default gateway router to the host, thus reducing hops between the SRs and directly forwarding IP traffic to the L3 cloud regardless which SR traffic comes through.



Designated traffic, such as ping to the MAGP interface is not supported. One of the two switches will be able to ping, so a ping from one switch can be done.

### 6.9.1 Configuring MAGP

Prerequisite steps:

- Step 1.** Enable IP routing functionality. Run:

```
switch (config)# ip routing
```

- Step 2.** Enable the desired VLAN. Run:

```
switch (config)# vlan 20
switch (config vlan 20)#
```



The VLAN cannot be the same one configured for the MLAG IPL, if MLAG is used.

- Step 3.** Add this VLAN to the desired interface. Run:

```
switch (config)# interface ethernet 1/1
switch (config interface ethernet 1/1)# switchport access vlan 20
```

- Step 4.** Create a VLAN interface. Run:

```
switch (config)# interface vlan 20
switch (config interface vlan 20)#
```

- Step 5.** Set an IP address to the VLAN interface. Run:

```
switch (config interface vlan 20)# ip address 11.11.11.11 /8
```

- Step 6.** Enable the interface. Run:

```
switch (config interface vlan 20)# no shutdown
```

➤ **To configure MAGP:**

- Step 1.** Enable MAGP protocol globally. Run:

```
switch (config)# protocol magp
```

- Step 2.** Create a virtual router group for an IP interface. Run:

```
switch (config interface vlan 20)# magp 100
```



Up to 255 MAGP IDs are supported.

**Step 3.** Set a virtual router primary IP address. Run:

```
switch (config interface vlan 20 magp 100)# ip virtual-router address 11.11.11.254
```



The IP address must be in the same subnet of the VLAN interface. This IP address is the default gateway for this MAGP instance. This should become the default gateway configured on the hosts connected to the relevant MLAG.

**Step 4.** Set a virtual router primary MAC address. Run:

```
switch (config interface vlan 20 magp 100)# ip virtual-router mac-address  
AA:BB:CC:DD:EE:FF
```



To obtain the virtual router's MAC address, please run the command "show vrrp detail".

➤ **To verify the MAGP configuration, run:**

```
switch (config)# show magp 100  
MAGP 100  
  Interface vlan: 20  
  Admin state: Master  
  State: Enabled  
  Virtual IP: 11.11.11.254  
  Virtual MAC: AA:BB:CC:DD:EE:FF
```



This output is to be expected in both MAGP switches.



For more advanced configuration options, please refer to the following Mellanox Community post: <https://community.mellanox.com/docs/DOC-1476>.

## 6.9.2 Commands

### protocol magp

**protocol magp**  
**no protocol magp**

Enables MAGP globally and unhides MAGP commands.  
The no form of the command deletes all the MAGP configuration and hides MAGP commands.

<b>Syntax Description</b>	N/A
<b>Default</b>	Disabled
<b>Configuration Mode</b>	Config
<b>History</b>	3.3.4500
<b>Role</b>	admin
<b>Example</b>	<pre>switch (config)# protocol magp switch (config)#{/pre}</pre>
<b>Related Commands</b>	
<b>Note</b>	IP routing must be enabled to enable MAGP.

## magp

```
magp <instance>
no magp <instance>
```

Creates an MAGP instance on this interface and enters a new configuration mode.  
The no form of the command deletes the MAGP instance.

<b>Syntax Description</b>	instance	MAGP instance number. Range: 1-255.
<b>Default</b>	Disabled	
<b>Configuration Mode</b>	Config Interface VLAN	
<b>History</b>	3.3.4500	
<b>Role</b>	admin	
<b>Example</b>	<pre>switch (config interface vlan 20)# magp 100 switch (config interface vlan 20 magp 100)# </pre>	
<b>Related Commands</b>		
<b>Note</b>	<ul style="list-style-type: none"><li>Only one MAGP instance can be created on an interface</li><li>Different interfaces cannot share an MAGP instance</li><li>MAGP and VRRP are mutually exclusive</li></ul>	

## shutdown

**shutdown**  
**no shutdown**

Enables MAGP instance.

The no form of the command disables the MAGP instance.

<b>Syntax Description</b>	N/A
<b>Default</b>	Disabled
<b>Configuration Mode</b>	Config Interface VLAN MAGP
<b>History</b>	3.3.4500
<b>Role</b>	admin
<b>Example</b>	<pre>switch (config interface vlan 10 magp 1)# shutdown</pre>
<b>Related Commands</b>	
<b>Note</b>	

## ip virtual-router address

```
ip virtual-router address <ip-address>
no ip virtual-router address
```

Sets MAGP virtual IP address.

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

<b>Syntax Description</b>	ip-address	The virtual router IP address.
<b>Default</b>	N/A	
<b>Configuration Mode</b>	Config Interface VLAN MAGP	
<b>History</b>	3.3.4500	
<b>Role</b>	admin	
<b>Example</b>	<pre>switch (config interface vlan 10 magp 1)# ip virtual-router address 10.10.10.10 switch (config interface vlan 10 magp 1)# </pre>	
<b>Related Commands</b>		
<b>Note</b>	The MAGP virtual IP address must be different from the interface IP address	

## ip virtual-router mac-address

```
ip virtual-router mac-address <mac-address>
no ip virtual-router mac-address
```

Sets MAGP virtual MAC address.

The no form of the command resets the MAC address to its default.

Syntax Description	mac-address	MAC address. Format: AA:BB:CC:DD:EE:FF.
<b>Default</b>	00:00:5E:00:01-<magp instance>	
<b>Configuration Mode</b>	Config Interface VLAN MAGP	
<b>History</b>	3.3.4500	
<b>Role</b>	admin	
<b>Example</b>	<pre>switch (config interface vlan 10 magp 1)# ip virtual-router mac-address AA:BB:CC:DD:EE:FF switch (config interface vlan 10 magp 1)# </pre>	
<b>Related Commands</b>		
<b>Note</b>		

## show magp

**show magp [<instance>]**

Displays the MAGP configuration.

<b>Syntax Description</b>	instance	Displays configuration of a specific MAGP instance Range: 1-255
<b>Default</b>	N/A	
<b>Configuration Mode</b>	Any Command Mode	
<b>History</b>	3.3.4500	
	3.6.5000	Updated Example
<b>Role</b>	admin	
<b>Example</b>	<pre>switch (config)# show magp MAGP 1   Interface vlan: 12   Admin state: Enabled   State: Init   Virtual IP: 172.3.12.5   Virtual MAC: 00:00:00:00:00:00  MAGP 2   Interface vlan: 4000   Admin state: Enabled   State: Init   Virtual IP: 0.0.0.0   Virtual MAC: 00:00:00:00:00:00</pre>	

---

### Related Commands

---

### Note

## show magp interface vlan

**show magp interface vlan <id>**

Displays the configuration of a specific MAGP instance.

<b>Syntax Description</b>	instance	MAGP instance number. Range: 1-255.
<b>Default</b>	N/A	
<b>Configuration Mode</b>	Any Command Mode	
<b>History</b>	3.3.4500	
	3.6.5000	Updated Example
<b>Role</b>	admin	
<b>Example</b>	<pre>switch (config)# show magp interface vlan 12 MAGP 1   Interface vlan: 12   Admin state: Enabled   State: Init   Virtual IP: 172.3.12.5   Virtual MAC: 00:00:00:00:00:00</pre>	
<b>Related Commands</b>		
<b>Note</b>		

## 6.10 DHCP Relay



DHCP Relay (DHCP-R) is not supported on SX10xx-xxxR and SX60xx-xxxR systems.

Since Dynamic Host Configuration Protocol must work correctly even before DHCP clients have been configured, the DHCP server and DHCP client need to be connected to the same network.

In larger networks, this is not always practical because each network link contains one or more DHCP relay agents. These DHCP-R agents receive messages from DHCP clients and forward them to DHCP servers thus extending the reach of the DHCP beyond the local network.

DHCP-R is supported for both IPv4 and IPv6.

### 6.10.1 DHCP-R Virtual Routing and Forwarding (VRF) Auto-Helper

In some cases it is desired that DHCP-R functionality is automatically enabled to all IP interfaces in the system. For this purpose a vrf-auto-helper may be configured on a DHCP-R instance which would provide DHCP-R services automatically for each newly created interface on a VRF.

Only one instance in each VRF can have vrf-auto-helper capability. Whenever a new instance is created in a VRF, it automatically becomes a vrf-auto-helper.

It is possible to manually disable auto-helper capability for the instance. See command “[vrf-auto-helper](#)” on page [1401](#) for more information.

## 6.10.2 Commands

### ip dhcp relay

```
ip dhcp relay [instance <instance-id>]  
no ip dhcp relay [instance <instance-id>]
```

Enters DHCP relay instance configuration mode, and creates DHCP instance in active VRF context.

The no form of the command deletes the instance and DHCP relay process corresponding to it.

<b>Syntax Description</b>	instance-id	Range: 1-8
<b>Default</b>	N/A	
<b>Configuration Mode</b>	Config	
<b>History</b>	3.6.3004	
<b>Role</b>	admin	
<b>Example</b>	<pre>switch (config)# ip dhcp relay instance 1 switch (config ip dhcp relay instance 1)#+</pre>	
<b>Related Commands</b>	N/A	
<b>Note</b>	If an instance is not specified then instance 1 is used (if nonexistent, then it is created).	

## address

**address <ip-address>**  
**no address <ip-address>**

Configures the DHCP server IP address on a particular instance.  
The no form of the command deletes the DHCP server IP address.

<b>Syntax Description</b>	ip-address	Valid IP unicast address of DHCP server.
<b>Default</b>	N/A	
<b>Configuration Mode</b>	Config IP DHCP Relay	
<b>History</b>	3.3.4150	
	3.6.1002	Added VRF parameter
	3.6.3004	Enhanced command for DHCP-R multi-instance
<b>Role</b>	admin	
<b>Example</b>	switch (config ip dhcp relay instance 1)# address 1.2.3.4	
<b>Related Commands</b>	ip dhcp relay	
<b>Note</b>	<ul style="list-style-type: none"><li>Up to 16 IP addresses may be configured</li><li>To enable DHCP relay instance, at least one IP address should be configured, or always-on parameter should be turned on using the command “ip dhcp relay always-on”</li><li>The following option for running this command is also possible: ip dhcp relay instance 1 address &lt;ip-address&gt;. However, if an instance is not specified then instance 1 is used (if nonexistent, then it is created).</li></ul>	

## always-on

**always-on**  
**no always-on**

Enables broadcast mode on a particular instance.

The no form of the command disables the broadcast mode from instance.

<b>Syntax Description</b>	vrf	VRF name
<b>Default</b>	Disabled	
<b>Configuration Mode</b>	Config IP DHCP Relay	
<b>History</b>	3.3.4150	
	3.6.1002	Added VRF parameter
	3.6.3004	Enhanced command for DHCP-R multi-instance
<b>Role</b>	admin	
<b>Example</b>	switch (config ip dhcp relay instance 1)# always-on	
<b>Related Commands</b>	ip dhcp relay	
<b>Note</b>	<ul style="list-style-type: none"> <li>Broadcasts DHCP requests to all interfaces with the DHCP relay agent for given VRF</li> <li>In order to enable DHCP relay, at least one IP address should be configured, or always-on parameter should be turned on using this command</li> <li>When DHCP servers are configured, requests are forwarded only to configured servers</li> <li>The following option for running this command is also possible: ip dhcp relay instance 1 always-on. However, if an instance is not specified then instance 1 is used (if nonexistent, then it is created).</li> </ul>	

## information option

**information option**  
**no information option**

Enables DHCP relay agents to insert option 82 on the packets of a particular instance. The no form of the command removes option 82 from the packets.

<b>Syntax Description</b>	N/A
<b>Default</b>	Disabled
<b>Configuration Mode</b>	Config IP DHCP Relay
<b>History</b>	3.3.4150 3.6.3004 Enhanced command for DHCP-R multi-instance
<b>Role</b>	admin
<b>Example</b>	switch (config ip dhcp relay instance 1)# information option
<b>Related Commands</b>	ip dhcp relay
<b>Note</b>	The following option for running this command is also possible: ip dhcp relay instance 1 information option. However, if an instance is not specified then instance 1 is used (if nonexistent, then it is created).

**vrf**

```
vrf <vrf-name>
no vrf <vrf-name>
```

Configures mention instance in the given VRF.  
The no form of the command moves the instance back to default VRF.

<b>Syntax Description</b>	N/A
<b>Default</b>	N/A
<b>Configuration Mode</b>	Config IP DHCP Relay
<b>History</b>	3.6.3004
<b>Role</b>	admin
<b>Example</b>	<pre>switch (config ip dhcp relay instance 1)# vrf 2</pre>
<b>Related Commands</b>	N/A
<b>Note</b>	<ul style="list-style-type: none"><li>• If no VRF is specified, then the DHCP-R instance is created in the active VRF</li><li>• If the VRF is changed, then the configuration of the DHCP-R instance is automatically deleted</li><li>• The following option for running this command is also possible: ip dhcp relay instance 1 vrf &lt;vrf-name&gt;. However, if an instance is not specified then instance 1 is used (if nonexistent, then it is created).</li></ul>

## port

```
port <udp-port>
no port <udp-port>
```

Changes the UDP port for the given instance.  
The no form of the command sets the UDP port to default value.

<b>Syntax Description</b>	udp-port	UDP port Range: 1-65534
<b>Default</b>	67	
<b>Configuration Mode</b>	Config IP DHCP Relay	
<b>History</b>	3.6.3004	
<b>Role</b>	admin	
<b>Example</b>	switch (config ip dhcp relay instance 1)# port 65534	
<b>Related Commands</b>	N/A	
<b>Note</b>	<ul style="list-style-type: none"><li>The system allocated 2 ports: One is the server port (udp-port), and another is client port (udp-port+1)</li><li>The following option for running this command is also possible: ip dhcp relay instance 1 port &lt;udp-port&gt;. However, if an instance is not specified then instance 1 is used (if nonexistent, then it is created).</li></ul>	

## vrf-auto-helper

**vrf-auto-helper**  
**no vrf-auto-helper**

Makes all L3 interfaces (existing/newly created) to be part of the given instance.  
The no form of the command resets this parameter to its default

<b>Syntax Description</b>	N/A
<b>Default</b>	N/A
<b>Configuration Mode</b>	Config IP DHCP Relay
<b>History</b>	3.6.3004
<b>Role</b>	admin
<b>Example</b>	<pre>switch (config ip dhcp relay instance 1)# vrf-auto-helper</pre>
<b>Related Commands</b>	N/A
<b>Note</b>	<ul style="list-style-type: none"><li>Every new DHCP-R instance created in a VRF automatically becomes the VRF auto-helper if no other DHCP-R instance has been configured VRF auto-helper previously in that VRF</li><li>The following option for running this command is also possible: ip dhcp relay instance 1 vrf-auto-helper. However, if an instance is not specified then instance 1 is used (if nonexistent, then it is created).</li></ul>

## ip dhcp relay instance

**ip dhcp relay [instance <instance-id>]  
no ip dhcp relay [instance <instance-id>]**

Enables the given interface to listen for DHCP packets coming from specified instance (i.e. binds interface to that instance).

The no form of the command removes the interface mapping from that instance.

<b>Syntax Description</b>	instance-id	DHCP instance ID Range: 1-8
<b>Default</b>	N/A	
<b>Configuration Mode</b>	Config Interface VLAN Config Interface Port Channel Config Interface Ethernet set as router port interface	
<b>History</b>	3.6.3004	
<b>Role</b>	admin	
<b>Example</b>	switch (config interface vlan 10)# ip dhcp relay instance 7	
<b>Related Commands</b>	N/A	
<b>Note</b>	<ul style="list-style-type: none"> <li>• In order to enable DHCP relay, at least one IP address should be configured, or always-on parameter should be turned on using the command “ip dhcp relay always-on”</li> <li>• When DHCP servers are configured, requests are forwarded only to configured servers</li> <li>• Only an existent DHCP-R may be specified</li> </ul>	

## clear ip dhcp relay counters

**clear ip dhcp relay counters [vrf {<vrf-name> | all} | instance <instance-id>]**

Clears all DHCP relay counters (all interfaces) in a given VRF or instance.

<b>Syntax Description</b>	vrf-name instance-id	VRF name or “all” for all VRFs DHCP instance ID Range: 1-8
<b>Default</b>	N/A	
<b>Configuration Mode</b>	Config	
<b>History</b>	3.3.4150 3.6.1002 3.6.3004 3.6.5000	Added VRF parameter Enhanced command for DHCP-R multi-instance Added “all” parameter
<b>Role</b>	admin	
<b>Example</b>	switch (config)# clear ip dhcp relay counters	
<b>Related Commands</b>	N/A	
<b>Note</b>	<ul style="list-style-type: none"><li>If no DHCP-R instance is specified, then the counters of all DHCP-R instances are cleared</li><li>If a VRF is specified, then the counters of all instances on that VRF are cleared</li><li>The command “clear counters all” may also be used to clear all DHCP-R counters</li></ul>	

### 6.10.2.1 Interface Commands

#### ip dhcp relay information option circuit-id

```
ip dhcp relay information option circuit-id <label>
no ip dhcp relay information option circuit-id
```

Specifies the content of the circuit ID sub-option attached to the client DHCP packet when it is forwarded a DHCP server.

The no form of the command removes the label assigned.

<b>Syntax Description</b>	label	Specifies the label attached to packets. The string may be up to 15 characters.
<b>Default</b>	The label is taken from the IP interface name (e.g. “vlan1”)	
<b>Configuration Mode</b>	Config Interface VLAN Config Interface Ethernet set as router port interface Config Interface Port Channel set as router port interface	
<b>History</b>	3.3.4150	
	3.6.1002	Added VRF parameter
<b>Role</b>	admin	
<b>Example</b>	switch (config interface vlan 10)# ip dhcp relay information options circuit-id my-label	
<b>Related Commands</b>	N/A	
<b>Note</b>	The circuit ID sub-option is an IP interface attribute which is shared across all DHCP-R instances.	

### 6.10.2.2 Show Commands

#### show ip dhcp relay

**show ip dhcp relay [instance <instance-id>]**

Displays general DHCP configuration.

<b>Syntax Description</b>	instance-id	If instance ID is specified, then a particular instance configuration is displayed
<b>Default</b>	N/A	
<b>Configuration Mode</b>	Any Command Mode	
<b>History</b>	3.3.4150	
	3.6.1002	Added VRF and all parameters
	3.6.3004	Updated output and parameters
<b>Role</b>	admin	
<b>Example</b>	<pre>switch (config)# show ip dhcp relay instance 7  Instance ID: 7 VRF Name : default DHCP Servers: 1.1.2.1 DHCP relay agent options:     always-on : Disabled     Information Option : Disabled     UDP port : 90     Auto-helper : Enabled      Interface   Label     -----     vlan40      N/A     vlan50      my-instance</pre>	
<b>Related Commands</b>	N/A	
<b>Note</b>	If no DHCP-R instance is given, then all DHCP-R instances are displayed	

## show ip dhcp relay counters

**show ip dhcp relay counters [instance <instance-id> | vrf <vrf-name>]**

Displays the DHCP relay counters.

<b>Syntax Description</b>	instance-id vrf	Displays the DHCP relay counters for a given instance Displays the DHCP relay counters in a given VRF
<b>Default</b>	N/A	
<b>Configuration Mode</b>	Any Command Mode	
<b>History</b>	3.3.4150 3.6.1002 3.6.5000	Added VRF and all parameters Updated output example
<b>Role</b>	admin	
<b>Example</b>	<pre>switch (config) # show ip dhcp relay counters instance 2  Instance: 2 VRF Name: vrf-default  DHCP Counter flags:   SPR: Server Packets Received   SPE: Server Packets Error   SPRE: Server Packet Relayed   CPR: Client Packets Received   RP: Relay Packets   RE: Relay Errors  ----- Req/Resp      Received      Forwarded ----- All Req        2            2 All Res        2            2  ----- If          SPRE      SPE      SPR      CPR ----- vlan40       0          0        2        0 vlan50       2          0        0        2  Packets Relayed to Server: ----- Server      RP      RE ----- 1.1.3.1     2        0 </pre>	
<b>Related Commands</b>	N/A	
<b>Note</b>		

## 6.10.3 DHCPv6 Relay

### 6.10.3.1 Commands

#### 6.10.3.1.1Config

##### **ipv6 dhcp relay instance**

[no] **ipv6 dhcp relay instance <instance-id> [vrf-auto-helper]**

Enables DHCP relay instance configuration mode, and creates DHCP instance in active VRF context.

An instance without an assigned addresses is sent to All\_DHCP\_servers address.  
The “no” form of the command deletes the DHCP relay instance.

<b>Syntax Description</b>	instance-id	DHCP instance ID Range: 1-8
	vrf-auto-helper	Instance becomes VTF auto helper
<b>Default</b>	Disabled	
<b>Configuration Mode</b>	Config Router BGP	
<b>History</b>	3.6.4070	First release
<b>Role</b>	admin	
<b>Example</b>	switch (config)# ipv6 dhcp relay instance 1	
<b>Related Commands</b>		
<b>Note</b>		

## ipv6 dhcp relay instance

[no] **ipv6 dhcp relay instance <instance-id> address <ipv6-address or list of addresses>**

Configure the server address on a particular instance.

Instance without assigned addresses will send to All\_DHCP\_servers address.

The no form of the command will delete the server address from instance.

<b>Syntax Description</b>	instance-id	DHCP instance ID. Range: 1-8.
	ipv6-address	Valid global unicast IPv6 server address. Up to 16 addresses can be assigned per instance.
<b>Default</b>	instance-id	No
<b>Configuration Mode</b>	Config	
<b>History</b>	3.6.4070	First release
<b>Role</b>	admin	
<b>Example</b>	switch (config)# ipv6 dhcp relay instance 1 address 2001::1	
<b>Related Commands</b>		
<b>Note</b>		

## ipv6 dhcp relay instance address

[no] **ipv6 dhcp relay instance <instance-id> address <link local address>**

Configure the server address on a particular instance on specific interface. Only link local address is supported

The no form of the command will delete the server address from instance.

<b>Syntax Description</b>	instance-id	DHCP instance ID. Range: 1-8.
	ipv6-address	Valid global unicast IPv6 server address. Up to 16 addresses can be assigned per instance.
<b>Default</b>	instance-id	No
<b>Configuration Mode</b>	Config	
<b>History</b>	3.6.4070	First release
<b>Role</b>	admin	
<b>Example</b>	switch (config)# ipv6 dhcp relay instance 1 address fe80::1	
<b>Related Commands</b>		
<b>Note</b>		

## ipv6 dhcp relay instance interface-id option

[no] ipv6 dhcp relay instance <instance-id> interface-id option

Enables the instance to insert interface-id option. Default interface-id is an interface name e.g. vlan1, eth1/1

The no form of the command will disable this option.

<b>Syntax Description</b>	instance-id	DHCP instance ID. Range: 1-8.
<b>Default</b>	instance-id	No
<b>Configuration Mode</b>	Config	
<b>History</b>	3.6.4070	First release
<b>Role</b>	admin	
<b>Example</b>	switch (config)# ipv6 dhcp relay instance 1 interface-id option	
<b>Related Commands</b>		
<b>Note</b>		

## ipv6 dhcp relay instance vrf

[no] **ipv6 dhcp relay instance <instance-id> vrf <vrf-name>**

Configures instance in the given VRF.

The no form of the command will move the instance back to default VRF.

<b>Syntax Description</b>	instance-id	DHCP instance ID. Range: 1-8.
	vrf-name	Name of VRF.
<b>Default</b>	instance-id	No
<b>Configuration Mode</b>	Config	
<b>History</b>	3.6.4070	First release
<b>Role</b>	admin	
<b>Example</b>	switch (config)# ipv6 dhcp relay 1 vrf blue	
<b>Related Commands</b>		
<b>Note</b>	When an instance is moved from one VRF to another - it loses all its current configuration.	

## ipv6 dhcp relay instance port

[no] **ipv6 dhcp relay instance <instance-id> port <udp-port>**

Modifies the UDP port for the given instance.

The no form of the command will set the UDP port to default value.

<b>Syntax Description</b>	instance-id	DHCP instance ID. Range: 1-8.		
	vrf-name	UDP Port ID. Range: 1-65534. Default: 547.		
<b>Default</b>	instance-id	No		
<b>Configuration Mode</b>	Config			
<b>History</b>	3.6.4070	First release		
<b>Role</b>	admin			
<b>Example</b>	switch (config)# ipv6 dhcp relay 1 port 555			
<b>Related Commands</b>				
<b>Note</b>				

## ipv6 dhcp relay instance

**ipv6 dhcp relay instance <instance-id> [upstream | downstream]**

Modifies the UDP port for the given instance.

The no form of the command will set the UDP port to default value.

<b>Syntax Description</b>	instance-id	DHCP instance ID. Range: 1-8.
	upstream	The interface on which queries will be received from clients or from other relay agents.
	downstream	The interface to which queries from clients and other relay agents should be forwarded.
<b>Default</b>	N/A	
<b>Configuration Mode</b>	Config	
<b>History</b>	3.6.4070	First release
<b>Role</b>	admin	
<b>Example</b>	switch (config)# ipv6 dhcp relay instance 1 upstream	
<b>Related Commands</b>		
<b>Note</b>	<ul style="list-style-type: none"> <li>• Error will occur if interface/port is already bind to an existing instance</li> <li>• If instance doesn't exist, it will be created</li> <li>• Each interface is either upstream or downstream. Setting another value overwrites the previous</li> <li>• An instance must have at least one upstream and one downstream interface to become active</li> </ul>	

## ipv6 dhcp relay instance interface-id option

**ipv6 dhcp relay instance <instance-id> interface-id option [user-defined-id]**

Specifies the content of the interface-id option that will be sent by the relay agent.

<b>Syntax Description</b>	instance-id	DHCP instance ID. Range: 1-8.
	user-defined-id	Interface-id option content. Length: 1-15 (char) Default: interface name
<b>Default</b>	N/A	
<b>Configuration Mode</b>	Config	
<b>History</b>	3.6.4070	First release
<b>Role</b>	admin	
<b>Example</b>	switch (config)# ipv6 dhcp relay instance <instance-id> interface-id option eth1/1	
<b>Related Commands</b>		
<b>Note</b>		

## clear ipv6 dhcp relay counters

```
clear ipv6 dhcp relay counters [vrf {<vrf-name> | all} | instance <instance-id> |  
interface <name>]
```

Clears DHCP relay counters for specific instance or all instances in given VRF or all instances in the system.

Syntax Description	vrf-name	VRF name or “all” for all VRFs
	instance-id	DHCP instance ID Range: 1-8
Default	N/A	
Configuration Mode	Config	
History	3.6.4070	First release
	3.6.5000	Added “all” parameter
Role	admin	
Example	switch (config)# clear ipv6 dhcp relay counters vrf all	
Related Commands		
Note		

### 6.10.3.1.2 Show

#### show ipv6 dhcp relay

```
show ipv6 dhcp relay [instance <instance-id>]
```

Displays general DHCP configuration on all instances.

If instance id is defined then specific instance configuration is displayed.

<b>Syntax Description</b>	instance-id	DHCP instance ID. Range: 1-8.
<b>Default</b>	instance-id	No
<b>Configuration Mode</b>	Config	
<b>History</b>	3.6.4070	First release
	3.6.5000	Updated example
<b>Role</b>	admin	
<b>Example</b>	<pre>switch (config)# show ipv6 dhcp relay instance 1</pre> <pre>----- Interface      DHCPv6 Enabled    DHCPv6 Running   Valid lease  Client ID -----</pre> <pre>dummy0         no            no          no lo             no            no          no mgmt0          no            no          no mgmt1          no            no          no mgmts0         no            no          no mgmts1         no            no          no vif1           no            no          no</pre> <pre>DHCPv6 primary interface: Configured: mgmt0 Active:     (none)</pre> <pre>DHCPv6 client options: Stateless query: no</pre> <pre>switch (config)# </pre>	
<b>Related Commands</b>		
<b>Note</b>		

## show ipv6 dhcp relay counters

**show ipv6 dhcp relay counters [vrf <vrf-name> | instance <instance-id>]**

Displays counters of all DHCP instances configured on the system.

<b>Syntax Description</b>	instance-id	DHCP instance ID. Range: 1-8.
<b>Default</b>	instance-id	No
<b>Configuration Mode</b>	Config	
<b>History</b>	3.6.4070	First release
<b>Role</b>	admin	
<b>Example</b>	<pre>switch (config router bgp)# show ipv6 dhcp relay counters DHCP Counter flags: SPR: Server Packets Received, SPE: Server Packets Error SPRE: Server Packet Relayed, CPR: Client Packets Received RP: Relay Packets, RE: Relay Errors Instance: 1 VRF Name: vrf-default  Req/Resp      Received      Forwarded -----  -----  ----- All Req        0            0 All Res        0            0  If          SPRE      SPE      SPR      CPR -----  -----  -----  -----  ----- Packets Relayed to Server:  Server      RP      RE -----  -----  ----- 2001::1      0            0  Instance: 7 VRF Name: vrf-default  Req/Resp      Received      Forwarded -----  -----  ----- All Req        2            2 All Res        2            2  If          SPRE      SPE      SPR      CPR -----  -----  -----  -----  ----- vlan40       2            0            2            0 vlan50       2            0            0            2 Packets Relayed to Server:  Server      RP      RE -----  -----  ----- 2001::2      2            0  switch (config router bgp)# </pre>	

---

**Related Commands**

---

**Note**

---

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

## A.1 Overview

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



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

## A.2 Web Certificate

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 MLNX-OS User Manual.

**Step 2.** Show crypto certificate detail. Run:

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

Search for “signature algorithm” in the output.

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

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

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

**Step 1.** Define the default hash algorithm. Run:

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

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

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



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

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



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



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



Make sure not to confuse “signature algorithm” with “Thumbprint algorithm”.

### A.3 SNMP

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

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

```
switch (config) # snmp-server user <username> v3 auth sha <password1> priv aes-128
<password2>
```

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

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



To test strict mode, configure users and check them using the CLI, then run an SNMP request with the new users.

For more information please refer to the MLNX-OS User Manual.



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

### A.4 SSH

The SSH server on the switch by default uses secure and unsecure ciphers, message authentication code (MAC), key exchange methods, and public key algorithm. When configuring SSH

server to strict mode, the aforementioned security methods only use approved algorithms as detailed in the NIST 800-181A specification and the user can connect to the switch via SSH in strict mode only.

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

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



The 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.5 HTTPS

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

- RSA\_WITH\_AES\_128\_CBC\_SHA256
- RSA\_WITH\_AES\_256\_CBC\_SHA256
- DHE\_RSA\_WITH\_AES\_128\_CBC\_SHA256
- DHE\_RSA\_WITH\_AES\_256\_CBC\_SHA256
- TLS\_RSA\_WITH\_AES\_128\_GCM\_SHA256
- TLS\_RSA\_WITH\_AES\_256\_GCM\_SHA384
- TLS\_DHE\_RSA\_WITH\_AES\_128\_GCM\_SHA256
- TLS\_DHE\_RSA\_WITH\_AES\_256\_GCM\_SHA384

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

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

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

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

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

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

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

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

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

  Web file transfer proxy:
    Proxy enabled: no

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

```

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

- **To disable HTTP, run:**

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

## A.6 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: Show Commands Supported by JSON API

Table 62 lists the “show” commands which currently support JSON API.



The character “\*” indicates a wildcard.

**Table 62 - JSON API Show Commands**

802.1x Protocol
show dot1x
show dot1x interfaces ethernet
show dot1x interfaces ethernet *
show dot1x interfaces ethernet * statistics
Configuration Management
show configuration
show configuration audit
show configuration expanded
show configuration files *
show configuration files * expanded
show configuration running
show configuration text files
show files debug-dump
show files stats
show files system
show files system detail
show files tcpdump
show running-config
show running-config expanded
show running-config protocol *
Cryptographic (X.509, IPSec) and Encryption
show crypto encrypt-data
DHCP
show ip dhcp
show ipv6 dhcp
DHCP Relay
show ip dhcp relay counters instance *

**Table 62 - JSON API Show Commands**

<b>OpenFlow</b>
show openflow table * match-keys supported
show openflow tables
<b>Port Mirroring</b>
show monitor session summary
show monitor session *
<b>VRRP</b>
show vrrp
show vrrp detail
show vrrp detail interface vlan *
show vrrp detail interface vlan * vr *
show vrrp detail vr *
show vrrp interface vlan *
show vrrp interface vlan * vr *
show vrrp statistics
show vrrp statistics all
show vrrp statistics interface vlan *
show vrrp statistics interface vlan * vr *
show vrrp statistics vr *
show vrrp vr *
<b>VRF</b>
show ip arp vrf * count
show ip arp vrf * *
show ip interface vrf * brief
show ip interface vrf * ethernet *
show ip interface vrf * loopback *
show ip interface vrf * port-channel *
show ip interface vrf * vlan *
show routing-context vrf
show vrf
show vrf *
<b>VLAN</b>
show interfaces switchport
show vlan

**Table 62 - JSON API Show Commands**

show vlan id *
<b>User Management and Security</b>
show aaa authentication attempts
show aaa authentication attempts configured
show aaa authentication attempts status
show system secure-mode
show usernames
show users
show whoami
<b>Statistics and Alarms</b>
show stats alarm
show stats chd
show stats chd *
show stats cpu
show stats sample
show stats sample *
<b>Spanning Tree</b>
show spanning-tree detail
show spanning-tree interface ethernet *
show spanning-tree interface mlag-port-channel *
show spanning-tree interface port-channel *
show spanning-tree mst interface ethernet *
show spanning-tree mst interface port-channel *
show spanning-tree mst * interface ethernet *
show spanning-tree mst * interface port-channel *
show spanning-tree root
show spanning-tree vlan * detail
show spanning-tree vlan * interface ethernet *
show spanning-tree vlan * interface mlag-port-channel *
show spanning-tree vlan * interface port-channel *
<b>SNMP</b>
show snmp events
show snmp set-permission

**Table 62 - JSON API Show Commands**

QoS
show dcb ets interface ethernet *
show dcb ets interface mlag-port-channel *
show dcb ets interface port-channel *
show qos interface ethernet *
show qos interface mlag-port-channel *
show qos interface port-channel *
Priority Flow Control
show dcb priority-flow-control
show dcb priority-flow-control detail
show dcb priority-flow-control interface ethernet *
show dcb priority-flow-control interface ethernet * detail
show dcb priority-flow-control interface mlag-port-channel *
show dcb priority-flow-control interface mlag-port-channel * detail
show dcb priority-flow-control interface port-channel *
show dcb priority-flow-control interface port-channel * detail
MLAG
show mlag
show mlag statistics
show mlag-vip
MAC Address Table
show mac-address-table
show mac-address-table address *
show mac-address-table aging-time
show mac-address-table interface ethernet *
show mac-address-table multicast
show mac-address-table summary
show mac-address-table unicast
show mac-address-table vlan range *
show mac-address-table vlan *
MAGP
show magp
show magp interface vlan *
show magp *

**Table 62 - JSON API Show Commands**

LLDP
show dcb application-priority
show lldp interfaces
show lldp interfaces ethernet *
show lldp interfaces ethernet * med-cap
show lldp local
show lldp remote
show lldp statistics
show lldp statistics global
show lldp statistics interface ethernet *
show lldp timers
LAG
show lacp
show lacp interfaces ethernet *
show lacp interfaces mlag-port-channel * system-identifier
show lacp interfaces port-channel * system-identifier
Ethernet L3
show interfaces vlan
show interfaces vlan status
show interfaces vlan *
show ip arp interface
show ip arp interface ethernet
show ip arp interface ethernet *
show ip arp interface port-channel
show ip arp interface port-channel *
show ip arp interface vlan
show ip arp interface vlan *
show ip arp interface *
show ip arp *
show ip interface brief
show ip interface ethernet *
show ip interface loopback *
show ip interface port-channel *
show ip interface vlan *
show ip interface *

**Table 62 - JSON API Show Commands**

show ip load-sharing
show ip route summary
<b>Interface Isolation</b>
show isolation-group
show isolation-group *
<b>IP Interfaces</b>
show interfaces loopback
show interfaces loopback *
<b>Interface Ethernet (L2)</b>
show interfaces ethernet
show interfaces ethernet capabilities
show interfaces ethernet description
show interfaces ethernet rates
show interfaces ethernet rates GB
show interfaces ethernet rates KB
show interfaces ethernet rates MB
show interfaces ethernet status
show interfaces ethernet transceiver
show interfaces ethernet transceiver diagnostics
show interfaces ethernet transceiver raw
show interfaces ethernet *
show interfaces ethernet * capabilities
show interfaces ethernet * congestion-control
show interfaces ethernet * counters
show interfaces ethernet * counters pfc prio *
show interfaces ethernet * counters pg *
show interfaces ethernet * counters priority *
show interfaces ethernet * counters switch-priority *
show interfaces ethernet * counters tc *
show interfaces ethernet * description
show interfaces ethernet * status
show interfaces ethernet * transceiver
show interfaces ethernet * transceiver counters
show interfaces ethernet * transceiver counters details
show interfaces ethernet * transceiver diagnostics

**Table 62 - JSON API Show Commands**

show interfaces ethernet * transceiver raw
show interfaces mlag-port-channel
show interfaces mlag-port-channel summary
show interfaces mlag-port-channel *
show interfaces mlag-port-channel * congestion-control
show interfaces mlag-port-channel * counters
show interfaces mlag-port-channel * counters priority *
show interfaces mlag-port-channel * counters switch-priority *
show interfaces port-channel
show interfaces port-channel load-balance
show interfaces port-channel summary
show interfaces port-channel *
show interfaces port-channel * congestion-control
show interfaces port-channel * counters
show interfaces port-channel * counters priority *
show interfaces port-channel * counters switch-priority *
<b>IGMP</b>
show ip igmp groups
show ip igmp groups ethernet *
show ip igmp groups port-channel *
show ip igmp groups vlan *
show ip igmp groups *
show ip igmp interface
show ip igmp interface brief
show ip igmp interface ethernet *
show ip igmp interface ethernet * brief
show ip igmp interface port-channel *
show ip igmp interface port-channel * brief
show ip igmp interface vlan *
show ip igmp interface vlan * brief
show ip igmp snooping
show ip igmp snooping groups
show ip igmp snooping groups vlan *
show ip igmp snooping groups vlan * group *
show ip igmp snooping interfaces

**Table 62 - JSON API Show Commands**

show ip igmp snooping membership
show ip igmp snooping membership vlan *
show ip igmp snooping membership vlan * group *
show ip igmp snooping mrouter
show ip igmp snooping querier
show ip igmp snooping querier counters
show ip igmp snooping querier counters vlan *
show ip igmp snooping querier counters vlan * group *
show ip igmp snooping querier vlan *
show ip igmp snooping statistics
show ip igmp snooping vlan *
<b>Chassis Management</b>
show asic-version
show bios
show cpld
show fan
show inventory
show leds
show leds *
show memory
show module
show power
show power consumers
show protocols
show resources
show system capabilities
show system mac
show system profile
show system resource table
show system resource table *
show system type
show temperature
show version
show version concise
show voltage

**Table 62 - JSON API Show Commands**

Licenses
show licenses
Management Interface
show ip arp
show ip arp count
Network Management Interfaces
show json-gw
show xml-gw
User Interfaces
show banner
show ftp-server
show services small-servers
show telnet-server

## Appendix C: 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.

### C.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.

### C.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:

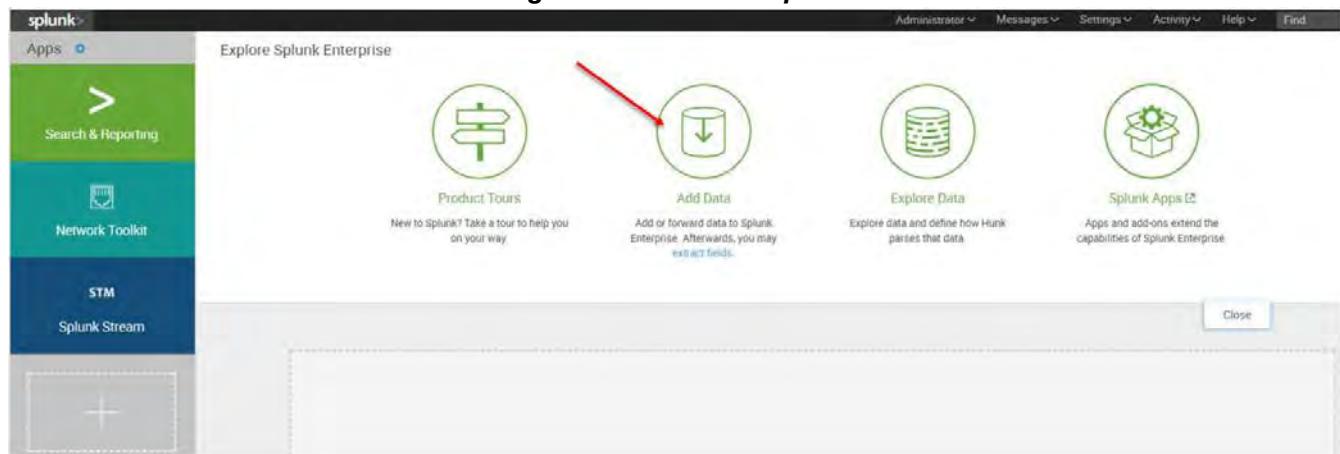
switch (config) # show running-config
## Logging configuration
##
  logging 10.212.23.1
  logging 10.212.23.1 port 8597
  logging 10.212.23.1 trap info
  logging 10.212.23.1 trap override class events priority err
  logging monitor events notice
  logging receive
## SNMP configuration
no snmp-server 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

```

### C.3 Adding a Task

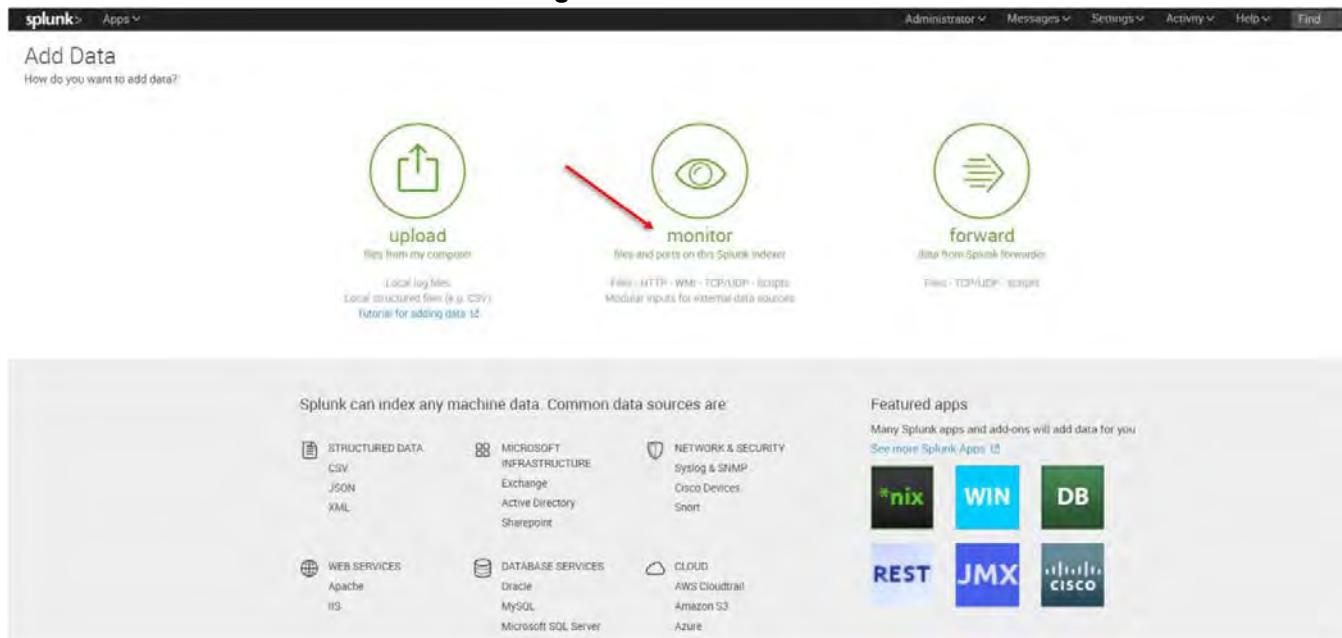
**Step 6.** The first screen encountered after signing into the Splunk WebUI includes the “Add Data” icon.

**Figure 41: 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 42: Monitor Icon**



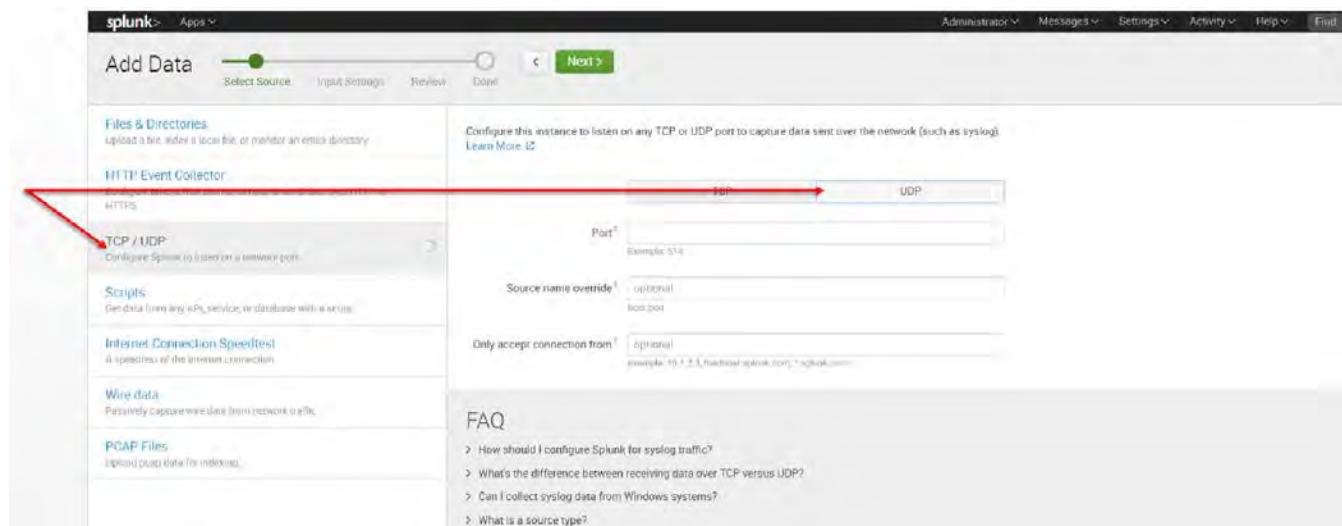
In the Monitor option, the following four categories are available:

- File & Directories: Monitor files/folders
- HTTP Event Collector: Monitor data streams over HTTP
- TCP/UDP: Monitor service ports
- Scripts: Monitor scripts

## C.4 Retrieving Data from TCP and UDP Ports

**Step 8.** Per our current purpose, we choose TCP/UDP option.

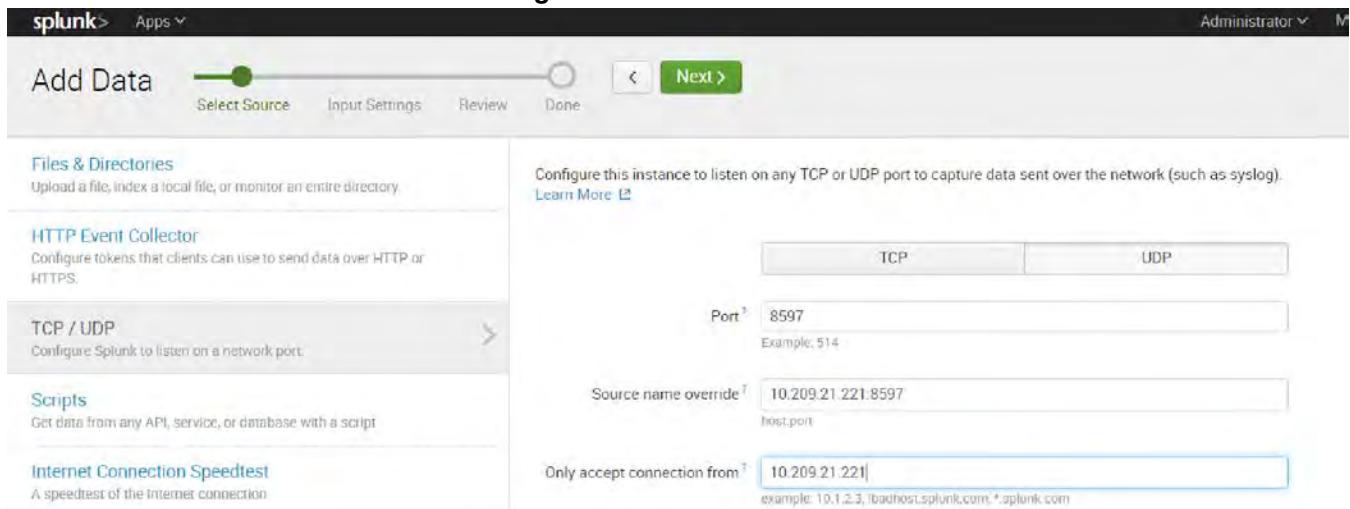
**Figure 43: TCP/UDP**



**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.

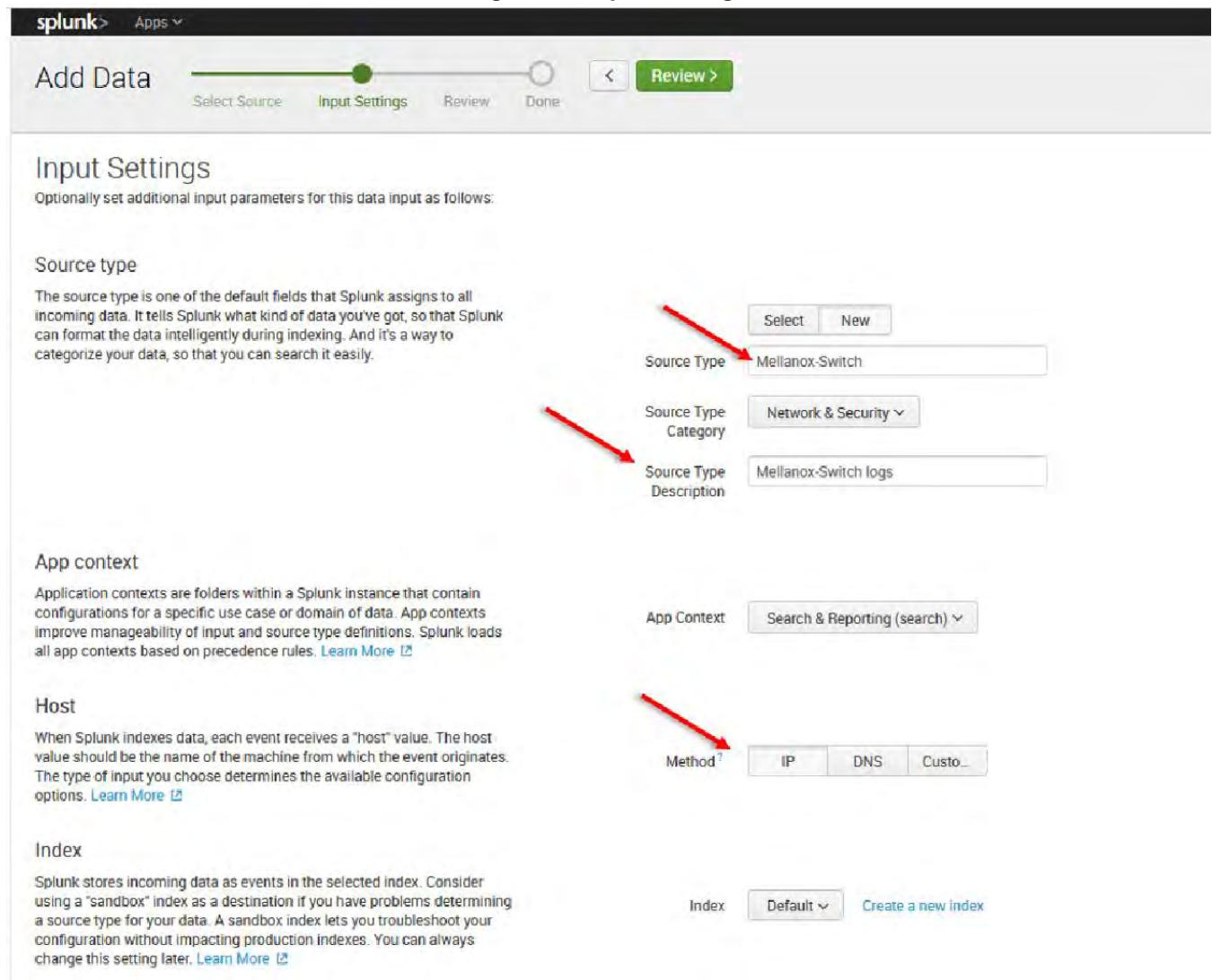
**Step 10.** In the “Source name override” field, enter a new source name to override the default source value, if required.

**Figure 44: 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 45: Input Settings**



The screenshot shows the 'Input Settings' page in Splunk. The top navigation bar includes 'splunk>' and 'Apps <'. Below it, a progress bar shows 'Add Data' with four steps: 'Select Source' (green dot), 'Input Settings' (yellow dot, currently active), 'Review' (grey dot), and 'Done' (grey dot). A green 'Review >' button is on the right. The main content area has a title 'Input Settings' and a sub-instruction: 'Optional set additional input parameters for this data input as follows:'.

**Source type**

The source type is one of the default fields that Splunk assigns to all incoming data. It tells Splunk what kind of data you've got, so that Splunk can format the data intelligently during indexing. And it's a way to categorize your data, so that you can search it easily.

Source Type:  (highlighted by a red arrow)

Source Type Category:

Source Type Description:

**App context**

Application contexts are folders within a Splunk instance that contain configurations for a specific use case or domain of data. App contexts improve manageability of input and source type definitions. Splunk loads all app contexts based on precedence rules. [Learn More](#)

App Context:

**Host**

When Splunk indexes data, each event receives a "host" value. The host value should be the name of the machine from which the event originates. The type of input you choose determines the available configuration options. [Learn More](#)

Method:  (highlighted by a red arrow)

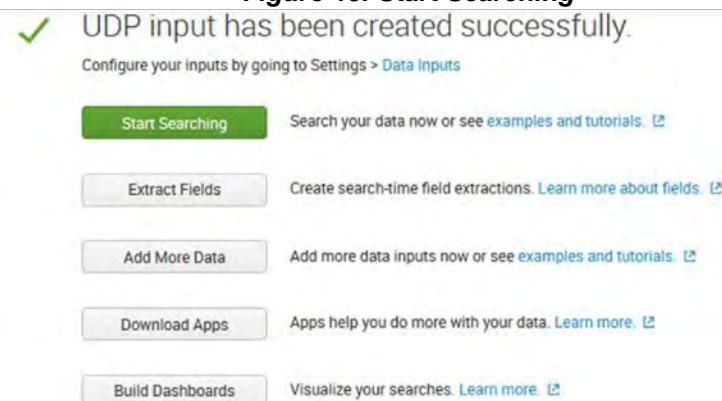
**Index**

Splunk stores incoming data as events in the selected index. Consider using a "sandbox" index as a destination if you have problems determining a source type for your data. A sandbox index lets you troubleshoot your configuration without impacting production indexes. You can always change this setting later. [Learn More](#)

Index:  [Create a new index](#)

**Step 12.** Click Next > Review > Done > Start Searching

**Figure 46: Start Searching**



## C.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.

### C.5.1 Getting Started

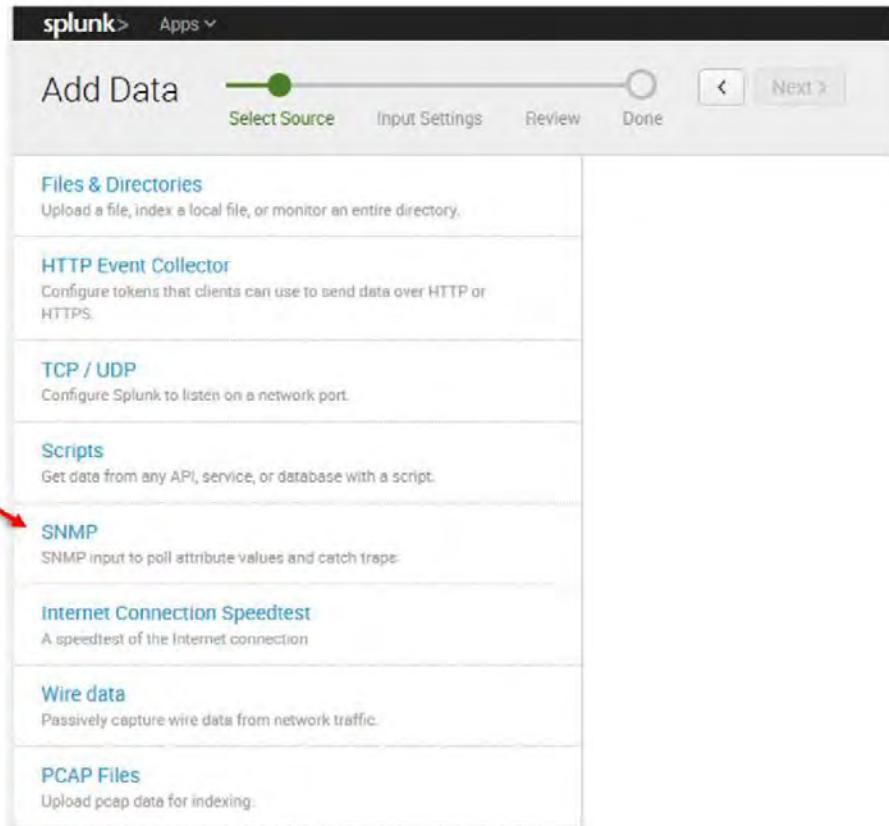
Browse to Splunkbase and download the SNMP Modular Input from <https://splunkbase.splunk.com/app/1537/>.

To install, simply untar the file to SPLUNK\_HOME/etc/apps and restart Splunk.

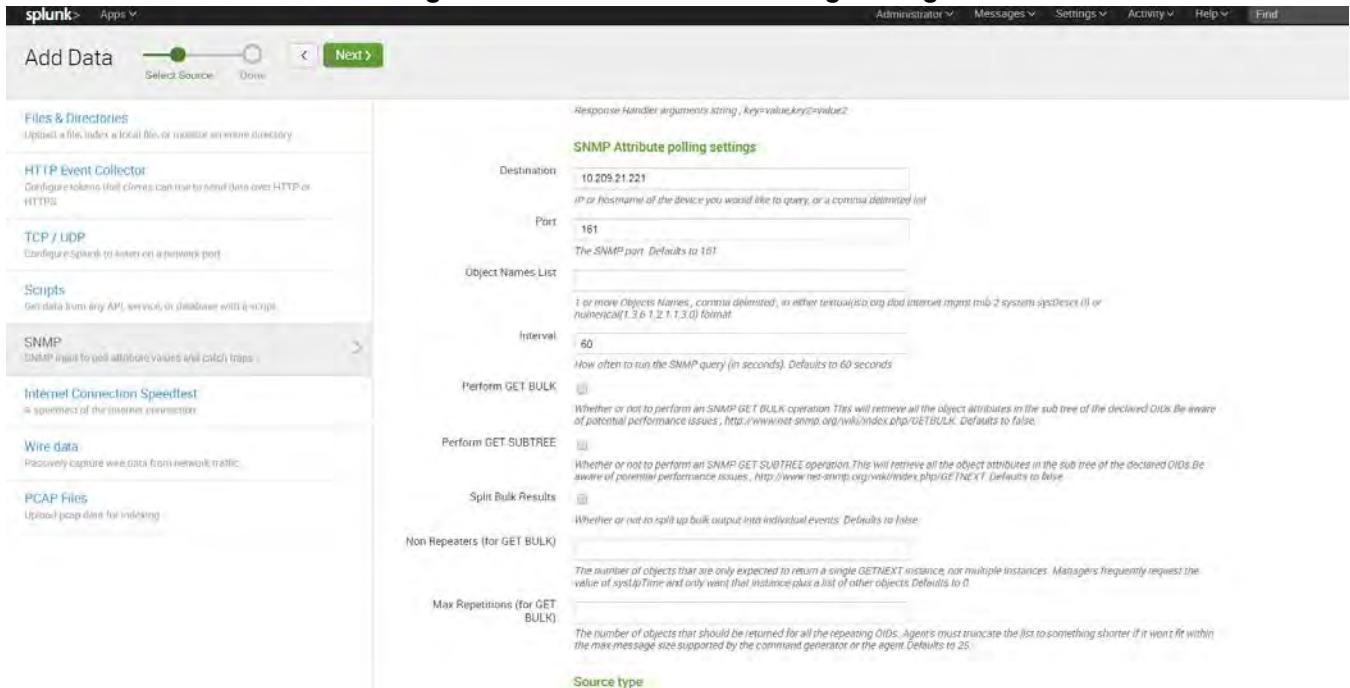
### C.5.2 Configuration

Login to the Splunk WebUI and go to Manager > Add Data > Monitor > SNMP > New, and set up your input data.

**Figure 47: SNMP**



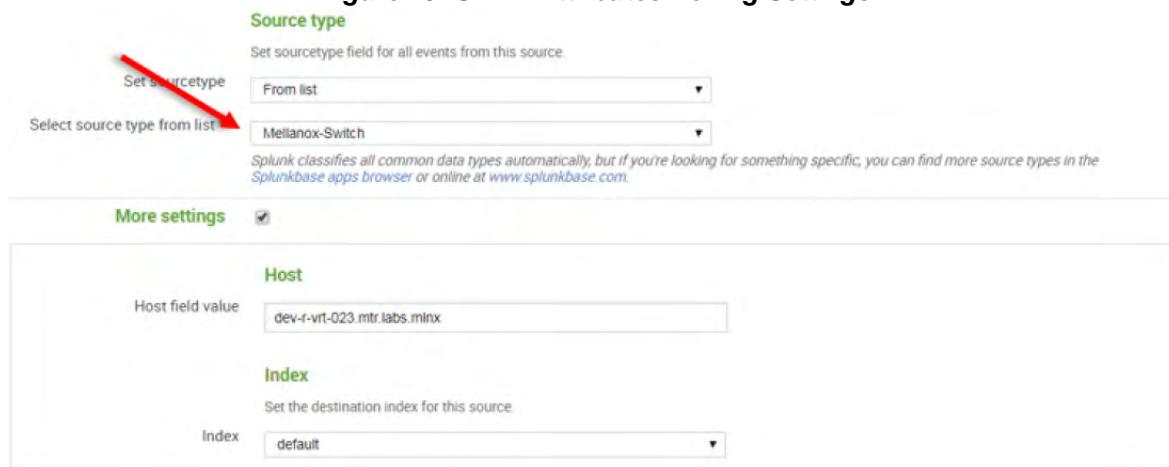
**Figure 48: SNMP Attributes Polling Settings**



The screenshot shows the 'Add Data' wizard in Splunk, specifically the 'Input Settings' step for the 'SNMP' source selected in Figure 47. The right pane contains the following configuration fields:

- Response Handler arguments:** string , key1=value,key2=value2
- SNMP Attribute polling settings:**
  - Destination:** 10.209.21.221 (IP or hostname of the device you would like to query, or a comma delimited list)
  - Port:** 161 (The SNMP port. Defaults to 161)
  - Object Names List:** 1 or more Object Names, comma delimited, in either textual (iso dot integer integer mib-2 system sysDescr 0) or numerical (1.3.6.1.2.1.1.3.0) format.
  - Interval:** 60 (How often to run the SNMP query (in seconds). Defaults to 60 seconds)
  - Perform GET BULK:** (checkbox) Whether or not to perform an SNMP GET BULK operation. This will retrieve all the object attributes in the sub tree of the declared OIDs. Be aware of potential performance issues. <http://www.net-snmp.org/wiki/index.php/GETBULK>. Defaults to false.
  - Perform GET-SUBTREE:** (checkbox) Whether or not to perform an SNMP GET-SUBTREE operation. This will retrieve all the object attributes in the sub tree of the declared OIDs. Be aware of potential performance issues. <http://www.net-snmp.org/wiki/index.php/GETSUBTREE>. Defaults to false.
  - Split Bulk Results:** (checkbox) Whether or not to split up bulk output into individual events. Defaults to false.
  - Non Repeaters (for GET BULK):** (text input) The number of objects that are only expected to return a single GETNEXT instance, not multiple instances. Managers frequently request the value of sysUpTime and only want that instance plus a list of other objects. Defaults to 0.
  - Max Repetitions (for GET BULK):** (text input) The number of objects that should be returned for all the repeating OIDs. Agents must truncate the list to something shorter if it won't fit within the max message size supported by the command generator or the agent. Defaults to 25.
- Source type:** (dropdown menu)

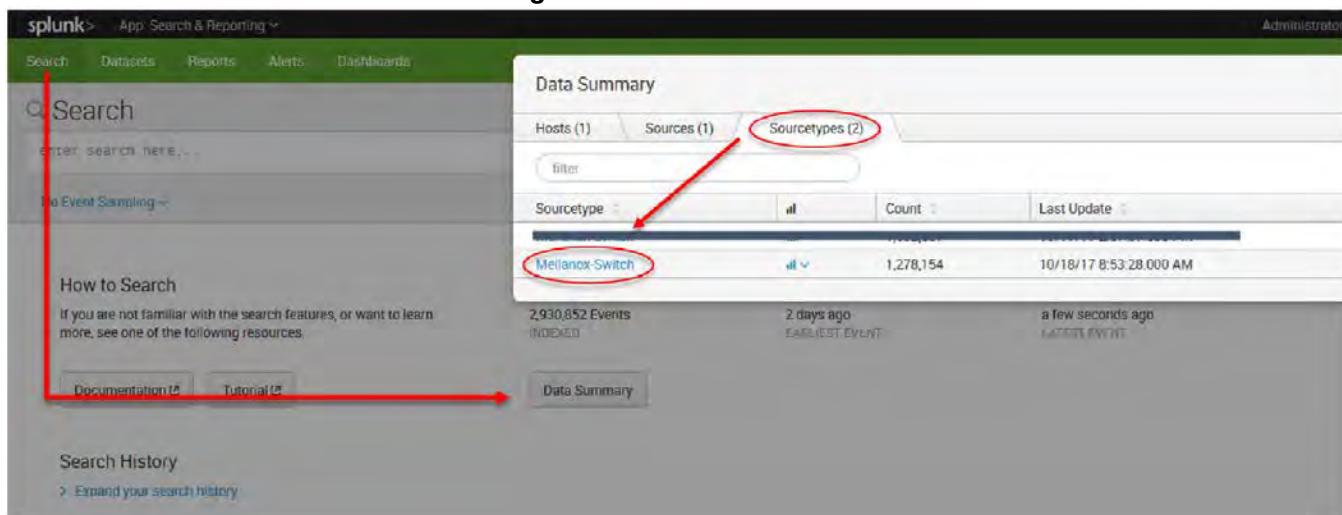
**Figure 49: SNMP Attributes Polling Settings**



The screenshot shows the 'Source type' configuration page in Splunk. It includes fields for setting sourcetype (From list: Mellanox-Switch), host field value (dev-r-vrt-023.mtr.labs.mlnx), and index (default). A red arrow points from the text 'Select source type from list' to the 'From list' dropdown.

**Step 13.** After configuration is complete it is recommend to run Mellanox-Switch again:  
Search > Data Summary > Sourcetypes > Mellanox-Switch.

**Figure 50: Mellanox-Switch**

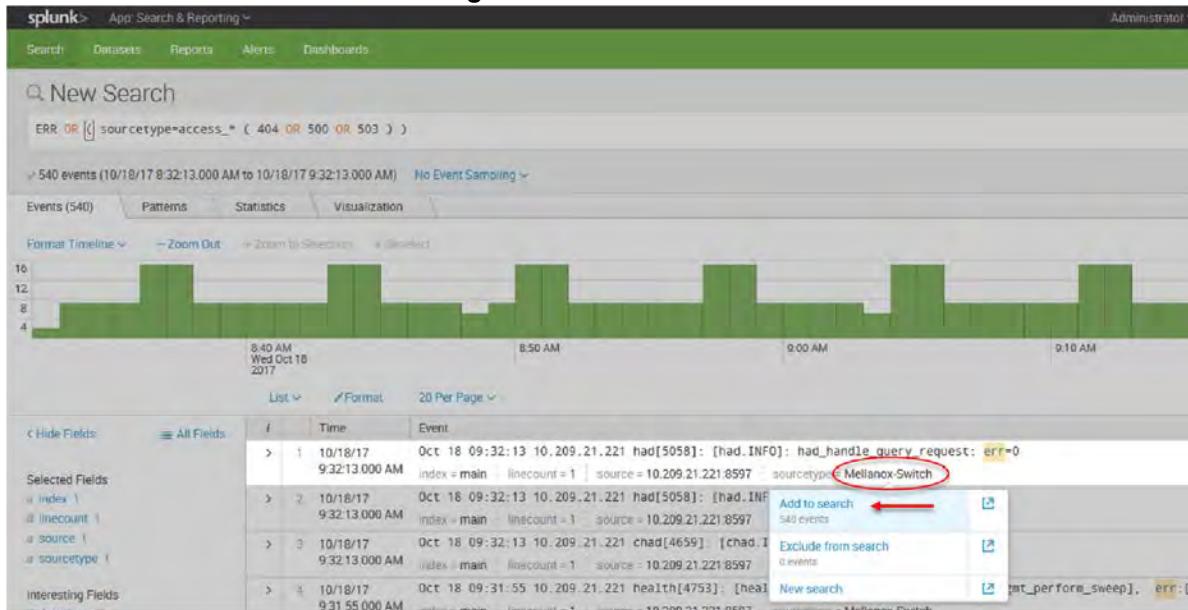


The screenshot shows the Splunk search interface with a red arrow pointing to the 'Search' bar. On the right, the 'Data Summary' page is displayed, showing a table with one host, one source, and two sourcetypes. The sourcetype 'Mellanox-Switch' is highlighted with a red circle. Another red circle highlights the 'Sourcetypes (2)' tab. A red arrow points from the 'Documentation' and 'Tutorial' buttons at the bottom left to the 'Data Summary' button at the bottom right.

Sourcetype	Count	Last Update
Mellanox-Switch	1,278,154	10/18/17 8:53:28.000 AM

**Step 14.** Select “Mellanox-Switch” and “Add to search”.

**Figure 51: Add to Search**



**Step 15.** You can add to search any value that is relevant for you.

**Figure 52: Search Options**

