Mellanox MLNX-OS® User Manual for Ethernet

Rev 4.60
Software Version 3.6.3508
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.
# Table of Contents

Document Revision History .................................................. 5  
About this Manual ......................................................... 26  
Chapter 1 Introduction ..................................................... 30  
  1.1 System Features .................................................. 30  
  1.2 Ethernet Features ................................................. 31  
Chapter 2 Getting Started .................................................. 33  
  2.1 Configuring the Switch for the First Time ..................... 33  
    2.1.1 Re-Running the Wizard ................................... 39  
  2.2 Starting the Command Line (CLI) ................................. 39  
  2.3 Starting the Web User Interface (WebUI) ...................... 40  
  2.4 Licenses .......................................................... 44  
    2.4.1 Installing MLNX-OS® License (CLI) ...................... 44  
    2.4.2 Installing MLNX-OS License (Web) ...................... 45  
    2.4.3 Retrieving a Lost License Key .......................... 47  
    2.4.4 Commands .................................................. 48  
Chapter 3 User Interfaces .................................................... 53  
  3.1 Command Line Interface Overview ............................... 53  
    3.1.1 CLI Modes ................................................ 53  
    3.1.2 Syntax Conventions ...................................... 54  
    3.1.3 Getting Help ............................................... 54  
    3.1.4 Prompt and Response Conventions ...................... 55  
    3.1.5 Using the “no” Form ...................................... 56  
    3.1.6 Parameter Key ............................................. 57  
    3.1.7 CLI Pipeline Operator Commands ....................... 58  
      3.1.7.1 “include” and “exclude” CLI Filtration Options . 58  
      3.1.7.2 “watch” CLI Monitoring Option .................... 59  
      3.1.7.3 “json-print” CLI Option ............................ 60  
    3.1.8 CLI Shortcuts ............................................... 61  
  3.2 Web Interface Overview .......................................... 62  
    3.2.1 Setup Menu ............................................... 63  
    3.2.2 System Menu ............................................... 64  
    3.2.3 Security Menu ............................................. 65  
    3.2.4 Ports Menu ................................................ 65  
    3.2.5 Status Menu ............................................... 66  
    3.2.6 ETH Mgmt .................................................. 67  
    3.2.7 IP Route ................................................... 67
4.3.7 Commands ........................................... 215
4.4 Configuration Management .................................. 228
  4.4.1 Saving a Configuration File ............................. 228
  4.4.2 Loading a Configuration File ............................ 228
  4.4.3 Restoring Factory Default Configuration ................... 228
  4.4.4 Managing Configuration Files ........................... 229
    4.4.4.1 BIN Configuration Files ............................ 229
    4.4.4.2 Text Configuration Files .......................... 230
  4.4.5 Commands ............................................ 231
    4.4.5.1 File System ........................................ 231
    4.4.5.2 Configuration Files .................................. 241
4.5 Logging .................................................. 262
  4.5.1 Monitor .............................................. 262
  4.5.2 Remote Logging ........................................ 262
  4.5.3 Commands ............................................ 263
4.6 Debugging .................................................. 286
  4.6.1 Commands ............................................ 287
4.7 Event Notifications ........................................... 307
  4.7.1 Supported Events ....................................... 307
  4.7.2 Terminal Notifications .................................. 308
  4.7.3 Email Notifications .................................... 309
  4.7.4 Commands ............................................ 311
    4.7.4.1 Email Notification ................................... 311
4.8 Telemetry .................................................. 330
  4.8.1 Commands ............................................ 330
4.9 User Management and Security ................................ 346
  4.9.1 User Accounts ......................................... 346
  4.9.2 Authentication, Authorization and Accounting (AAA) ....... 346
    4.9.2.1 User Re-authentication ............................... 347
    4.9.2.2 RADIUS ........................................... 347
    4.9.2.3 TACACS+ ........................................ 347
    4.9.2.4 LDAP ............................................ 347
  4.9.3 System Secure Mode ..................................... 348
  4.9.4 Commands ............................................ 350
    4.9.4.1 User Accounts ....................................... 350
    4.9.4.2 AAA Methods ........................................ 355
    4.9.4.3 RADIUS ........................................... 370
    4.9.4.4 TACACS+ ........................................ 374
    4.9.4.5 LDAP ............................................ 378
    4.9.4.6 System Secure Mode ................................ 396
4.10 Cryptographic (X.509, IPSec) and Encryption ...................... 398
  4.10.1 System File Encryption ................................ 398
4.15.5.2 VLAN Capabilities ........................................ 533
4.15.5.3 Layer 2 Ethernet Interface Capabilities ................. 533
4.15.5.4 LAG (Port-Channel) Capabilities ........................ 534
4.15.5.5 Layer 3 Interface Capabilities ............................ 534
4.15.5.6 OSPF Interface Capabilities .............................. 534
4.15.5.7 OSPF Area Capabilities ................................. 536
4.15.5.8 Router OSPF Capabilities .............................. 536
4.15.5.9 Protocol LLDP, SNMP, IP Routing and Spanning Tree Capabilities ................................. 536
4.15.5.10 Fetched Image Capabilities ............................... 536
4.15.5.11 Installed Image Capabilities ............................ 537
4.15.6 Supported Resources for Each Type ......................... 537
4.15.7 Troubleshooting ............................................ 539
  4.15.7.1 Switch and Server Clocks are not Synchronized ....... 539
  4.15.7.2 Outdated or Invalid SSL Certificates Either on the Switch or the Server .......................... 539
  4.15.7.3 Communications Issue .................................. 539
4.15.8 Commands .................................................. 540
4.16 Virtual Machine .............................................. 547
  4.16.1 Virtual Machine Configuration ............................. 547
4.16.2 Commands .................................................. 550
  4.16.2.1 Config .................................................. 550
  4.16.2.2 Show .................................................. 565
4.17 IP Table Filtering .............................................. 573
  4.17.1 Configuring IP Table Filtering ............................... 573
  4.17.2 Modifying IP Table Filtering .............................. 575
4.17.3 Rate-limit Rule Configuration ............................... 575
  4.17.4 Commands .................................................. 576
4.18 Resource Scale .................................................. 582
  4.18.1 Ethernet Resources .......................................... 582
    4.18.1.1 Strict Mode ........................................ 582
    4.18.1.2 Loose Mode – SwitchX® ............................. 583
    4.18.1.3 Loose Mode – Spectrum™ ............................. 583
  4.18.2 Commands .................................................. 584

Chapter 5 Ethernet Switching ........................................ 587

  5.1 Interface ...................................................... 587
    5.1.1 Break-Out Cables ......................................... 587
      5.1.1.1 Changing the Module Type to a Split Mode ........ 588
      5.1.1.2 Unsplitting a Split Port ................................ 589
    5.1.2 56GbE Link Speed ......................................... 589
    5.1.3 Transceiver Information .................................. 590
    5.1.4 High Power Transceivers .................................. 591
    5.1.5 Forward Error Correction .................................. 592
    5.1.6 Commands .................................................. 592
5.2 Interface Isolation ........................................... 618
  5.2.1 Configuring Isolated Interfaces ......................... 618
  5.2.2 Commands ............................................. 619
5.3 Link Aggregation Group (LAG) ................................ 626
  5.3.1 Configuring Static Link Aggregation Group (LAG) ....... 626
  5.3.2 Configuring Link Aggregation Control Protocol (LACP) ... 626
  5.3.3 Commands ............................................. 627
5.4 MLAG ...................................................... 647
  5.4.1 MLAG Keepalive and Failover ............................ 649
  5.4.2 Unicast and Multicast Sync ............................. 649
  5.4.3 MLAG Port Sync ....................................... 649
  5.4.4 MLAG Virtual System-MAC ............................. 650
  5.4.5 Upgrading MLAG Pair .................................. 650
  5.4.6 Configuring MLAG ..................................... 650
  5.4.7 Commands ............................................. 654
5.5 VLANs ...................................................... 673
  5.5.1 Configuring Access Mode and Assigning Port VLAN ID (PVID) ... 673
  5.5.2 Configuring Hybrid Mode and Assigning Port VLAN ID (PVID) ... 674
  5.5.3 Configuring Trunk Mode VLAN Membership ................ 674
  5.5.4 Configuring Hybrid Mode VLAN Membership .............. 675
  5.5.5 Commands ............................................. 676
5.6 Voice VLAN .................................................. 687
  5.6.1 Configuring Voice VLAN ................................ 688
  5.6.2 Limitations ............................................ 691
5.7 QinQ ....................................................... 692
  5.7.1 QinQ Operation Modes ................................ 692
  5.7.2 Configuring QinQ ..................................... 692
  5.7.3 Commands ............................................. 694
5.8 MAC Address Table .......................................... 696
  5.8.1 Configuring Unicast Static MAC Address .................. 696
  5.8.2 MAC Learning Considerations ........................... 696
  5.8.3 Commands ............................................. 697
5.9 Spanning Tree ............................................... 704
  5.9.1 Port Priority and Cost .................................. 704
  5.9.2 Port Type ............................................. 704
  5.9.3 BPDU Filter ........................................... 705
  5.9.4 BPDU Guard ........................................... 705
  5.9.5 Loop Guard ........................................... 705
  5.9.6 Root Guard ........................................... 706
  5.9.7 MSTP .................................................. 706
  5.9.8 RPVST ............................................... 706
  5.9.8.1 RPVST and VLAN Limitations ....................... 707
5.9.8.2 RPVST and RSTP Interoperability ................................. 708
5.9.9 Commands ............................................................. 708

5.10 OpenFlow ............................................................. 739
5.10.1 Flow Table ............................................................ 739
5.10.2 OpenFlow 1.3 Support ................................................ 740
  5.10.2.1 ACL Rule Tables (0-249) .................................... 741
  5.10.2.2 FDB Table (250) .............................................. 744
  5.10.2.3 Router Table (251) ........................................... 745
5.10.3 Configuring OpenFlow ............................................. 745
5.10.4 Configuring Secure Connection to OpenFlow ..................... 746
5.10.5 Commands ............................................................ 749

5.11 Network Virtualization Edge .......................................... 769
5.11.1 Configuring VTEP .................................................... 769
5.11.2 VMware Network Virtualization and Security Platform (NSX) Configuration 770
  5.11.2.1 Hardware Topology ........................................... 770
  5.11.2.2 Switch Configuration ....................................... 771
5.11.3 NSX Manager Configuration ....................................... 773
  5.11.3.1 Adding Hosts to Replication Cluster ........................ 773
  5.11.3.2 Adding the Mellanox Switch to NSX ....................... 774
5.11.4 Mapping a Logical Switch to a Physical Switch Port ............ 774
5.11.5 Commands ............................................................ 776

5.12 IGMP Snooping ......................................................... 793
5.12.1 Configuring IGMP Snooping ....................................... 793
5.12.2 Defining a Multicast Router Port on a VLAN ..................... 793
5.12.3 IGMP Snooping Querier ............................................ 795
5.12.4 Commands ............................................................ 796

5.13 Link Layer Discovery Protocol (LLDP) .............................. 816
5.13.1 Configuring LLDP .................................................... 816
5.13.2 DCBX ................................................................. 817
5.13.3 Commands ............................................................ 817

5.14 Quality of Service (QoS) ............................................... 833
5.14.1 QoS Classification .................................................. 833
  5.14.1.1 Trust Levels .................................................. 833
  5.14.1.2 Switch Priority to IEEE Priority Mapping ................. 834
  5.14.1.3 Default QoS Configuration .................................. 834
5.14.2 QoS Rewrite .......................................................... 835
  5.14.2.1 Switch-priority to PCP,DEI Re-marking Mapping .......... 835
  5.14.2.2 Switch-priority to DSCP Re-marking Mapping .......... 835
  5.14.2.3 DSCP to Switch-priority in Router ....................... 835
  5.14.2.4 Default Configuration ..................................... 835
5.14.3 Queuing and Scheduling (ETS) for SwitchX ....................... 836
5.14.4 Queuing and Scheduling (ETS) for Spectrum .................... 837
Chapter 6 IP Routing

6.1 General
6.1.1 IP Interfaces
6.1.2 Equal Cost Multi-Path Routing (ECMP)
6.1.3 Virtual Routing and Forwarding
6.1.4 Commands

6.2 OSPF
6.2.1 Router ID
6.2.2 ECMP
6.2.3 Configuring OSPF
6.2.4 Verifying OSPF
6.2.5 Commands
List of Figures

Figure 1: Managing an Ethernet Fabric Using MLNX-OS .............................................. 32
Figure 2: Console Ports SX10xx Systems ................................................................. 33
Figure 3: MLNX-OS Login Window ............................................................................... 41
Figure 4: EULA Prompt ................................................................................................. 42
Figure 5: Welcome Popup ......................................................................................... 43
Figure 6: Display After Login .................................................................................. 43
Figure 7: No Licenses Installed .............................................................................. 45
Figure 8: Enter License Key(s) in Text Box .............................................................. 46
Figure 9: Installed License ....................................................................................... 46
Figure 10: WebUI ....................................................................................................... 63
Figure 11: Index Scheme ......................................................................................... 69
Figure 12: JSON API WebUI Example ..................................................................... 504
Figure 13: Accepting an Agent Request through the Console ................................. 530
Figure 14: Break-Out Cable ..................................................................................... 587
Figure 15: Interface Isolation Example ...................................................................... 618
Figure 16: Basic MLAG Setup .................................................................................. 647
Figure 17: Basic MLAG Topology .......................................................................... 650
Figure 18: Tagging Voice Packets with a Different VLAN ID .................................. 687
Figure 19: MAC Learning Disable Example Case .................................................... 696
Figure 20: RPVST Network Config ......................................................................... 707
Figure 21: RPVST and RSTP Cluster ...................................................................... 708
Figure 22: MLNX-OS and OpenFlow Pipeline ......................................................... 740
Figure 23: RED/ECN Drop Profiles ....................................................................... 839
Figure 24: Overview of Mirroring Functionality ....................................................... 887
Figure 25: Mirror to Analyzer Mapping .................................................................... 887
Figure 26: Header Format Options .......................................................................... 890
Figure 27: Mirroring Session ................................................................................... 891
Figure 28: sFlow Functionality Overview ............................................................... 904
Figure 29: RoCEv2 and RoCE Frame Format Differences ......................................... 920
Figure 30: RoCEv2 Protocol Stack ......................................................................... 921
Figure 31: Xon/Xoff Configuration ........................................................................ 944
Figure 32: ECMP ...................................................................................................... 971
Figure 33: Multiple Hash Functions ....................................................................... 972
Figure 34: OSPF Basic Topology .......................................................................... 1016
Figure 35: Basic BGP Configuration ......................................................... 1058
Figure 36: Common VRRP Configuration with Load Balancing ............... 1202
Figure 37: NEO GUI ................................................................. 1245
Figure 38: NEO Jobs ................................................................. 1247
Figure 39: Fabric Dashboard .......................................................... 1249
Figure 40: 24-Hour View ............................................................. 1249
Figure 41: Device Heatmap ............................................................ 1250
Figure 42: Device Heatmap Dialog .................................................. 1250
Figure 43: Device Heatmap Dialog Example ....................................... 1251
Figure 44: Device Heatmap Example ................................................ 1251
Figure 45: Device Heatmap Key ......................................................... 1251
Figure 46: NEO Fabric Utilization Display ......................................... 1252
Figure 47: Fabric Utilization of Device per Category .............................. 1252
Figure 48: Top Alerted Devices ......................................................... 1253
Figure 49: Recent Activity Examples ............................................... 1253
List of Tables

Table 1: Reference Documents ................................................................. 15
Table 2: Glossary .................................................................................. 15
Table 3: General System Features ............................................................. 18
Table 4: Ethernet Features .................................................................... 19
Table 5: Configuration Wizard Session - IP Configuration by DHCP .......... 22
Table 6: Configuration Wizard Session - IP Zeroconf Configuration .......... 24
Table 7: Configuration Wizard Session - Static IP Configuration .............. 25
Table 8: LED Behavior Details ................................................................. 40
Table 9: CLI Modes and Config Context .................................................. 40
Table 10: Syntax Conventions ................................................................. 41
Table 11: Angled Brackets Parameter Description .................................... 45
Table 12: CLI Keyboard Shortcuts ............................................................ 49
Table 13: WebUI Setup Submenus ............................................................ 51
Table 14: WebUI System Submenus .......................................................... 52
Table 15: WebUI Security Submenus ......................................................... 53
Table 16: WebUI Ports Submenus ............................................................. 53
Table 17: WebUI Status Submenus ........................................................... 54
Table 18: WebUI ETH Mgmt Submenus .................................................... 55
Table 19: WebUI IP Route Submenus ....................................................... 55
Table 20: Module Type .......................................................................... 57
Table 21: Device Type ............................................................................. 57
Table 22: Sensor Type ............................................................................ 58
Table 23: Supported Event Notifications and MIB Mapping ..................... 294
Table 24: User Roles (Accounts) and Default Passwords ......................... 333
Table 25: Chassis Manager Information .................................................. 434
Table 26: System Health Monitor Alerts Scenarios ................................... 435
Table 27: LWR Configuration Behavior .................................................. 442
Table 28: Standard MIBs – Textual Conventions and Conformance MIBs .... 475
Table 29: Standard MIBs – Chassis and Switch ....................................... 475
Table 30: Private MIBs Supported ............................................................. 476
Table 31: SNMP Traps .......................................................................... 476
Table 32: Supported SET OIDs ............................................................... 481
Document Revision History

Rev 4.60 – January 31, 2017

Added:

- Section 5.11.2, “VMware Network Virtualization and Security Platform (NSX) Configuration,” on page 770
- the command “protocol nve” on page 776
- the command “interface nve” on page 777
- the command “shutdown” on page 778
- the command “vxlan source interface loopback” on page 779
- the command “nve mode only” on page 780
- the command “clear nve counters” on page 781
- the command “show interfaces nve” on page 782
- the command “show interfaces nve counters” on page 783
- the command “show interfaces nve flood” on page 784
- the command “show interfaces nve mac-address-table” on page 785
- the command “show interfaces nve mac-address-table local learned unicast” on page 786
- the command “show interfaces nve mac-address-table remote configured multicast” on page 787
- the command “show interfaces nve mac-address-table remote configured unicast” on page 788
- the command “show interfaces nve peers” on page 789
- the command “ovs ovsdb server” on page 790
- the command “ovs ovsdb manager remote” on page 791
- the command “ovs ovsdb server listen” on page 792
- Section 3.1.7.3, “json-print” CLI Option,” on page 70
- Section 4.14.2, “JSON API,” on page 499
- Section 4.14.4.3, “JSON API Commands,” on page 527
- Section 4.8, “Telemetry,” on page 330 (Including subsections)
- the command “neighbor no-password” on page 1087
- the command “neighbor no-route-map” on page 1093
- the command “neighbor no-update-source” on page 1100
- the command “show snmp set-permission” on page 524
- the command “snmp-server enable set-permission” on page 512
• the command “show openflow groups” on page 763
• the command “show openflow meters” on page 764
• the command “show openflow flows table” on page 765
• the command “show openflow flows cookie” on page 766
• the command “show openflow table match-keys” on page 767
• the command “show openflow table match-keys supported” on page 768
• the command “show interfaces ethernet counters tc” on page 848
• the command “show interfaces ethernet counters pg” on page 849
• the command “show interfaces ethernet counters pfc prio” on page 850
• the command “show ip igmp snooping membership” on page 810
• the command “show lldp remote” on page 828
• the command “ip dhcp relay” on page 1225
• the command “ip dhcp relay instance” on page 1232
• the command “vrf” on page 1229
• the command “port” on page 1230
• the command “vrf-auto-helper” on page 1231
• Section 5.11, “OVS VTEP,” on page 751
• Appendix C, “Show Commands Supported by JSON API,” on page 1254

Updated:

• the command “redistribute” on page 1026
• the command “show ip ospf request-list” on page 1055
• the command “show ip ospf retransmission-list” on page 1056
• the command “show ip ospf summary-address” on page 1057
• the command “system resource table” on page 584
• the command “show system resource table” on page 585
• the command “bestpath as-path multipath-relax” on page 1066
• the command “bgp listen range peer-group” on page 1069
• the command “cluster-id” on page 1070
• the command “graceful-restart helper” on page 1074
• the command “neighbor advertisement-interval” on page 1076
• the command “neighbor allowas-in” on page 1077
• the command “neighbor ebgp-multihop” on page 1079
• the command “neighbor export-localpref” on page 1080
• the command “neighbor import-localpref” on page 1081
• the command “neighbor local-as” on page 1082
• the command “neighbor maximum-prefix” on page 1083
• the command “neighbor next-hop-peer” on page 1084
• the command “neighbor peer-group” on page 1088
• the command “neighbor route-reflector-client” on page 1094
• the command “neighbor send-community” on page 1095
• the command “neighbor timers” on page 1097
• the command “neighbor transport connection-mode passive” on page 1098
• the command “router-id” on page 1104
• the command “match as-path” on page 1126
• the command “set community-list” on page 1140
• the command “hostname” on page 159
• the command “image options” on page 225 “serve all” parameter description
• Note in Section 4.3.4, “Downgrading MLNX-OS Software,” on page 209
• Section 4.4.4.2, “Text Configuration Files,” on page 230
• the command “show running-config” on page 260
• Section 4.14.3, “XML API,” on page 504
• Section 4.18, “Resource Scale,” on page 582
• the command “fec-override” on page 680
• Section 5.10.2, “OpenFlow 1.3 Support,” on page 740
• the command “ip igmp snooping static-group” on page 802
• the command “ip igmp snooping version” on page 804
• the command “openflow mode hybrid” on page 751
• the command “show ip igmp snooping groups” on page 808
• the command “show ip igmp snooping querier” on page 812
• the command “show ip igmp snooping statistics” on page 814
• the command “show sflow” on page 919
• Section 6.3.4, “Commands,” on page 1061 under BGP
• Section 6.4, “Policy Rules,” on page 1119
• the command “address” on page 1226
• the command “always-on” on page 1227
• the command “information option” on page 1228
• the command “clear ip dhcp relay counters” on page 1233
• the command “show ip dhcp relay” on page 1235
• the command “show ip dhcp relay counters” on page 1235
• the command “clear ip bgp” on page 1062
• the command “logging port” on page 263
• the command “logging trap” on page 282
• the command “show logging” on page 283
• the command “show log” on page 284

Rev 4.50 – September 30, 2016

Added:
• Section 3.1.7.2, “watch” CLI Monitoring Option,” on page 59
• the command “ntp server trusted-enable” on page 197
• 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 4.4.4.1, “BIN Configuration Files,” on page 229
• Section 4.4.4.2, “Text Configuration Files,” on page 230
• the command “reset factory” on page 245
• the command “show running-config” on page 260
• Section 4.5.2, “Remote Logging,” on page 262 with Step 3
• the command “username” on page 350
• Section 4.13.5, “Unit Identification LED,” on page 468
• the command “led uid” on page 471
• the command “show leds” on page 471
• 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


Added:
• Section 4.3.4.3, “Switching to Partition with Older Software Version,” on page 211 for clarity
• Section 4.4.4.1, “BIN Configuration Files,” on page 229
• 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

**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
Rev 4.20 – August 16, 2015

Added:

- Section 4.3.6, “Image Maintenance via Mellanox ONIE,” on page 222
- Section 4.9.3, “System Secure Mode,” on page 357
- the command “system secure-mode enable” on page 405
- the command “show system secure-mode” on page 406
- the command “switchport dot1q-tunnel qos-mode” on page 760
- Section 5.7, “QinQ,” on page 771
- the command “dot1x host-mode” on page 1007
- the command “show ip route” on page 1091
- the command “vlan-pop” on page 960
- the command “vlan-push” on page 961

Updated:

- Table 7, “Configuration Wizard Session - IP Configuration by DHCP,” on page 45
- Section 2.4, “Licenses,” on page 54
- the command “ssh server host-key” on page 103
- notes of the command “aaa authorization” on page 375
- Table 28, “System Health Monitor Alerts Scenarios,” on page 457
- the command “show module” on page 482
- the command “snmp-server user” on page 529
- Section 5.1.2, “56GbE Link Speed,” on page 666
- the command “switchport mode” on page 758
- the command “ip ospf authentication-key” on page 1133
- the command “neighbor password” on page 1175
- the command “neighbor peer-group” on page 1177


Added:

- Section 2.1, “Configuring the Switch for the First Time,” on page 43 with MLNX-OS® Boot Menu step
- the command “ssh server security strict” on page 110
- the command “ssh server tcp-forwarding enable” on page 111
• Section 4.1.5, “In-Band Management,” on page 141
  This feature can now be enabled with IP Routing. Also updated the flow of setting an in-band management channel.
• the command “show module” on page 482
• Section 5.1.1, “Break-Out Cables,” on page 664
• the command “ip address dhcp” on page 679
• the command “ip address dhcp” on page 713
• Section 5.4.4, “MLAG Virtual System-MAC,” on page 729
• Section 5.4.5, “Upgrading MLAG Pair,” on page 729
• Section 5.19, “802.1x Protocol,” on page 1001
• Section 5.1.3, “Virtual Routing and Forwarding,” on page 1062
• the command “ip l3” on page 1063
• the command “vrf definition” on page 1064
• the command “routing-context vrf” on page 1065
• the command “description” on page 1067
• the command “rd” on page 1068
• the command “vrf forwarding” on page 1069
• the command “show routing-context vrf” on page 1071
• the command “show vrf” on page 1072
• the command “ip address dhcp” on page 1077
• Section 6.2, “IPv6,” on page 990 commands by adding loopback interface configuration mode to the commands
• Section 6.5.2, “PIM Load-Sharing,” on page 1243
• the command “ip pim multipath rp” on page 1261

Updated:
• the command “tcpdump” on page 193
• Section 4.3.1, “Upgrading MLNX-OS Software,” on page 213 with HA group note
• Section 4.3.2, “Upgrading MLNX-OS HA Groups,” on page 216
• the command “show inventory” on page 479
• the command “show asic-version” on page 474
• Section 5.4.1, “MLAG Keepalive and Failover,” on page 728
• Step 10 in Section 5.4.6, “Configuring MLAG,” on page 729
• the example of the command “upgrade-timeout” on page 745
• the command “ip routing” on page 1066
• the command “show ip routing” on page 1070
• the command “show ip interface” on page 1084
• the command “interface loopback” on page 1085 “id” parameter range
• the command “ip route” on page 1089
• the command “show ip route” on page 1091
• the command “clear ip arp” on page 1096
• the command “show ip arp” on page 1097
• the command “ping” on page 1099
• the command “traceroute” on page 1100
• the command “tcpdump” on page 1102

Removed:
• the command “interface vlan create” from Section 4.1.7, “Commands,” on page 143
• the command “ipv6 dhcp client”

Split:
• the command “ipv6 dhcp”

**Rev 3.70 – March 19, 2015**

Updated:
• the command “speed” on page 1334
• the command “show interfaces ib” on page 1341
• the command “show interfaces ib status” on page 1343

**Rev 3.70 – March 19, 2015**

No changes

**Rev 3.60 – March 05, 2015**

Added:
• MLAG configuration Step 10
• the command “system-mac” on page 744
• the command “upgrade-timeout” on page 745
• Section 5.9.4, “BPDU Guard,” on page 784

Updated:
• MLAG configuration verification Step 1 with system MAC and upgrade timeout
• the command “show mlag” on page 746

Rev 3.60 – March 05, 2015
No changes

Rev 3.50 – February 24, 2015
Added:
• the command “show version concise” on page 494
Updated:
• the command “show uboot” on page 492

Rev 3.40 – February 11, 2015
Added:
• “List of Tables” and “List of Figures” Sections
• Updated Section 2.4, “Licenses,” on page 54
• the command “license delete” on page 60
• the command “license install” on page 61
• the command “telnet” on page 120
• the command “terminal” on page 89
• the command “web cache-enable” on page 125
• the command “ip default-gateway” on page 146
• the command “boot system” on page 226
• the command “configuration write” on page 264
• the command “logging trap” on page 291
• the command “email autosupport enable” on page 320
• the command “crypto ipsec ike” on page 409
• the command “lACP-individual enable” on page 712
• the command “show interfaces port-channel” on page 720
• the command “show interfaces port-channel compatibility-parameters” on page 723
• the command “show interfaces port-channel load-balance” on page 724
• the command “show interfaces port-channel summary” on page 725
• Section 5.9.8, “RPVST,” on page 785
• the command “spanning-tree vlan forward-time” on page 807
• the command “spanning-tree vlan hello-time” on page 808
• the command “spanning-tree vlan max-age” on page 809
• the command “spanning-tree vlan priority” on page 810
• the command “show spanning-tree vlan” on page 816
• Section 6.2, “IPv6,” on page 990
• the command “auto-cost reference-bandwidth” on page 1113
• the command “show ip multicast interface proxy-arp” on page 1630

Updated:
• Section 2.3, “Starting the Web User Interface (WebUI),” on page 50
• the command “image options” on page 234
• the command “reload” on page 244
• Section 4.5.2, “Remote Logging,” on page 271
• the command “logging debug-files” on page 276
• Section 4.6.1, “Commands,” on page 296
• Section 4.9.1, “User Accounts,” on page 355
• the command “username” on page 359
• the command “aaa authentication attempts fail-delay” on page 366
• the command “radius-server host” on page 380
• the command “tacacs-server host” on page 384
• Table 28, “System Health Monitor Alerts Scenarios,” on page 457
• the command “snmp-server auto-refresh” on page 514
• the command “snmp-server user” on page 529
• the command “show interfaces ethernet description” on page 687
• the command “show interfaces ethernet status” on page 689
• the command “show interfaces port-channel summary” on page 725
• the command “show interfaces mlag-port-channel summary” on page 750
• the command “spanning-tree mode” on page 789
• the command “show spanning-tree” on page 811
• the command “show spanning-tree detail” on page 812
• the command “show spanning-tree interface” on page 813
• the command “show spanning-tree mst” on page 814
• the command “show spanning-tree root” on page 815
• Section 5.12.2, “Defining a Multicast Router Port on a VLAN,” on page 868
• the command “dcb application-priority” on page 901
• the command “dcb priority-flow-control enable” on page 1023
• Section 5.17.1, “Flow Samples,” on page 981
• the command “ip arp timeout” on page 1095
• the command “redistribute” on page 1115

Rev 3.30 – November 19, 2014
Added:
• Section 5.1.4, “High Power Transceivers,” on page 668

Updated:
• the command “web https” on page 133
• the command “show interfaces ethernet” on page 682
• the command “show interfaces ethernet transceiver” on page 690
• the command “dcb application-priority” on page 901
• Section A.5, “HTTPS,” on page 1328
• Section B.7, “Password Hashing,” on page 1757

Rev 3.20 – November 09, 2014
Added:
• Section 4.16, “Virtual Machine,” on page 557
• Section 5.8.2, “MAC Learning Considerations,” on page 775
• the command “mac-learning disable” on page 778
• Appendix A, “Enhancing System Security According to NIST SP 800-131A,” on page 1326

Updated:
• Section 1.2, “Ethernet Features,” on page 41
• Section 3.2, “Web Interface Overview,” on page 72
• the command “reset factory” on page 245
• Section 4.14.1.7, “SNMP SET Operations,” on page 503
• the command “interface port-channel” on page 706
• the command “show lacp interfaces neighbor” on page 716
• Section 5.4, “MLAG,” on page 726
• the command “mlag-channel-group mode” on page 741
• the command “show mlag statistics” on page 751
• the command “ip icmp redirect” on page 1083
• Section 6.3, “BGP,” on page 1147
• Section 6.6.2, “Configuring VRRP,” on page 1291

Replaced:
• the command “show lacp interfaces port-channel” with the command “show lacp” on page 718
• the command “show lacp system-identifier” with the command “show lacp interfaces system-identifier” on page 719

Rev 3.10 – July 20, 2014
Added:
• Section 5.18, “Transport Applications,” on page 997
• Section 6.1.1, “IP Interfaces,” on page 1057
• Section 6.3, “BGP,” on page 1147
• the command “show ip pim upstream joins” on page 1271

Updated:
• Chapter 1, “Introduction” on page 40
• Section 4.14.1.8, “IF-MIB and Interface Information,” on page 508
• Section 4.14.3, “XML API,” on page 513
• MAC addresses note in Section 5.4, “MLAG,” on page 726
• Chapter 6, “IP Routing” on page 1057 with the appropriate configuration modes for the new configuration contexts and commands added
• the command “route-map” on page 1209
• the command “continue <sequence-number>” on page 1210
• the command “abort” on page 1212
• the command “exit” on page 1213
• Section 6.5, “Multicast (IGMP and PIM),” on page 1242
• the command “ip pim join-prune-interval” on page 1258
• the command “show ip pim bsr” on page 1264
• the command “show ip mroute” on page 1275

Rev 3.00 – June 05, 2014
Updated:
• Section 6.5, “Multicast (IGMP and PIM),” on page 1242
• Section 6.6.3, “Verifying VRRP,” on page 1293
Rev 2.90 – 19 May, 2014
Added:
• Section 6.5, “Multicast (IGMP and PIM),” on page 1242

Updated:
• the command “show configuration” on page 267
• the command “show uboot” on page 492
• the command “show voltage” on page 495
• Section 5.4, “MLAG,” on page 726
• the command “show mlag” on page 746
• Section 6.1.4.2, “IP Interfaces,” on page 1073
• Section 6.1.4.4, “Loopback Interface,” on page 1085

Rev 2.80 – May 08, 2014
Added:
• supported versions note in Section 5.12, “IGMP Snooping,” on page 868
• Section 6.6, “VRRP,” on page 1290
• Section 6.7, “MAGP,” on page 1305
• Section 6.8, “DHCP Relay,” on page 1313

Rev 2.70 – April 30, 2014
Added:
• Appendix A, “Enhancing System Security According to NIST SP 800-131A,” on page 1326
• supported versions note in Section 5.12, “IGMP Snooping,” on page 868

Updated:
• the command “show ssh server” on page 119
• the command “web auto Logout” on page 123
• the command “web https” on page 133
• the command “show web” on page 139
• the command “show usernames” on page 361
• the command “ldap base-dn” on page 387
• the command “ldap ssl” on page 398
Rev 2.60 – April 10, 2014
Updated:
• Table 32, “Private MIBs Supported,” on page 499

Rev 2.50 – April 2014
Updated:
• Section 3.1.7, “CLI Pipeline Operator Commands,” on page 68
• the command “show protocols” on page 485
• the command “show mac-address-table” on page 780
• the command “deny/permit (MAC ACL rule)” on page 953
• the command “show mac/ipv4 access-lists” on page 963
Added:
• Section 5.4, “MLAG,” on page 726
• configuration mode Config Interface MLAG Port Channel to the following commands:
  • “flowcontrol” on page 672
  • “mtu” on page 674
  • “shutdown” on page 675
  • “description” on page 676
  • “speed” on page 677
  • “load-interval” on page 678
  • “clear counters” on page 681
  • “switchport mode” on page 758
  • “switchport access” on page 761
  • “spanning-tree port-priority” on page 793
  • “spanning-tree cost” on page 794
  • “spanning-tree port type” on page 795
  • “spanning-tree guard” on page 796
  • “ip igmp snooping fast-leave” on page 875
  • “dcb priority-flow-control mode on” on page 1025
  • “ipv4/mac port access-group” on page 952
  • “sflow enable (interface)” on page 995
Rev 2.40 – February, 2014

Updated:
- Section 4.3.5.2, “Importing Firmware and Changing the Default Firmware,” on page 222 – updated Step 1
- the command “show running-config” on page 269
- the command “show log” on page 293
- Section 4.10, “Cryptographic (X.509, IPSec) and Encryption,” on page 407
- Section 5.3.1, “Configuring Static Link Aggregation Group (LAG),” on page 704 – removed unnecessary step
- the command “lldp tlv-select” on page 899

Added:
- Section 3.1.7, “CLI Pipeline Operator Commands,” on page 68
- FCoE and SX1700 GW license in Section 2.4, “Licenses,” on page 54
- Section 4.14.1.8, “IF-MIB and Interface Information,” on page 508


Updated:
- Section 4.15.4, “Writing Configuration Classes,” on page 539
- the command “crypto certificate generation” on page 415
- the command “crypto certificate name” on page 417

Rev 2.20 – January, 2014

Updated:
- Section 4.15.5.11, “Installed Image Capabilities,” on page 546

Rev 2.10 – January, 2014

Added:
- Section 4.13.2.1, “Width Reduction Power Saving,” on page 463

Updated:
- Section 2.2, “Starting the Command Line (CLI),” on page 49
- Section 2.3, “Starting the Web User Interface (WebUI),” on page 50
- Section 4.3.1, “Upgrading MLNX-OS Software,” on page 213 with EULA note
- Section 4.15, “Puppet Agent,” on page 538
- the command “load-interval” on page 678 with Config Interface Port Channel
• the command “spanning-tree port-priority” on page 793 with Config Interface Port Channel
• Section 5.10, “OpenFlow,” on page 818
• the command “openflow description (SwitchX)” on page 830
• the command “show openflow” on page 842
• the command “switchport {hybrid, trunk} allowed-vlan” on page 762 with Config Interface Port Channel
• the command “spanning-tree cost” on page 794 with Config Interface Port Channel
• the command “spanning-tree port type” on page 795 with Config Interface Port Channel
• the command “spanning-tree guard” on page 796 with Config Interface Port Channel
• the command “spanning-tree bpdufilter” on page 797 with Config Interface Port Channel
• the command “deny/permit (IPv4 ACL rule)” on page 955
• the command “sflow enable (interface)” on page 995 with Config Interface Port Channel
• Section 6.2, “OSPF,” on page 1104
• the command “router-id” on page 1111

Rev 2.00 – December 2013
Added:
• Section 5.1.3, “Transceiver Information,” on page 667
• the command “run-interval” on page 552
Updated:
• Section 4.3.1, “Upgrading MLNX-OS Software,” on page 213
• Section 4.3.3, “Deleting Unused Images,” on page 217
• Section 4.6, “Debugging,” on page 295
• the example of the command “show cpld” on page 476
• “Notification Indicator” column in Section 8.4.2, “Standalone Proxy-ARP Configuration,” on page 1573
• the command “show puppet-agent” on page 554
• the command “lldp tlv-select” on page 899
Moved:
Section 3.3, “Secure Shell (SSH),” on page 78 from 4.13.2
Removed:
• mention of the MLNX-OS Command Reference Guide
• the command “lldp tlv-select dcbx”

**Rev 1.90 – November 2013**

Added Appendix A, “MEX6200 System,” on page 1635

**Rev 1.80 – October 2013**

Added:
- Section 4.15, “Puppet Agent,” on page 538
- Section 5.9.7, “MSTP,” on page 785
- Section 5.10, “OpenFlow,” on page 818
- Section 5.12.3, “IGMP Snooping Querier,” on page 870
- the command “ip igmp snooping querier”
- the command “igmp snooping querier query-interval”
- the command “show ip igmp snooping querier”
- Section 5.13.2, “DCBX,” on page 892
- the command “lldp tlv-select dcbx”
- the command “dcb application-priority”
- the command “show dcb application-priority”

Updated:
- the command “show lldp interfaces”

**Rev 1.7.0 – October 2013**

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**

<table>
<thead>
<tr>
<th>Document Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>System Hardware User Manual</td>
<td>This document contains hardware descriptions, LED assignments and hardware specifications among other things.</td>
</tr>
<tr>
<td>Switch Product Release Notes</td>
<td>Please look up the relevant SwitchX®-based switch system/series release note file</td>
</tr>
<tr>
<td>Mellanox Virtual Modular Switch Reference Guide</td>
<td>This reference architecture provides general information concerning Mellanox L2 and L3 Virtual Modular Switch (VMS) configuration and design.</td>
</tr>
<tr>
<td>MLNX-OS® XML API Reference Guide</td>
<td>This manual provides general information concerning MLNX-OS® XML API.</td>
</tr>
</tbody>
</table>

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**

<table>
<thead>
<tr>
<th>AAA</th>
<th>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.</th>
</tr>
</thead>
<tbody>
<tr>
<td>ARP</td>
<td>Address Resolution Protocol. A protocol that translates IP addresses into MAC addresses for communication over a local area network (LAN).</td>
</tr>
<tr>
<td>CLI</td>
<td>Command Line Interface. A user interface in which you type commands at the prompt</td>
</tr>
<tr>
<td>DCB</td>
<td>Data Center Bridging</td>
</tr>
</tbody>
</table>
### Table 2 - Glossary

<table>
<thead>
<tr>
<th>Term</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DCBX</td>
<td>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.</td>
</tr>
<tr>
<td>DHCP</td>
<td>The Dynamic Host Configuration Protocol (DHCP) is an automatic configuration protocol used on IP networks.</td>
</tr>
<tr>
<td>DNS</td>
<td>Domain Name System. A hierarchical naming system for devices in a computer network.</td>
</tr>
<tr>
<td>ETS</td>
<td>ETS provides a common management framework for assignment of bandwidth to traffic classes.</td>
</tr>
<tr>
<td>FTP/TFTP/sFTP</td>
<td>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.</td>
</tr>
<tr>
<td>Gateway</td>
<td>A network node that interfaces with another network using a different network protocol.</td>
</tr>
<tr>
<td>HA (High Availability)</td>
<td>A system design protocol that provides redundancy of system components, thus enables overcoming single or multiple failures in minimal downtime.</td>
</tr>
<tr>
<td>Host</td>
<td>A computer platform executing an Operating System which may control one or more network adapters.</td>
</tr>
<tr>
<td>LACP</td>
<td>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).</td>
</tr>
<tr>
<td>LDAP</td>
<td>The Lightweight Directory Access Protocol is an application protocol for reading and editing directories over an IP network.</td>
</tr>
<tr>
<td>LLDP (Link Layer Discov-ery Protocol)</td>
<td>A vendor neutral link layer protocol used by network devices to advertise their identity, capabilities and for neighbor discovery</td>
</tr>
<tr>
<td>MAC</td>
<td>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.</td>
</tr>
<tr>
<td>MTU (Maximum Transfer Unit)</td>
<td>The maximum size of a packet payload (not including headers) that can be sent/received from a port</td>
</tr>
<tr>
<td>Network Adapter</td>
<td>A hardware device that allows for communication between computers in a network.</td>
</tr>
<tr>
<td>PFC/FC</td>
<td>Priority Based Flow Control applies pause functionality to traffic classes OR classes of service on the Ethernet link.</td>
</tr>
</tbody>
</table>
### Table 2 - Glossary

<table>
<thead>
<tr>
<th>Term</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>RADIUS</td>
<td>Remote Authentication Dial In User Service. A networking protocol that enables AAA centralized management for computers to connect and use a network service.</td>
</tr>
<tr>
<td>RDMA (Remote Direct Memory Access)</td>
<td>Accessing memory in a remote side without involvement of the remote CPU.</td>
</tr>
<tr>
<td>RSTP</td>
<td>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.</td>
</tr>
<tr>
<td>SA (Subnet Administrator)</td>
<td>The interface for querying and manipulating subnet management data.</td>
</tr>
<tr>
<td>SCP</td>
<td>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.</td>
</tr>
<tr>
<td>SSH</td>
<td>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.</td>
</tr>
<tr>
<td>syslog</td>
<td>A standard for forwarding log messages in an IP network.</td>
</tr>
<tr>
<td>TACACS+</td>
<td>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.</td>
</tr>
</tbody>
</table>
1 Introduction

Mellanox® Operating System (MLNX-OS®) enables the management and configuration of Mellanox Technologies’ SwitchX® Family silicon based switch 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*

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Software Management</td>
<td>• Dual software image</td>
</tr>
<tr>
<td></td>
<td>• Software and firmware updates</td>
</tr>
<tr>
<td>File management</td>
<td>• FTP</td>
</tr>
<tr>
<td></td>
<td>• TFTP</td>
</tr>
<tr>
<td></td>
<td>• SCP</td>
</tr>
<tr>
<td>Logging</td>
<td>• Event history log</td>
</tr>
<tr>
<td></td>
<td>• SysLog support</td>
</tr>
<tr>
<td>Management Interface</td>
<td>• DHCP/Zeroconf</td>
</tr>
<tr>
<td></td>
<td>• IPv6</td>
</tr>
<tr>
<td>Chassis Management</td>
<td>• Monitoring environmental controls</td>
</tr>
<tr>
<td></td>
<td>• Power management</td>
</tr>
<tr>
<td></td>
<td>• Auto-temperature control</td>
</tr>
<tr>
<td></td>
<td>• High availability</td>
</tr>
<tr>
<td>Network Management</td>
<td>• SNMP v1, v2c, v3</td>
</tr>
<tr>
<td>Interfaces</td>
<td>• interfaces (XML Gateway)</td>
</tr>
<tr>
<td></td>
<td>• Puppet Agent</td>
</tr>
<tr>
<td>Security</td>
<td>• SSH</td>
</tr>
<tr>
<td></td>
<td>• Telnet</td>
</tr>
<tr>
<td></td>
<td>• RADIUS</td>
</tr>
<tr>
<td></td>
<td>• TACACS+</td>
</tr>
<tr>
<td>Date and Time</td>
<td>• NTP</td>
</tr>
<tr>
<td>Cables &amp; Transceivers</td>
<td>• Transceiver info</td>
</tr>
<tr>
<td>Unbreakable links</td>
<td>• LLR</td>
</tr>
</tbody>
</table>
## 1.2 Ethernet Features

*Table 4 - Ethernet Features*

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>General</td>
<td>• ACL – 6400 rules (permit/deny)</td>
</tr>
<tr>
<td></td>
<td>• Breakout cables</td>
</tr>
<tr>
<td></td>
<td>• Jumbo Frames (9K)</td>
</tr>
<tr>
<td>Ethernet support</td>
<td>• 48K unicast MAC addresses on SwitchX®-2 based systems</td>
</tr>
<tr>
<td></td>
<td>• 2K static multicast MAC addresses</td>
</tr>
<tr>
<td></td>
<td>• 90100 unicast MAC addresses on Spectrum™ based systems</td>
</tr>
<tr>
<td></td>
<td>• DCBX</td>
</tr>
<tr>
<td></td>
<td>• DHCP Relay</td>
</tr>
<tr>
<td></td>
<td>• ETS (802.1Qaz)</td>
</tr>
<tr>
<td></td>
<td>• Flow control (802.3x)</td>
</tr>
<tr>
<td></td>
<td>• IGMP snooping v1,2</td>
</tr>
<tr>
<td></td>
<td>• LAG/LACP (802.3ad), 16 links per LAG (64 LAGs)</td>
</tr>
<tr>
<td></td>
<td>• LLDP</td>
</tr>
<tr>
<td></td>
<td>• MLAG</td>
</tr>
<tr>
<td></td>
<td>• MSTP</td>
</tr>
<tr>
<td></td>
<td>• OpenFlow 1.3</td>
</tr>
<tr>
<td></td>
<td>• PFC (802.1Qbb)</td>
</tr>
<tr>
<td></td>
<td>• Rapid Spanning Tree (802.1w)</td>
</tr>
<tr>
<td></td>
<td>• sFlow</td>
</tr>
<tr>
<td></td>
<td>• VLAN (802.1Q) – 4K</td>
</tr>
<tr>
<td>IP routing</td>
<td>• BGP</td>
</tr>
<tr>
<td></td>
<td>• DHCP Relay</td>
</tr>
<tr>
<td></td>
<td>• ECMP</td>
</tr>
<tr>
<td></td>
<td>• IGMP</td>
</tr>
<tr>
<td></td>
<td>• IPv4</td>
</tr>
<tr>
<td></td>
<td>• IPv6</td>
</tr>
<tr>
<td></td>
<td>• OSPF</td>
</tr>
<tr>
<td></td>
<td>• PIM</td>
</tr>
<tr>
<td></td>
<td>• VLAN interface</td>
</tr>
<tr>
<td></td>
<td>• Loopback interface</td>
</tr>
<tr>
<td></td>
<td>• Router interface</td>
</tr>
<tr>
<td></td>
<td>• VRRP</td>
</tr>
</tbody>
</table>
**Figure 1: Managing an Ethernet Fabric Using MLNX-OS**

Diagram showing a network topology with servers, switches, Ethernet fabric, and remote management node.
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.

Step 2.

![Console Ports SX10xx Systems](image)

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 3. 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.
Step 4. You are prompted with the boot menu.

Mellanox MLNX-OS Boot Menu:

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

Choice:

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

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

Step 5. 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 6. Go through the Mellanox configuration wizard.

---

**Table 5 - Serial Terminal Program Configuration for PPC Based Systems**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Baud Rate</td>
<td>9600</td>
</tr>
<tr>
<td>Data bits</td>
<td>8</td>
</tr>
<tr>
<td>Stop bits</td>
<td>1</td>
</tr>
<tr>
<td>Parity</td>
<td>None</td>
</tr>
<tr>
<td>Flow Control</td>
<td>None</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Baud Rate</td>
<td>115200</td>
</tr>
<tr>
<td>Data bits</td>
<td>8</td>
</tr>
<tr>
<td>Stop bits</td>
<td>1</td>
</tr>
<tr>
<td>Parity</td>
<td>None</td>
</tr>
<tr>
<td>Flow Control</td>
<td>None</td>
</tr>
</tbody>
</table>
The following table shows an example of a wizard session.

**Table 7 - Configuration Wizard Session - IP Configuration by DHCP (Sheet 1 of 2)**

<table>
<thead>
<tr>
<th>Wizard Session Display (Example)</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mellanox configuration wizard Do you want to use the wizard for initial configuration? yes</td>
<td>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 &lt;Enter&gt;.</td>
</tr>
<tr>
<td><strong>Step1:</strong> Hostname? [switch-1]</td>
<td>If you wish to accept the default hostname, then press &lt;Enter&gt;. Otherwise, type a different hostname and press &lt;Enter&gt;.</td>
</tr>
<tr>
<td><strong>Step 2:</strong> Use DHCP on mgmt0 interface? [yes]</td>
<td>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 &lt;Enter&gt;. 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 static IP, and the session will continue as shown in Table 9.</td>
</tr>
<tr>
<td><strong>Step 3:</strong> Enable IPv6 [yes]</td>
<td>Perform this step to enable IPv6 on management ports. If you wish to enable IPv6, type “yes” and press &lt;Enter&gt;. If you enter “no” (no IPv6), then you will automatically be referred to Step 5.</td>
</tr>
<tr>
<td><strong>Step 4:</strong> Enable IPv6 autoconfig (SLAAC) on mgmt0 interface</td>
<td>Perform this step to enable StateLess address autoconfig on external management port. If you wish to enable it, type “yes” and press &lt;Enter&gt;. If you wish to disable it, enter “no”.</td>
</tr>
<tr>
<td><strong>Step 5:</strong> Use DHCPv6 on mgmt0 interface? [yes]</td>
<td>Perform this step to enable DHCPv6 on the MGMT0 interface.</td>
</tr>
</tbody>
</table>
**Table 7 - Configuration Wizard Session - IP Configuration by DHCP (Sheet 2 of 2)**

<table>
<thead>
<tr>
<th>Wizard Session Display (Example)</th>
<th>Comments</th>
</tr>
</thead>
</table>
| **Step 5:** Admin password (Press `<Enter>` to leave unchanged)? `<new_password>`
Step 4: Confirm admin password? `<new_password>` | To avoid illegal access to the machine, please type a password and then press `<Enter>`. Then confirm the password by re-entering it. Note that password characters are not printed. |
| You have entered the following information: | The wizard displays a summary of your choices and then asks you to confirm the choices or to re-edit them. |
| 1. Hostname: `<switch name>`
2. Use DHCP on mgmt0 interface: yes
3. Enable IPv6: yes
4. Enable IPv6 autoconfig (SLAAC) on mgmt0 interface: yes
5. Enable DHCPv6 on mgmt0 interface: no
6. Admin password (Enter to leave unchanged): (CHANGED) | Either press `<Enter>` to save changes and exit, or enter the configuration step number that you wish to return to. Note: To run the command “configuration jump-start” you must be in Config mode. |
| To change an answer, enter the step number to return to. Otherwise hit `<enter>` to save changes and exit. | |
| Choice: `<Enter>` | |
| Configuration changes saved. To return to the wizard from the CLI, enter the “configuration jump-start” command from configuration mode. Launching CLI... | |
| `<switch name> [standalone: master] >` | |
Table 8 - Configuration Wizard Session - IP Zeroconf Configuration

Wizard Session Display - IP Zeroconf Configuration (Example)

Mellanox configuration wizard

Do you want to use the wizard for initial configuration? y

Step 1: Hostname? [switch-112126]
Step 2: Use DHCP on mgmt0 interface? [no]
Step 3: Use zeroconf on mgmt0 interface? [no] yes
Step 4: Default gateway? [192.168.10.1]
Step 5: Primary DNS server?
Step 6: Domain name?
Step 7: Enable IPv6? [yes] yes
Step 8: Enable IPv6 autoconfig (SLAAC) on mgmt0 interface? [no] no
Step 9: Admin password (Enter to leave unchanged)?

You have entered the following information:

1. Hostname: switch-112126
2. Use DHCP on mgmt0 interface: no
3. Use zeroconf on mgmt0 interface: yes
4. Default gateway: 192.168.10.1
5. Primary DNS server:
6. Domain name:
7. Enable IPv6: yes
8. Enable IPv6 autoconfig (SLAAC) on mgmt0 interface: yes
9. Admin password (Enter to leave unchanged): (unchanged)

To change an answer, enter the step number to return to. Otherwise hit <enter> to save changes and exit.

Choice:

Configuration changes saved.

To return to the wizard from the CLI, enter the “configuration jump-start” command from configure mode. Launching CLI...

<switch name> [standalone: master>
Table 9 - Configuration Wizard Session - Static IP Configuration

<table>
<thead>
<tr>
<th>Wizard Session Display - Static IP Configuration (Example)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mellanox configuration wizard</td>
</tr>
<tr>
<td>Do you want to use the wizard for initial configuration? y</td>
</tr>
<tr>
<td>Step 1: Hostname? [switch-112126]</td>
</tr>
<tr>
<td>Step 2: Use DHCP on mgmt0 interface? [yes] n</td>
</tr>
<tr>
<td>Step 3: Use zeroconf on mgmt0 interface? [no]</td>
</tr>
<tr>
<td>Step 4: Primary IP address? 192.168.10.4</td>
</tr>
<tr>
<td>Mask length may not be zero if address is not zero (interface mgmt0)</td>
</tr>
<tr>
<td>Step 5: Netmask? [0.0.0.0] 255.255.255.0</td>
</tr>
<tr>
<td>Step 6: Default gateway? 192.168.10.1</td>
</tr>
<tr>
<td>Step 7: Primary DNS server?</td>
</tr>
<tr>
<td>Step 8: Domain name?</td>
</tr>
<tr>
<td>Step 9: Enable IPv6? [yes] yes</td>
</tr>
<tr>
<td>Step 10: Enable IPv6 autoconfig (SLAAC) on mgmt0 interface? [no] no</td>
</tr>
<tr>
<td>Step 11: Admin password (Enter to leave unchanged)?</td>
</tr>
</tbody>
</table>

You have entered the following information:

1. Hostname: switch-112126
2. Use DHCP on mgmt0 interface: no
3. Use zeroconf on mgmt0 interface: no
4. Primary IP address: 192.168.10.4
5. Netmask: 255.255.255.0
6. Default gateway: 192.168.10.1
7. Primary DNS server:
8. Domain name:
9. Enable IPv6: yes
10. Enable IPv6 autoconfig (SLAAC) on mgmt0 interface: no
11. Admin password (Enter to leave unchanged): (unchanged)

To change an answer, enter the step number to return to. Otherwise hit <enter> to save changes and exit.

Choice:

Configuration changes saved.

To return to the wizard from the CLI, enter the “configuration jump-start” command from configure mode. Launching CLI...

<switch name>[standalone: master] >
Step 7. 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 state
Admin up: yes
Link up: yes
IP address: 169.254.15.134
Netmask: 255.255.0.0
IPv6 enabled: yes
Autoconf enabled: yes
Autoconf route: yes
Autoconf privacy: 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
Comment:
RX bytes: 11700449 TX bytes: 15139846
RX packets: 55753 TX packets: 28452
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
```

2.1.1 Re-Running 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> <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
```

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.
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 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.

**Figure 6: Display After Login**

A default status summary is displayed as shown in Figure 6.
2.4 Licenses

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

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

The following licenses are offered with MLNX-OS software:

Table 10 - MLNX-OS Licenses

<table>
<thead>
<tr>
<th>OPN</th>
<th>Valid on Product</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>UPG-6012-GW</td>
<td>SX6012</td>
<td>Ethernet L2/L3, Gateway</td>
</tr>
<tr>
<td>UPG-1012-GW</td>
<td>SX1012</td>
<td>Ethernet L3, Gateway</td>
</tr>
<tr>
<td>UPG-6018-GW</td>
<td>SX6018</td>
<td>Ethernet L2/L3, Gateway</td>
</tr>
<tr>
<td>UPG-6036-GW</td>
<td>SX6036</td>
<td>Ethernet L2/L3, Gateway</td>
</tr>
<tr>
<td>UPG-1036-GW</td>
<td>SX1036</td>
<td>Ethernet L3, Gateway</td>
</tr>
<tr>
<td>UPG-1710-GW</td>
<td>SX1710</td>
<td>Ethernet L3, Gateway</td>
</tr>
<tr>
<td>UPG-6710-GW</td>
<td>SX6710</td>
<td>Ethernet L3, Gateway</td>
</tr>
<tr>
<td>UPG-xxxx-FCOE-J</td>
<td>All systems supporting Ethernet directly or via license</td>
<td>Enables FCoE protocol</td>
</tr>
</tbody>
</table>

2.4.1 Installing MLNX-OS® License (CLI)

➢ To install an MLNX-OS license via CLI:

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

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

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

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

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

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

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

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

```
switch (config) # configuration write
```
2.4.2 Installing MLNX-OS License (Web)

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

  **Step 1.** Log in as `admin`.
  
  **Step 2.** Click the **Setup** tab and then **Licensing** on the left side navigation pane.

  ![Figure 7: No Licenses Installed](image)

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

  If you wish to add another license key in the future, you can simply enter it in the text box and click “Add Licenses” to install it.
Figure 8: Enter License Key(s) in Text Box

All installed licenses should now be displayed.

Figure 9: Installed License
Step 4. Save the configuration to complete the license installation.

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

2.4.3 Retrieving a Lost License Key

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

- To obtain the switch’s chassis serial number:
  
  Step 1. Login to the switch.
  
  Step 2. Retrieve the switch’s chassis serial number using the command “show inventory”.

```
switch (config) # show inventory
```

<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>PSI</td>
<td>MSX60-FF</td>
<td>MT1206X06697</td>
<td>N/A</td>
<td>A2</td>
</tr>
</tbody>
</table>

```
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 44.

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

#### file eula upload

*file eula upload <filename> <URL>*

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

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>filename</th>
<th>The Mellanox End User License Agreement</th>
</tr>
</thead>
<tbody>
<tr>
<td>URL</td>
<td>URL or scp://username[:password]@hostname/path/filename</td>
<td></td>
</tr>
</tbody>
</table>

**Default**

N/A

**Configuration Mode**

Config

**History**

3.4.1100

**Role**

monitor/admin

**Example**

```
switch (config) # file help-docs upload Mellanox_End_User_License_Agreement.pdf <scp://username[:password]@hostname/path/filename>
switch (config) #
```

**Related Commands**

license

**Note**
### file help-docs upload

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

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

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>filename</td>
<td>The file to upload to a remote host</td>
</tr>
<tr>
<td>URL</td>
<td>URL or scp://username[:password]@hostname/path/filename</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Default</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuration Mode</td>
<td>Config</td>
</tr>
<tr>
<td>History</td>
<td>3.4.1100</td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
</tr>
</tbody>
</table>

**Example**

```
```

**Related Commands**

**Note**
**license delete**

`license delete <license-number>`

Removes license keys by ID.

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

license install <license-key>

Installs a new license key.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>N/A</td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Config</td>
</tr>
<tr>
<td>History</td>
<td>3.4.1100</td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
</tr>
</tbody>
</table>
| Example            | switch (config) # licenses install <license-key>
|                    | switch (config) # |

Related Commands

Note
show licenses

show licenses

Displays a list of all installed licenses. For each license, the following is displayed:
• a unique ID which is a small integer
• the text of the license key as it was added
• whether or not it is valid and active
• which feature(s) it is activating
• a list of all licensable features specifying whether or not it is currently activated by a license

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>N/A</td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Config</td>
</tr>
<tr>
<td>History</td>
<td>3.4.1100</td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
</tr>
</tbody>
</table>
| Example            | switch (config) # show licenses  
License 1: <license key>  
Feature: SX_CONFIG  
Valid: yes  
Active: yes  
switch (config) # |

Related Commands

Note
3 User Interfaces

3.1 Command Line Interface 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).

3.1.1 CLI Modes

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

Table 11 - CLI Modes and Config Context

<table>
<thead>
<tr>
<th>Configuration Mode</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Standard</td>
<td>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.</td>
</tr>
<tr>
<td>Enable</td>
<td>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.</td>
</tr>
<tr>
<td>Config</td>
<td>The configure terminal command moves the user from Enable mode to Config mode. Config mode is allowed only for user accounts in the “admin” role (or capabilities). This mode has a full unrestricted set of commands to view anything, take any action, and change any configuration. Its commands are a superset of those in Enable mode. To return to Enable mode, enter exit or no configure. Note that moving directly from/to Standard mode to/from Config mode is not possible.</td>
</tr>
<tr>
<td>Config Interface Management</td>
<td>Configuration mode for management interface mgmt0, mgmt1 and loopback.</td>
</tr>
<tr>
<td>Config Interface Ethernet</td>
<td>Configuration mode for Ethernet interface.</td>
</tr>
<tr>
<td>Config Interface Port Channel</td>
<td>Configuration mode for Port channel (LAG).</td>
</tr>
<tr>
<td>Config VLAN</td>
<td>Configuration mode for VLAN.</td>
</tr>
<tr>
<td>Any Command Mode</td>
<td>Several commands such as “show” can be applied within any context.</td>
</tr>
</tbody>
</table>
3.1.2 Syntax Conventions

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

**Table 12 - Syntax Conventions**

<table>
<thead>
<tr>
<th>Syntax Convention</th>
<th>Description</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt; &gt; Angled brackets</td>
<td>Indicate a value/variable that must be replaced.</td>
<td>&lt;1...65535&gt; or &lt;switch interface&gt;</td>
</tr>
<tr>
<td>[ ] Square brackets</td>
<td>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.</td>
<td>[destination-ip</td>
</tr>
<tr>
<td>{ } Braces</td>
<td>Enclose alternatives or variables that are required for the parameter in square brackets.</td>
<td>[mode {active</td>
</tr>
<tr>
<td></td>
<td>Vertical bars</td>
<td>Identify mutually exclusive choices.</td>
</tr>
</tbody>
</table>

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

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

3.1.3 Getting Help

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

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

```
switch > ?
cli Configure CLI shell options
enable Enter enable mode
exit Log out of the CLI
help View description of the interactive help system
no Negate or clear certain configuration options
```
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, you can hit double tabs to obtain the disambiguation options. Thus, if you are in Enable mode and wish to learn which commands start with the letter “c”, type “c” and click twice on the tab key to get the following:

```
switch # c<tab>
clear cli configure
switch # c
```

(There are three commands that start with the letter “c”: clear, cli and configure.)

### 3.1.4 Prompt and Response Conventions

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

```
switch >  (Standard mode)
switch #  (Enable mode)
switch (config) #  (Config mode)
```
The following session shows how to move between command modes:

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

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

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

### 3.1.5 Using the “no” Form

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

The following example performs the following:

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

```
// 1. Display the current CLI session options
switch (config) # show cli
CLI current session settings:
Maximum line size:          8192
Terminal width:             157 columns
Terminal length:            60 rows
Terminal type:              xterm
Auto-logout:                15 minutes
Paging:                     enabled
Progress tracking:          enabled
Prefix modes:               enabled
...

// 2. Disable auto-logout
switch (config) # no cli session auto-logout

// 3. Display the new CLI session options
switch-1 [standalone: master] (config) # show cli
CLI current session settings:
```
3.1.6 Parameter Key

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

Table 13 - Angled Brackets Parameter Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;domain&gt;</td>
<td>A domain name, e.g. “mellanox.com”.</td>
</tr>
<tr>
<td>&lt;hostname&gt;</td>
<td>A hostname, e.g. “switch-1”.</td>
</tr>
<tr>
<td>&lt;ifname&gt;</td>
<td>An interface name, e.g. “mgmt0”, “mgmt1”, “lo” (loopback), etc.</td>
</tr>
<tr>
<td>&lt;index&gt;</td>
<td>A number to be associated with aliased (secondary) IP addresses.</td>
</tr>
<tr>
<td>&lt;IP address&gt;</td>
<td>An IPv4 address, e.g. “192.168.0.1”</td>
</tr>
<tr>
<td>&lt;log level&gt;</td>
<td>A syslog logging severity level. Possible values, from least to most severe, are: “debug”, “info”, “notice”, “warning”, “error”, “crit”, “alert”, “emerg”.</td>
</tr>
<tr>
<td>&lt;GUID&gt;</td>
<td>Globally Unique Identifier. A number that uniquely identifies a device or component.</td>
</tr>
</tbody>
</table>
3.1.7 CLI Pipeline Operator Commands

3.1.7.1 “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:

```bash
switch (config) # <show command> | {include | exclude} <extended regular expression>
```

Table 13 - Angled Brackets Parameter Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;MAC address&gt;</td>
<td>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”.</td>
</tr>
<tr>
<td>&lt;netmask&gt;</td>
<td>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.</td>
</tr>
<tr>
<td>&lt;network prefix&gt;</td>
<td>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”.</td>
</tr>
<tr>
<td>&lt;regular expression&gt;</td>
<td>An extended regular expression as defined by the “grep” in the man page. (The value you provide here is passed on to “grep -E”).</td>
</tr>
<tr>
<td>&lt;node id&gt;</td>
<td>ID of a node belonging to a cluster. This is a numerical value greater than zero.</td>
</tr>
<tr>
<td>&lt;cluster id&gt;</td>
<td>A string specifying the name of a cluster.</td>
</tr>
<tr>
<td>&lt;port&gt;</td>
<td>TCP/UDP port number.</td>
</tr>
<tr>
<td>&lt;TCP port&gt;</td>
<td>A TCP port number in the full allowable range [0...65535].</td>
</tr>
</tbody>
</table>
| <URL>            | A normal URL, using any protocol that wget supports, including http, https, ftp, sftp, and tftp; or a pseudo-URL specifying an scp file transfer. The scp pseudo-URL format is scp://username:password@hostname/path/filename.  
Note that the path is an absolute path. Paths relative to the user's home directory are not currently supported. The implementation of ftp does not support authentication, so use scp or sftp for that. 
Note also that if you omit the “:password” part, you may be prompted for the password in a follow up prompt, where you can type it securely (without the characters being echoed). This prompt will occur if the “cli default prompt empty-password” setting is true; otherwise, the CLI will assume you do not want any password. If you include the “:” character, this will be taken as an explicit declaration that the password is empty, and you will not be prompted in any case. |
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
```

### 3.1.7.2 “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:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>PS1</td>
<td>power-mon</td>
<td>input 85.36</td>
<td>238.00</td>
<td>3.38</td>
<td>400.00</td>
<td>AC</td>
<td>OK</td>
</tr>
<tr>
<td>PS2</td>
<td>power-mon</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Total power used: 85.36 Watts
Total power capacity: 400.00 Watts
Total power available: 375.60 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
```

### 3.1.7.3 “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 4.14.2, “JSON API,” on page 508.
3.1.8 **CLI Shortcuts**

Table 14 presents the available keyboard shortcuts on the MLNX-OS® CLI.

<table>
<thead>
<tr>
<th>Key Combination</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ctrl-a</td>
<td>Move cursor to beginning of line</td>
</tr>
<tr>
<td>Ctrl-b</td>
<td>Move cursor backward one character without deleting</td>
</tr>
<tr>
<td>Ctrl-c</td>
<td>Terminate operation</td>
</tr>
<tr>
<td>Ctrl-d</td>
<td>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.</td>
</tr>
<tr>
<td>Ctrl-e</td>
<td>Move cursor to end of line</td>
</tr>
<tr>
<td>Ctrl-f</td>
<td>Move cursor forward one character</td>
</tr>
<tr>
<td>Ctrl-h</td>
<td>Delete one character backwards from cursor</td>
</tr>
<tr>
<td>Ctrl-i</td>
<td>Auto-complete current word (same as TAB)</td>
</tr>
<tr>
<td>Ctrl-j</td>
<td>Return carriage (same as ENTER)</td>
</tr>
<tr>
<td>Ctrl-k</td>
<td>Delete line after cursor</td>
</tr>
<tr>
<td>Ctrl-l</td>
<td>Clear screen and show line at the top of terminal window</td>
</tr>
<tr>
<td>Ctrl-m</td>
<td>Return carriage (same as ENTER)</td>
</tr>
<tr>
<td>Ctrl-n</td>
<td>Next line (same as DOWN ARROW)</td>
</tr>
<tr>
<td>Ctrl-p</td>
<td>Next line (same as UP ARROW)</td>
</tr>
<tr>
<td>Ctrl-t</td>
<td>Transpose the two characters on either side of cursor</td>
</tr>
<tr>
<td>Ctrl-u</td>
<td>Delete line</td>
</tr>
<tr>
<td>Ctrl-y</td>
<td>Retrieve (“yank”) last item deleted</td>
</tr>
<tr>
<td>Esc b</td>
<td>Move cursor one word backward</td>
</tr>
<tr>
<td>Esc c</td>
<td>Capitalizes first letter in word after cursor</td>
</tr>
<tr>
<td>Esc d</td>
<td>Delete one word forward from cursor</td>
</tr>
<tr>
<td>Esc f</td>
<td>Move one word forward from cursor</td>
</tr>
<tr>
<td>Esc l</td>
<td>Change word after cursor to lowercase letters</td>
</tr>
<tr>
<td>Esc Ctrl-h</td>
<td>Delete one word backward from cursor</td>
</tr>
<tr>
<td>Esc [ A</td>
<td>Next line (same as DOWN ARROW)</td>
</tr>
<tr>
<td>Esc [ B</td>
<td>Next line (same as UP ARROW)</td>
</tr>
</tbody>
</table>
### 3.2 Web Interface Overview

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

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

The web interface makes available the following perspective tabs:

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

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

<table>
<thead>
<tr>
<th>Key Combination</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Esc [ C</td>
<td>Move forward one character from cursor</td>
</tr>
<tr>
<td>Esc [ D</td>
<td>Move backward one character from cursor</td>
</tr>
</tbody>
</table>
3.2.1 Setup Menu

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

**Table 15 - WebUI Setup Submenus**

<table>
<thead>
<tr>
<th>Submenu Title</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interfaces</td>
<td>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.</td>
</tr>
<tr>
<td>Routing</td>
<td>Configures, removes or displays the default gateway, and the static and dynamic routes.</td>
</tr>
<tr>
<td>Hostname</td>
<td>Configures or modifies the hostname. Configures or deletes static hosts.</td>
</tr>
<tr>
<td>DNS</td>
<td>Configures, removes, modifies or displays static and dynamic name servers.</td>
</tr>
<tr>
<td>Login Messages</td>
<td>Edits the login messages: Message of the Day (MOTD), Remote Login message, and Local Login message.</td>
</tr>
</tbody>
</table>
### 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

<table>
<thead>
<tr>
<th>Submenu Title</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Address Resolution</td>
<td>Adds static and dynamic ARP entries, and clears the dynamic ARP cache.</td>
</tr>
<tr>
<td>IPSec</td>
<td>Configures IPSec.</td>
</tr>
<tr>
<td>Neighbors</td>
<td>Displays IPv6 neighbor discovery protocol.</td>
</tr>
<tr>
<td>Virtualization</td>
<td>Manages the virtualization and virtual machines.</td>
</tr>
<tr>
<td>Virtual Switch Mgmt</td>
<td>Configures the system profile.</td>
</tr>
<tr>
<td>Web</td>
<td>Configures web user interface and proxy settings.</td>
</tr>
<tr>
<td>SNMP</td>
<td>Configures SNMP attributes, SNMP admin user, and trap sinks.</td>
</tr>
<tr>
<td>Email Alerts</td>
<td>Configures the destination of email alerts and the recipients to be notified.</td>
</tr>
<tr>
<td>XML gateway</td>
<td>Provides an XML request-response protocol to get and set hardware management information.</td>
</tr>
<tr>
<td>Logs</td>
<td>Sets up system log files, remote log sinks, and log formats.</td>
</tr>
<tr>
<td>Configurations</td>
<td>Manages, activates, saves, and imports MLNX-OS SwitchX configuration files, and executes CLI commands.</td>
</tr>
<tr>
<td>Date and Time</td>
<td>Configures the date, time, and time zone of the switch system.</td>
</tr>
<tr>
<td>NTP</td>
<td>Configures NTP (Network Time Protocol) and NTP servers.</td>
</tr>
<tr>
<td>Licensing</td>
<td>Manages MLNX-OS licenses.</td>
</tr>
<tr>
<td>Modules</td>
<td>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.</td>
</tr>
<tr>
<td>Inventory</td>
<td>Displays a table with the following information about the system modules: module name, type, serial number, ordering part number and ASIC firmware version.</td>
</tr>
</tbody>
</table>
### 3.2.3 Security Menu

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

#### Table 17 - WebUI Security Submenus

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

### 3.2.4 Ports Menu

The Ports menu displays the port state and enables some configuration attributes of a selected port. It also enables modification of the port configuration. A graphical display of traffic over time (last hour or last day) through the port is also available.

#### Table 18 - WebUI Ports Submenus

<table>
<thead>
<tr>
<th>Submenu Title</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ports</td>
<td>Manages port attributes, counters, transceiver info and displays a graphical counters histogram.</td>
</tr>
<tr>
<td>Phy Profile</td>
<td>Provides the ability to manage phy profiles.</td>
</tr>
</tbody>
</table>
### 3.2.5 Status Menu

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

**Table 19 - WebUI Status Submenus**

<table>
<thead>
<tr>
<th>Submenu Title</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Summary</td>
<td>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.</td>
</tr>
<tr>
<td>Profile and Capabilities</td>
<td>Displays general information about the switch system capabilities such as the enabled profiles (e.g IB/ETH) and their corresponding values.</td>
</tr>
<tr>
<td>Temperature</td>
<td>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.</td>
</tr>
<tr>
<td>Power Supplies</td>
<td>Provides a graphical display of one of the switch’s power supplies voltage level over time (1 hour).</td>
</tr>
<tr>
<td>Fans</td>
<td>Provides a graphical display of fan speeds over time (1 hour). The display is per fan unit within a fan module.</td>
</tr>
<tr>
<td>CPU Load</td>
<td>Provides a graphical display of the management CPU load over time (1 hour).</td>
</tr>
<tr>
<td>Memory</td>
<td>Provides a graphical display of memory utilization over time (1 day).</td>
</tr>
<tr>
<td>Network</td>
<td>Provides a graphical display of network usage (transmitted and received packets) over time (1 day). It also provides per interface statistics.</td>
</tr>
<tr>
<td>Logs</td>
<td>Displays the system log messages. It is possible to display either the currently saved system log or a continuous system log.</td>
</tr>
<tr>
<td>Maintenance</td>
<td>Performs specific maintenance operations automatically on a predefined schedule.</td>
</tr>
<tr>
<td>Alerts</td>
<td>Displays a list of the recent health alerts and enables the user to configure health settings.</td>
</tr>
<tr>
<td>Virtualization</td>
<td>Displays the virtual machines, networks and volumes.</td>
</tr>
</tbody>
</table>
3.2.6 ETH Mgmt

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

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

3.2.7 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

<table>
<thead>
<tr>
<th>Submenu Title</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Router Global</td>
<td>Enables/disables IP Routing protocol on the machine.</td>
</tr>
<tr>
<td>IP Route</td>
<td>Not implemented.</td>
</tr>
<tr>
<td>IP Interface</td>
<td>Not implemented.</td>
</tr>
<tr>
<td>Address Resolution</td>
<td>Not implemented.</td>
</tr>
<tr>
<td>IP Diagnostic</td>
<td>Not implemented.</td>
</tr>
</tbody>
</table>
3.3 Secure Shell (SSH)

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

3.3.1 Adding a Host and Providing an SSH Key

➢ To add entries to the global known-hosts configuration file and its SSH value:

Step 1. Change to Config mode Run:

```plaintext
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:

```plaintext
switch [standalone: master] (config) # ssh client global known-host "myserver ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAQEAEXeXeklc8T0E6zmmMcVcfhveaYzIVq4rVsrERljmlJh4mYYTa8hGGiKN
a1t5xw2d9rnXhLYK51bUsSgJ2wZ11Dpme3pAeMY7G42mgGIW9xOuaXgAA3eBexEuJFdi6+1BqchWk0nTb+gM
fI/MK/heQNns7AtTrvqg/OSryIc="
switch [standalone: master] (config) #
```

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

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

SSH Global Known Hosts:
Entry 1: myserver

No SSH user identities configured.
No SSH authorized keys configured.

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

3.3.2 Retrieving Return Codes when Executing Remote Commands

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

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

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

```plaintext
ssh <username>@<hostname> cli -h """"enable"""" """"show interfaces brief"""
```
3.4 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](image)

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

**Table 22 - Module Type**

<table>
<thead>
<tr>
<th>Number</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Chassis</td>
</tr>
<tr>
<td>2</td>
<td>Management</td>
</tr>
<tr>
<td>3</td>
<td>Spine</td>
</tr>
<tr>
<td>4</td>
<td>Leaf</td>
</tr>
<tr>
<td>5</td>
<td>Fan</td>
</tr>
<tr>
<td>6</td>
<td>Power supply</td>
</tr>
<tr>
<td>7</td>
<td>BBU</td>
</tr>
<tr>
<td>8</td>
<td>x86 CPU</td>
</tr>
<tr>
<td>9</td>
<td>Port module</td>
</tr>
</tbody>
</table>

**Table 23 - Device Type**

<table>
<thead>
<tr>
<th>Number</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>01</td>
<td>PS</td>
</tr>
<tr>
<td>02</td>
<td>FAN</td>
</tr>
<tr>
<td>03</td>
<td>BOARD_MONITOR</td>
</tr>
<tr>
<td>04</td>
<td>CPU_BOARD_MONITOR</td>
</tr>
</tbody>
</table>
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:
- “1913” indicates sensor index #1913

**Table 23 - Device Type**

<table>
<thead>
<tr>
<th>Number</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>05</td>
<td>SX</td>
</tr>
<tr>
<td>06</td>
<td>SIB</td>
</tr>
<tr>
<td>07</td>
<td>CPU_MEZZ_TEMP</td>
</tr>
<tr>
<td>08</td>
<td>CPU Package Sensor</td>
</tr>
<tr>
<td>09</td>
<td>CPU Core Sensor</td>
</tr>
<tr>
<td>10</td>
<td>SX_AMBIENT_TEMP</td>
</tr>
<tr>
<td>11</td>
<td>SX_MONITOR</td>
</tr>
<tr>
<td>12</td>
<td>AUX_IN_TMP_SNSR</td>
</tr>
<tr>
<td>13</td>
<td>AUX_OUT_TMP_SNSR</td>
</tr>
<tr>
<td>14</td>
<td>MAIN_IN_TMP_SNSR</td>
</tr>
<tr>
<td>15</td>
<td>MAIN_OUT_TMP_SNSR</td>
</tr>
<tr>
<td>16</td>
<td>CPU_MEZZ_TEMP</td>
</tr>
<tr>
<td>17</td>
<td>Controller</td>
</tr>
<tr>
<td>18</td>
<td>QSFP_TEMP</td>
</tr>
<tr>
<td>19</td>
<td>QSFP-ASIC</td>
</tr>
<tr>
<td>20</td>
<td>Board AMB temp</td>
</tr>
<tr>
<td>21</td>
<td>Ports AMB temp</td>
</tr>
<tr>
<td>22</td>
<td>Power monitor</td>
</tr>
<tr>
<td>23</td>
<td>PS_MONITOR</td>
</tr>
<tr>
<td>24</td>
<td>SWB AMB temp</td>
</tr>
<tr>
<td>25</td>
<td>PCIe-switch-temp</td>
</tr>
<tr>
<td>26</td>
<td>SPC</td>
</tr>
</tbody>
</table>

**Table 24 - Sensor Type**

<table>
<thead>
<tr>
<th>Number</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>t – temperature sensor</td>
</tr>
<tr>
<td>2</td>
<td>f – fan sensor</td>
</tr>
</tbody>
</table>

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.
3.5 Commands

3.5.1 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.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>N/A</td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Config</td>
</tr>
<tr>
<td>History</td>
<td>3.1.0000</td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
</tr>
</tbody>
</table>
| Example            | switch (config) # cli clear-history
                  | switch (config) # |
| Related Commands   | N/A         |
| Note               |             |
cli default

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

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

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>minutes</th>
<th>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.</th>
</tr>
</thead>
<tbody>
<tr>
<td>paging enable</td>
<td></td>
<td>Enables text viewing one screen at a time.</td>
</tr>
<tr>
<td>prefix-modes {enable</td>
<td>Configures the prefix modes feature of CLI.</td>
<td></td>
</tr>
<tr>
<td>show-config}</td>
<td></td>
<td>• “prefix-modes enable” enables prefix modes for current and all future sessions</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• “prefix-modes show-config” uses prefix modes in “show configuration” output for current and all future sessions</td>
</tr>
<tr>
<td>progress enable</td>
<td></td>
<td>Enables progress updates.</td>
</tr>
<tr>
<td>prompt confirm-reload</td>
<td></td>
<td>Prompts for confirmation before rebooting.</td>
</tr>
<tr>
<td>prompt confirm-reset</td>
<td></td>
<td>Prompts for confirmation before resetting to factory state.</td>
</tr>
<tr>
<td>prompt confirm-unsaved</td>
<td></td>
<td>Confirms whether or not to save unsaved changes before rebooting.</td>
</tr>
<tr>
<td>prompt empty-password</td>
<td></td>
<td>Prompts for a password if none is specified in a pseudo-URL for SCP.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Default</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuration Mode</td>
<td>Config</td>
</tr>
<tr>
<td>History</td>
<td>3.1.0000</td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
</tr>
</tbody>
</table>
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
```

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.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Number</th>
<th>Range: 3-60</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td></td>
<td>50 sessions</td>
</tr>
<tr>
<td>Configuration Mode</td>
<td></td>
<td>Config</td>
</tr>
<tr>
<td>History</td>
<td></td>
<td>3.5.0200</td>
</tr>
<tr>
<td>Role</td>
<td></td>
<td>admin</td>
</tr>
</tbody>
</table>
| Example            |        | switch (config) # cli max-sessions 40  
|                    |        | switch (config) # |
| Related Commands   |        | show terminal |
| Note               |        |             |
cli session

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

Configures default CLI options for all future sessions.
The no form of the command deletes or disables the CLI sessions.
<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>minutes</th>
<th>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.</th>
</tr>
</thead>
<tbody>
<tr>
<td>paging enable</td>
<td>Enable</td>
<td>Enables text viewing one screen at a time.</td>
</tr>
</tbody>
</table>
| prefix-modes enable        | prefix-modes show-config                                               | Configures the prefix modes feature of CLI.  
  * “prefix-modes enable” enables prefix modes for current and all future sessions  
  * “prefix-modes show-config” uses prefix modes in “show configuration” output for current and all future sessions |
| progress enable            | Enable                                                                  | Enables progress updates.                                                                                                                                                                |
| terminal length            | Set                                                                     | 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              | Set                                                                    | Sets the terminal type. Valid options are:  
  * ansi  
  * console  
  * dumb  
  * linux  
  * unknown  
  * vt52  
  * vt100  
  * vt102  
  * vt220  
  * vt320  
  * xterm |
| terminal width             | Set                                                                    | Sets the width of the terminal in characters. Valid range is 34-999.                                                                                                                      |
| x-display full <display>   | Set                                                                    | Specifies the display as a raw string, e.g local-host:0.0.                                                                                                                           |

<table>
<thead>
<tr>
<th>Default</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuration Mode</td>
<td>Config</td>
</tr>
<tr>
<td>History</td>
<td>3.1.0000</td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
</tr>
</tbody>
</table>
| Example    | switch (config) # cli session auto-logout  
switch (config) # |
<table>
<thead>
<tr>
<th>Related Commands</th>
<th>show terminal</th>
</tr>
</thead>
<tbody>
<tr>
<td>Note</td>
<td></td>
</tr>
</tbody>
</table>
## terminal

```
terminal {length <number of lines> | resize | type <terminal type> | width <number of characters>}
```

```
no terminal type
```

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

| Syntax Description | length | Sets the number of lines for this terminal
|                   | Range: 5-999 |
|                   | resize | Resizes the CLI terminal settings (to match with real terminal) |
|                   | type | Sets the terminal type. Possible values: ansi, console, dumb, linux, screen, vt52, vt100, vt102, vt220, xterm. |
|                   | width | Sets the width of this terminal in characters
|                   | Range: 34-999 |

| Default   | N/A               |

| Configuration Mode | Config         |

| History | 3.1.0000         |

| Role | admin          |

| Example | switch (config) # terminal length 500
|         | switch (config) # |

| Related Commands | show terminal |

**Note**
### terminal sysrq enable

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>terminal sysrq enable</td>
<td>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).</td>
</tr>
<tr>
<td>no terminal sysrq enable</td>
<td>Disable SysRq over the serial connection (RS232 or Console port).</td>
</tr>
</tbody>
</table>

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>N/A</th>
</tr>
</thead>
</table>

**Default**

<table>
<thead>
<tr>
<th>Default</th>
<th>Enabled</th>
</tr>
</thead>
</table>

**Configuration Mode**

<table>
<thead>
<tr>
<th>Configuration Mode</th>
<th>Config</th>
</tr>
</thead>
</table>

**History**

<table>
<thead>
<tr>
<th>History</th>
<th>3.4.3000</th>
</tr>
</thead>
</table>

**Role**

<table>
<thead>
<tr>
<th>Role</th>
<th>admin</th>
</tr>
</thead>
</table>

**Example**

```
switch (config) # terminal sysrq enable
switch (config) #
```

**Related Commands**

<table>
<thead>
<tr>
<th>Related Commands</th>
<th>show terminal</th>
</tr>
</thead>
</table>

**Note**

---

80 Mellanox Technologies Confidential  Rev 4.60
show cli

show cli

Displays the CLI configuration and status.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>N/A</td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Any Command Mode</td>
</tr>
<tr>
<td>History</td>
<td>3.1.0000</td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
</tr>
</tbody>
</table>

**Example**

```
switch (config) # show cli

CLI current session settings:
Maximum line size: 8192
Terminal width: 171 columns
Terminal length: 38 rows
Terminal type: xterm
X display setting: (none)
Auto-logout: disabled
Paging: enabled
Progress tracking: enabled
Prefix modes: disabled

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

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

**Related Commands**
cli default

**Note**
**show cli max-sessions**

*show cli max-sessions*

Displays maximum number of sessions.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>N/A</td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Any Command Mode</td>
</tr>
<tr>
<td>History</td>
<td>3.5.0200</td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
</tr>
</tbody>
</table>

**Example**

```
switch (config) # show cli max-sessions
Maximum number of CLI sessions: 50
switch (config) #
```

**Related Commands**

**Note**
**show cli num-sessions**

show cli num-sessions

Displays current number of sessions.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>N/A</td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Any Command Mode</td>
</tr>
<tr>
<td>History</td>
<td>3.5.0200</td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
</tr>
</tbody>
</table>

**Example**

switch (config) # show cli num-sessions
Current number of CLI sessions: 40
switch (config) #
### 3.5.2 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.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>string</td>
<td>Text string.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Default</th>
<th>“Mellanox MLNX-OS Switch Management”</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuration Mode</td>
<td>Config</td>
</tr>
<tr>
<td>History</td>
<td>3.1.0000</td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
</tr>
<tr>
<td>Example</td>
<td>switch (config) # banner login Example&lt;br&gt;switch (config) #</td>
</tr>
<tr>
<td>Related Commands</td>
<td>show banner</td>
</tr>
<tr>
<td>Note</td>
<td>If more than one word is used (there is a space) quotation marks should be added (i.e. “xxxx xxxx”).</td>
</tr>
</tbody>
</table>
### banner login-local

```bash
banner login-local <string>
no banner login-local
```

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

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>string</th>
<th>Text string.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>N/A</td>
<td></td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Config</td>
<td></td>
</tr>
<tr>
<td>History</td>
<td>3.1.0000</td>
<td></td>
</tr>
<tr>
<td></td>
<td>3.5.0200</td>
<td>Added no form of the command</td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
<td></td>
</tr>
<tr>
<td>Example</td>
<td>switch (config) # banner login-local Testing</td>
<td></td>
</tr>
<tr>
<td></td>
<td>switch (config) #</td>
<td></td>
</tr>
<tr>
<td>Related Commands</td>
<td>show banner</td>
<td></td>
</tr>
<tr>
<td>Note</td>
<td>• The login-local refers to the serial connection banner</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• If more than one word is used (there is a space) quotation marks should be added (i.e. “xxxx xxxx”).</td>
<td></td>
</tr>
</tbody>
</table>
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.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>string</th>
<th>Text string.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>N/A</td>
<td></td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Config</td>
<td></td>
</tr>
<tr>
<td>History</td>
<td>3.1.0000</td>
<td></td>
</tr>
<tr>
<td></td>
<td>3.5.0200</td>
<td>Added no form of the command</td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
<td></td>
</tr>
<tr>
<td>Example</td>
<td>switch (config) # banner login-remote Testing</td>
<td></td>
</tr>
<tr>
<td></td>
<td>switch (config) #</td>
<td></td>
</tr>
<tr>
<td>Related Commands</td>
<td>show banner</td>
<td></td>
</tr>
<tr>
<td>Note</td>
<td>• The login-remote refers to the SSH connections banner</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• If more than one word is used (there is a space) quotation marks should be added (i.e. “xxxx xxxx”).</td>
<td></td>
</tr>
</tbody>
</table>
**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.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>string</th>
<th>Text string.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>N/A</td>
<td></td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Config</td>
<td></td>
</tr>
<tr>
<td>History</td>
<td>3.5.0200</td>
<td></td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
<td></td>
</tr>
</tbody>
</table>
| Example            | switch (config) # banner logout Testing
switch (config) # |
| Related Commands   | show banner |            |
| Note               | If more than one word is used (there is a space) quotation marks should be added (i.e. “xxxx xxxx”). |
**banner logout-local**

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

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

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>string</th>
<th>Text string.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>N/A</td>
<td></td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Config</td>
<td></td>
</tr>
<tr>
<td>History</td>
<td>3.5.0200</td>
<td></td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
<td></td>
</tr>
</tbody>
</table>

**Example**

```
switch (config) # banner logout-local Testing
switch (config) #
```

**Related Commands**

```
show banner
```

**Note**

- The logout-local refers to the serial connection banner
- If more than one word is used (there is a space) quotation marks should be added (i.e. “xxxx xxxx”).
**banner logout-remote**

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

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

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>string</th>
<th>Text string.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>N/A</td>
<td></td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Config</td>
<td></td>
</tr>
<tr>
<td>History</td>
<td>3.5.0200</td>
<td></td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
<td></td>
</tr>
</tbody>
</table>
| Example            | switch (config) # banner logout-remote Testing
                  | switch (config) # |
| Related Commands   | show banner |         |

**Note**
- The logout-remote refers to SSH connections banner
- If more than one word is used (there is a space) quotation marks should be added (i.e. “xxxx xxxx”).
banner motd

banner motd <string>
no banner motd

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

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>string</th>
<th>Text string</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>“Mellanox Switch”</td>
<td></td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Config</td>
<td></td>
</tr>
<tr>
<td>History</td>
<td>3.1.0000</td>
<td></td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
<td></td>
</tr>
<tr>
<td>Example</td>
<td>switch (config) # banner motd &quot;My Banner&quot;</td>
<td></td>
</tr>
<tr>
<td>Related Commands</td>
<td>show banner</td>
<td></td>
</tr>
</tbody>
</table>
| Note               | • If more than one word is used (there is a space) quotation marks should be added (i.e. “xxxx xxxx”).
• To insert a multi-line MotD, hit Ctrl-V (escape sequence) followed by Ctrl-J (new line sequence). The symbol “^J” should appear. Then, whatever is typed after it becomes the new line of the MotD. Remember to also include the string between quotation marks. |
## show banner

### Syntax Description

N/A

### Default

N/A

### Configuration Mode

Config

### History

3.1.0000

3.5.0200 Updated Example

### Role

Any Command Mode

### Example

```
switch (config) # show banner
Banners:
   Message of the Day (MOTD):
   Mellanox Switch

   Login:
   Mellanox MLNX-OS Switch Management

   Logout:
   Goodbye
switch (config) #
```

### Related Commands

- `banner login`
- `banner login-local`
- `banner login-remote`
- `banner logout`
- `banner logout-local`
- `banner logout-remote`
- `banner motd`

### Note
### 3.5.3 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.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>SSH server is enabled</td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Config</td>
</tr>
<tr>
<td>History</td>
<td>3.1.0000</td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
</tr>
</tbody>
</table>

**Example**

```
switch (config) # ssh server enable
switch (config) # show ssh server
SSH server configuration:
  SSH server enabled: yes
  Server security strict mode: no
  Minimum protocol version: 2
  TCP forwarding enabled: yes
  X11 forwarding enabled: no
  SSH server ports: 22

  Interface listen enabled: yes
  No Listen Interfaces.

Host Key Finger Prints:
  RSA v1 host key: SHA256:ElFoK7Jts?ejIws0Jgs3yt46goOClkn0JzAGx0ue4 (2048)
  RSA v2 host key: SHA256:N4n+Un/1ErjtzmmDJH+qcdsmHgHcOit1YArFggP+UFl (2048)
  DSA v2 host key: SHA256:2rIuzmFD90ANqoQaEjI1SH5EF0Dj9DDSTaAMrZDFC4 (1024)
```

**Related Commands**

show ssh server

**Note**

Disabling SSH server does not terminate existing SSH sessions, it only prevents new ones from being established.
### ssh server host-key

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

Manipulates host keys for SSH.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>key-type</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• rsa1 - RSAv1</td>
</tr>
<tr>
<td></td>
<td>• rsa2 - RSAv2</td>
</tr>
<tr>
<td></td>
<td>• dsa2 - DSAv2</td>
</tr>
</tbody>
</table>

| private-key | Sets new private-key for the host keys of the specified type. |
| public-key  | Sets new public-key for the host keys of the specified type. |
| generate    | Generates new RSA and DSA host keys for SSH. |

| Default       | SSH keys are locally generated |
| Configuration Mode | Config |
| History       | 3.1.0000 |
|               | 3.4.2300 Added notes |
| Role          | admin |
Example

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

SSH server configuration:
  SSH server enabled:       yes
  Minimum protocol version: 2
  X11 forwarding enabled:   no
  SSH server ports:         22
  Interface listen enabled: yes
  No Listen Interfaces.

Host Key Finger Prints:

Name: SWITCH-5E8A38 1024 35
1245749799537401010549141686791998797677682016984375942831915584962796
993754065696858042722190424505456958705866658144854493132172365068789517
1357059420864369513833467001453542694677583792888489624165303724512
160918999830386157103621938557797859628221464453344413712105268654198
30229882225076029771297093*

RSA v2 host key: "switch-5ea5d8 ssh-rsa AAAAB3NzaC1yc2EAAAQIBAAAQEA-
  IEAEB915OnukAHNlOotCPmEn30m88k7f4Uqk+4f5faSn+50pYxrceuZeyuzXsoZ1fFTK2-
  FydwYoVmvOSKc2PuCPrPZV/GYd31QEnn22rEmr1PrKCrn11lxUy6DF1r3ogWM1baomDLG/gSizWz/gc4Jgfq2CyX-
  Fq4pza61j1arV="

DSA v2 host key: "switch-5e5d8 ssh-dss AAAAB3NzaC1kz3MAAC-BAMe3JS+n7yHhRbwv3tJgLlWtD35RZV5C54G4EwMMp28VL94OccyuGu39VCDMq9pEva17h
  z3rzgfrNqakb/Y7d/anGh3wip19Fx81fe0Rh3b4oJzG+mW85momboPCRwE6X1KABKE00-
  jLz1XnpxP0lXkjzwjF+TbR3dKSHVwZyYw/bAAAAPQoCBoqBPZza4+ky1KlZubabZ2qkhoGAAAA-
  IAJK+iStIQd0Rw15Cm2zr7e5l07DsFveXEsYTTrUb8tQVShFQpXYVdH49QdS9TfCM
  3VO35uHUG1TMDIX7+9mfbB87yyUu5a/ndb3GhnHnxHwzB2e19hqgL7FSHA7D9Y7BvoZ-
  RlqKHe4QkGqzYips/FE331ly7GC4EQAAARl/Os1H1p2fxvNRjlgfmRsRVVv/mgEO9vc9/
  AMUklJn5Chat55C2pwoC1LxLM0ojh03jW3b1czGxRObDA9vUbKXTNc8bkg0UxySAH1rH
  N0Pq7qTeT4L009AiTSp3m1mxHqds7jixTvO7EKKXrgczDmTB8+zjhUah/YuUbl2H
  g="
```

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

**Syntax**

```
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.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>enable</th>
<th>Enables SSH interface restrictions on access to this system.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>interface &lt;inf&gt;</td>
<td>Adds interface to SSH server access restriction list. Possible interfaces are “lo”, and “mgmt0”.</td>
</tr>
</tbody>
</table>

**Default**

SSH listen is enabled

**Configuration Mode**

Config

**History**

3.1.0000

**Role**

admin

**Example**

```
switch (config) # ssh server listen enable
switch (config) # show ssh server
SSH server configuration:
    SSH server enabled: yes
    Minimum protocol version: 2
    X11 forwarding enabled: no
    SSH server ports:  22

    Interface listen enabled: yes
    No Listen Interfaces.

Host Key Finger Prints:
switch (config) #
```

**Related Commands**

show ssh server

**Note**
ssh server login attempts

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

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

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

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

**Note**
### ssh server min-version

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

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

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>version</th>
<th>Possible versions are 1 and 2.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Config</td>
<td></td>
</tr>
<tr>
<td>History</td>
<td>3.1.0000</td>
<td></td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
<td></td>
</tr>
</tbody>
</table>

**Example**

```
switch (config) # ssh server min-version 2
switch (config) # show ssh server
SSH server configuration:
    SSH server enabled:       yes
    Minimum protocol version: 2
    X11 forwarding enabled:   no
    SSH server ports:         22

    Interface listen enabled: yes
    No Listen Interfaces.

    Host Key Finger Prints:
```

**Related Commands**  
show ssh server

**Note**
ssh server ports

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

Specifies which ports the SSH server listens on.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port number in [1...65535].</td>
<td>port</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Default</th>
<th>22</th>
</tr>
</thead>
</table>

**Configuration Mode**

Config

**History**

3.1.0000

**Role**

admin

**Example**

```
switch (config) # ssh server ports 22
switch (config) # show ssh server
SSH server configuration:
  SSH server enabled:       yes
  Minimum protocol version: 2
  X11 forwarding enabled:   no
  SSH server ports:         22
  Interface listen enabled: yes
  No Listen Interfaces.

Host Key Finger Prints:
```

**Related Commands**

show ssh server

**Note**

- Multiple ports can be specified by repeating the `<port>` parameter
- The command will remove any previous ports if not listed in the command
### ssh server security strict

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

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>N/A</td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Config</td>
</tr>
<tr>
<td>History</td>
<td>3.3.5060</td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
</tr>
</tbody>
</table>

#### Example

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

#### Related Commands

- show ssh server

#### Note

The following ciphers are disabled for SSH when strict security is enabled:
- aes256-cbc
- aes192-cbc
- aes128-cbc
- arcfour
- blowfish-cbc
- cast128-cbc
- rijndael-cbc@lysator.liu.se
**ssh server tcp-forwarding enable**

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

<table>
<thead>
<tr>
<th><strong>Syntax Description</strong></th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Default</strong></td>
<td>N/A</td>
</tr>
<tr>
<td><strong>Configuration Mode</strong></td>
<td>Config</td>
</tr>
<tr>
<td><strong>History</strong></td>
<td>3.1.0000</td>
</tr>
<tr>
<td><strong>Role</strong></td>
<td>admin</td>
</tr>
</tbody>
</table>
| **Example**            | switch (config) # ssh server tcp-forwarding enable  
                        | switch (config) # |
| **Related Commands**   | show ssh server |
| **Note**               | |


ssh server x11-forwarding

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

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

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>X11-forwarding is disabled.</td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Config</td>
</tr>
<tr>
<td>History</td>
<td>3.1.0000</td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
</tr>
</tbody>
</table>

**Example**

```
switch (config) # ssh server x11-forwarding enable
switch (config) # show ssh server
SSH server configuration:
    SSH server enabled:       yes
    Minimum protocol version: 2
    X11 forwarding enabled:   yes
    SSH server ports:         22

    Interface listen enabled: yes
    No Listen Interfaces.

Host Key Finger Prints:
```

**Related Commands**

N/A

**Note**
### ssh client global

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

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

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

**Default**

host-key-check - ask, no keys are configured by default

**Configuration Mode**

Config

**History**

3.1.0000

**Role**

admin
Example

switch (config) # ssh client global host-key-check no
switch (config) # ssh client global known-host "72.30.2.2 ssh-rsa
AAAAAB3NzaC1yc2EAAAABAIAwAAAIAEArB9i5OnuAKHNU0kwpCmE10m88kJqB-
zL22+p5tfa5n+S0pVYxrvceZeyuZxsoZ1VtFTK2Fydwy8YvMS0Kcv2PuCrFPZV/
GYd3lQEnn22rEmrlPrKCrM11XlUY6DFr30gwWm1baobmD1G/gSizWz/gc4Jgqf2CyX-
Fq4pzaR1jar1Vk="

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

No SSH user identities configured.
No SSH authorized keys configured.

Related Commands

show ssh client

Note
ssh client user

```bash
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.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>username</td>
<td>The specified user must be a valid account on the system. Possible values for this parameter are “admin”, “monitor”, “xmladmin”, and “xmluser”.</td>
</tr>
<tr>
<td>authorized-key sshv2 &lt;public key&gt;</td>
<td>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.</td>
</tr>
<tr>
<td>identity &lt;key type&gt;</td>
<td>Sets certain SSH client identity settings for a user, dsa2 or rsa2.</td>
</tr>
<tr>
<td>generate</td>
<td>Generates SSH client identity keys for specified user.</td>
</tr>
<tr>
<td>private-key</td>
<td>Sets private key SSH client identity settings for the user.</td>
</tr>
<tr>
<td>public-key</td>
<td>Sets public key SSH client identity settings for the user.</td>
</tr>
<tr>
<td>known-host &lt;known host&gt; remove</td>
<td>Removes host from user's known host file.</td>
</tr>
</tbody>
</table>

**Default**
No keys are created by default

**Configuration Mode**
Config

**History**
3.1.0000

**Role**
admin

**Example**
```
switch (config) # ssh client user admin known-host 172.30.1.116 remove
switch (config) #
```
<table>
<thead>
<tr>
<th>Related Commands</th>
<th>show ssh client</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Note</strong></td>
<td>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.</td>
</tr>
</tbody>
</table>
**slogin**

*slogin [slogin options] <hostname>*

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

**Syntax Description**

```
```

**Default**

N/A

**Configuration Mode**

Config

**History**

3.1.0000

**Role**

monitor/admin

**Example**

```bash
switch (config) # slogin 192.168.10.70
The authenticity of host '192.168.10.70 (192.168.10.70)' can't be established.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.168.10.70' (RSA) to the list of known hosts.

Mellanox MLNX-OS Switch Management

Last login: Sat Feb 28 22:55:17 2009 from 10.208.0.121

Mellanox Switch

switch (config) #
```

**Related Commands**

N/A

**Note**

N/A
### show ssh client

Displays the client configuration of the SSH server.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>N/A</td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Config</td>
</tr>
<tr>
<td>History</td>
<td>3.1.0000</td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
</tr>
</tbody>
</table>

#### Example

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

SSH Global Known Hosts:
  Entry 1: 72.30.2.2

No SSH user identities configured.
No SSH authorized keys configured.
```

#### Related Commands

N/A

#### Note
show ssh server

Displays SSH server configuration.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>N/A</td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Config</td>
</tr>
<tr>
<td>History</td>
<td>3.1.0000</td>
</tr>
<tr>
<td></td>
<td>3.4.0000 Updated Example</td>
</tr>
<tr>
<td></td>
<td>3.5.0200 Added SSH login timeout and max attempts</td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
</tr>
</tbody>
</table>
| Example            | switch (config) # show ssh server
SSH server configuration:
  SSH server enabled: yes
  Server security strict mode: no
  Minimum protocol version: 2
  TCP forwarding enabled: yes
  X11 forwarding enabled: no
  SSH login timeout: 120
  SSH login max attempts: 6
  SSH server ports: 22
  Interface listen enabled: yes
  No Listen Interfaces.
  Host Key Finger Prints and Key Lengths:
  RSA v2 host key: 15:e2:a8:45:1c:58:1b:00:cc:29:ec:00:38:83:49:00 (2048)

switch (config) #

Related Commands ssh server

Note
### 3.5.4 Remote Login

#### telnet

Logs into another system using telnet.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>N/A</td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Config</td>
</tr>
<tr>
<td>History</td>
<td>3.1.0000</td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
</tr>
</tbody>
</table>

**Example**

```
switch (config) # (config) # telnet
telnet>
```

**Related Commands**
telnet-server

**Note**
## telnet-server enable

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

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

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>Telnet server is disabled</td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Config</td>
</tr>
<tr>
<td>History</td>
<td>3.1.0000</td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
</tr>
</tbody>
</table>

### Example

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

### Related Commands

`show telnet-server`

### Note
**show telnet-server**

`show telnet-server` displays telnet server settings.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>N/A</td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Config</td>
</tr>
<tr>
<td>History</td>
<td>3.1.0000</td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
</tr>
</tbody>
</table>
| Example            | `switch (config) # show telnet-server`  
Telnet server enabled: yes  
switch (config) # |
| Related Commands   | telnet-server enable |
| Note               | |

**Note**
3.5.5 Web Interface

**web auto-log-out**

```bash
web auto-log-out <number of minutes>
nol web auto-log-out <number of minutes>
```

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

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>number of minutes</th>
<th>The length of user inactivity in minutes. 0 will disable the inactivity timer (same as a “no web auto-log-out” command).</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>60 minutes</td>
<td></td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Config</td>
<td></td>
</tr>
<tr>
<td>History</td>
<td>3.1.0000</td>
<td></td>
</tr>
<tr>
<td></td>
<td>3.4.0000</td>
<td>Updated Example</td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
<td></td>
</tr>
<tr>
<td>Example</td>
<td>switch (config) # web auto-log-out 60</td>
<td>switch (config) # show web</td>
</tr>
</tbody>
</table>

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) #
<table>
<thead>
<tr>
<th>Related Commands</th>
<th>show web</th>
</tr>
</thead>
<tbody>
<tr>
<td>Note</td>
<td>The no form of the command does not automatically log users out due to inactivity.</td>
</tr>
</tbody>
</table>
web cache-enable

 command:

```
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.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>Enabled</td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Config</td>
</tr>
<tr>
<td>History</td>
<td>3.4.1100</td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
</tr>
<tr>
<td>Example</td>
<td>switch (config) # no web cache-enable</td>
</tr>
<tr>
<td>Related Commands</td>
<td>N/A</td>
</tr>
<tr>
<td>Note</td>
<td></td>
</tr>
</tbody>
</table>
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.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>N/A</td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Config</td>
</tr>
<tr>
<td>History</td>
<td>3.2.3000</td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
</tr>
<tr>
<td>Example</td>
<td>switch (config) # web client cert-verify</td>
</tr>
<tr>
<td>Related Commands</td>
<td>N/A</td>
</tr>
<tr>
<td>Note</td>
<td></td>
</tr>
</tbody>
</table>
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.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>enable</td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Config</td>
</tr>
<tr>
<td>History</td>
<td>3.1.0000</td>
</tr>
<tr>
<td></td>
<td>3.4.0000 Updated Example</td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
</tr>
</tbody>
</table>
| Example            | switch (config) # web enable
switch (config) # show web

Web User Interface:
Web interface enabled: yes
HTTP enabled: yes
HTTP port: 80
HTTP redirect to HTTPS: no
HTTPS enabled: yes
HTTPS port: 443
HTTPS ssl-ciphers: all
HTTPS certificate name: default-cert
Listen enabled: yes
No Listen Interfaces.
Inactivity timeout: 1 hr
Session timeout: 2 hr 30 min
Session renewal: 30 min

Web file transfer proxy:
Proxy enabled: no

Web file transfer certificate authority:
HTTPS server cert verify: yes
HTTPS supplemental CA list: default-ca-list

switch (config) #

Related Commands | show web |

Note
**web http**

web http {enable | port <port number> | redirect}
no web http {enable | port | redirect}

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

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>enable</th>
<th>port number</th>
<th>redirect</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Enables HTTP access to the web-based management console.</td>
<td>Sets a port for HTTP access.</td>
<td>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.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Default</th>
<th>HTTP is enabled</th>
<th>HTTP TCP port is 80</th>
<th>HTTP redirect to HTTPS is disabled</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Configuration Mode</th>
<th>Config</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>History</th>
<th>3.1.0000</th>
<th>3.4.0000</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Role</th>
<th>admin</th>
</tr>
</thead>
</table>
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

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.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>Enables Web interface restrictions on access to this system.</td>
</tr>
<tr>
<td>interface &lt;ifName&gt;</td>
<td>Adds interface to Web server access restriction list (i.e. mgmt0, mgmt1)</td>
</tr>
</tbody>
</table>

**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) #
```
<table>
<thead>
<tr>
<th>Related Commands</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Note</strong></td>
<td>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.</td>
</tr>
</tbody>
</table>
**web https**

```bash
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.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th></th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>certificate regenerate</td>
<td></td>
<td>Re-generates certificate to use for HTTPS connections.</td>
</tr>
<tr>
<td>certificate name</td>
<td></td>
<td>Configure the named certificate to be used for HTTPS connections</td>
</tr>
<tr>
<td>certificate default-cert</td>
<td></td>
<td>Configure HTTPS to use the configured default certificate</td>
</tr>
<tr>
<td>enable</td>
<td></td>
<td>Enables HTTPS access to the web-based management console.</td>
</tr>
<tr>
<td>port</td>
<td></td>
<td>Sets a TCP port for HTTPS access.</td>
</tr>
<tr>
<td>ssl ciphers {all</td>
<td>TLS</td>
<td>TLS1.2}</td>
</tr>
</tbody>
</table>

**Default**

HTTPS is enabled  
Default port is 443

**Configuration Mode**  
Config

**History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.1.0000</td>
<td></td>
</tr>
<tr>
<td>3.4.0000</td>
<td>Added “ssl ciphers” parameter</td>
</tr>
<tr>
<td>3.4.0010</td>
<td>Added TLS parameter to “ssl ciphers”</td>
</tr>
</tbody>
</table>

**Role**

admin
Example

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

Web User Interface:
  Web interface enabled: yes
  HTTP enabled: yes
  HTTP port: 80
  HTTP redirect to HTTPS: no
  HTTPS enabled: yes
  HTTPS port: 443
  HTTPS ssl-ciphers: all
  HTTPS certificate name: default-cert
  Listen enabled: yes
No Listen Interfaces.
  Inactivity timeout: 1 hr
  Session timeout: 2 hr 30 min
  Session renewal: 30 min

Web file transfer proxy:
  Proxy enabled: no

Web file transfer certificate authority:
  HTTPS server cert verify: yes
  HTTPS supplemental CA list: default-ca-list
```

Related Commands

```
show web
web enable
```

Note

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

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

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

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>renewal &lt;minutes&gt;</th>
<th>Configures time before expiration to renew a session.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>timeout &lt;minutes&gt;</td>
<td>Configures time after which a session expires.</td>
</tr>
</tbody>
</table>

**Default**
- timeout - 2.5 hours
- renewal - 30 min

**Configuration Mode**
- Config

**History**
- 3.1.0000

**Role**
- admin

**Example**
```text
switch (config) # web session renewal 60
switch (config) # show web
```

Web User Interface:
- Web interface enabled: yes
- HTTP enabled: yes
- HTTP port: 80
- HTTP redirect to HTTPS: no
- HTTPS enabled: yes
- HTTPS port: 443
- HTTPS ssl-ciphers: all
- HTTPS certificate name: default-cert
- Listen enabled: yes
- Inactivity timeout: 1 hr
- Session timeout: 2 hr 30 min
- Session renewal: 60 min

Web file transfer proxy:
- Proxy enabled: no

Web file transfer certificate authority:
- HTTPS server cert verify: yes
- HTTPS supplemental CA list: default-ca-list

**Related Commands**
- N/A

**Note**
# web proxy auth

```
web proxy auth {authtype <type>| basic [password <password> | username <username>]
no web proxy auth {authtype | basic {password | username }
```

Configures authentication settings for web proxy authentication. The no form of the command resets the attributes to their default values.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
</table>
| type               | Configures the type of authentication to use with web proxy. The possible values are:  
  • basic - HTTP basic authentication  
  • none - No authentication |
| basic              | Configures HTTP basic authentication settings for proxy. The password is accepted and stored in plaintext. |
| password           | A password used for HTTP basic authentication with the web proxy. |
| username           | A username used for HTTP basic authentication with the web proxy. |

**Default**  
Web proxy is disabled.

**Configuration Mode**  
Config

**History**  
3.1.0000

**Role**  
admin
Example

```
switch (config) # web proxy auth authtype basic
switch (config) # web proxy auth basic username web-user
switch (config) # web proxy auth basic password web-password
switch (config) # show web
```

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

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

Web file transfer proxy:
- Proxy enabled: yes
- Proxy address: 10.10.10.11
- Proxy port: 40
- Authentication type: basic
- Basic auth username: web-user
- Basic auth password: web-password

Web file transfer certificate authority:
- HTTPS server cert verify: yes
- HTTPS supplemental CA list: default-ca-list

```
switch (config) #
```

Related Commands

- show web
- web proxy host

Note
web proxy host

web proxy host <IP address> [port <port number>]
no web proxy

Adds and enables a proxy to be used for any HTTP or FTP downloads. The no form of the command disables the web proxy.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>IP address</th>
<th>IPv4 or IPv6 address.</th>
</tr>
</thead>
<tbody>
<tr>
<td>port number</td>
<td></td>
<td>Sets the web proxy default port.</td>
</tr>
</tbody>
</table>

Default

1080

Configuration Mode

Config

History

3.1.0000

Role

admin

Example

switch (config) # web proxy host 10.10.10.10 port 1080
switch (config) # show web

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

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

Web file transfer proxy:
- Proxy enabled: yes
- Proxy address: 10.10.10.10
- Proxy port: 1080
- Authentication type: basic
- Basic auth username: web-user
- Basic auth password: web-password

Web file transfer certificate authority:
- HTTPS server cert verify: yes
- HTTPS supplemental CA list: default-ca-list

Related Commands

web proxy auth

Note
show web

show web

Displays the web configuration.

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>N/A</th>
</tr>
</thead>
</table>

**Default**

<table>
<thead>
<tr>
<th>Default</th>
<th>N/A</th>
</tr>
</thead>
</table>

**Configuration Mode**

<table>
<thead>
<tr>
<th>Configuration Mode</th>
<th>Config</th>
</tr>
</thead>
</table>

**History**

<table>
<thead>
<tr>
<th>History</th>
<th>3.1.0000</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.4.0000</td>
<td>Updated Example</td>
</tr>
<tr>
<td>3.4.1100</td>
<td>Updated Example</td>
</tr>
</tbody>
</table>

**Role**

<table>
<thead>
<tr>
<th>Role</th>
<th>admin</th>
</tr>
</thead>
</table>

**Example**

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

**Web User Interface:**

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

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

**Web file transfer proxy:**

- Proxy enabled: yes
- Proxy address: 10.10.10.11
- Proxy port: 40
- Authentication type: basic
- Basic auth username: web-user
- Basic auth password: web-password

Web file transfer certificate authority:

- HTTPS server cert verify: yes
- HTTPS supplemental CA list: default-ca-list

```
switch (config) #
```

**Related Commands**

- show web
- web proxy auth

**Note**
4 System Management

4.1 Management Interface

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.

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

In such case the serial connection should be used.

4.1.4 Default Gateway

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

```bash
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:

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

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

**Step 4.** (Optional) Verify in-band management configuration. Run:
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 enabled by default and will change the switch hostname if the hostname is not set by the user. Therefore, if a switch is part of an HA cluster (e.g.) 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.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>mgmt0</td>
<td>Management port 0 (out of band).</td>
</tr>
<tr>
<td>mgmt1</td>
<td>Management port 1 (out of band).</td>
</tr>
<tr>
<td>lo</td>
<td>Loopback interface.</td>
</tr>
<tr>
<td>vlan&lt;id&gt;</td>
<td>In-band management interface (e.g. vlan10).</td>
</tr>
</tbody>
</table>

**Default**

N/A

**Configuration Mode**

Config

**History**

3.1.0000

**Role**

admin

**Example**

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

**Related Commands**

```
show interfaces <ifname>
```

**Notes**
ip address

**ip address** `<IP address>` `<netmask>`

**no ip address**

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

**Syntax Description**

<table>
<thead>
<tr>
<th>IP address</th>
<th>IPv4 address</th>
</tr>
</thead>
<tbody>
<tr>
<td>netmask</td>
<td>Subnet mask of IP address</td>
</tr>
</tbody>
</table>

**Default**

0.0.0.0/0

**Configuration Mode**

Config Interface Management

**History**

3.1.0000

**Role**

admin

**Example**

```
switch (config) # interface mgmt0
switch (config interface mgmt0) # ip address 10.10.10.10 255.255.255.0
switch (config interface mgmt0) # show interfaces mgmt0
```

Interface mgmt0 state

- Admin up: yes
- Link up: yes
- IP address: 10.10.10.10
- Netmask: 255.255.255.0
- IPv6 enabled: yes
- Autoconf enabled: no
- Autoconf route: yes
- Autoconf privacy: no
- IPv6 addresses: 1
- IPv6 address: fe80:202:c9ff:fe5e:a5d8/64
- Speed: 1000M/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
RX queue len: 1000

switch (config interface mgmt0) #
<table>
<thead>
<tr>
<th>Related Commands</th>
<th>show interfaces &lt;ifname&gt;</th>
</tr>
</thead>
<tbody>
<tr>
<td>Notes</td>
<td>If DHCP is enabled on the specified interface, then the DHCP IP assignment will hold until DHCP is disabled.</td>
</tr>
</tbody>
</table>
**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.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>next hop IP address or interface name</td>
<td>IP address, lo, mgmt0, or mgmt1.</td>
</tr>
</tbody>
</table>

| Default | N/A |
| Configuration Mode | Config Interface Management |
| History | 3.1.0000 |
| Role | admin |

**Example**

```
switch (config) # ip default-gateway mgmt1
switch (config) #
```

**Related Commands**

**Notes**
**alias**

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

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

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>index</th>
<th>A number that is to be aliased to (associated with) the secondary IP.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>IP address</td>
<td>Additional IP address.</td>
</tr>
<tr>
<td></td>
<td>netmask</td>
<td>Subnet mask of the IP address.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Default</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuration Mode</td>
<td>Config Interface Management</td>
</tr>
<tr>
<td>History</td>
<td>3.1.0000</td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
</tr>
</tbody>
</table>
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
  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.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>bytes</th>
<th>The entry range is 68-1500.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>1500</td>
<td></td>
</tr>
</tbody>
</table>

**Configuration Mode**

Config Interface Management

**History**

3.6.3004

**Role**

admin

**Example**

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

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

switch (config interface mgmt0) #

**Related Commands**

show interfaces <ifname>

**Notes**
**duplex**

```plaintext
duplex <duplex>
no duplex
```

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

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
</table>
| duplex  | Sets the duplex mode of the interface. The following are the possible values:  
- half - half duplex  
- full - full duplex  
- auto - auto duplex sensing (half or full) |

**Default**

auto

**Configuration Mode**

Config Interface Management

**History**

3.1.0000

**Role**

admin

**Example**

```
switch (config interface mgmt0) # duplex auto
switch (config interface mgmt0) # show interfaces mgmt0
Interface mgmt0 state
  Admin up: yes
  Link up: yes
  IP address: 172.30.2.2
  Netmask: 255.255.0.0
  Secondary address: 9.9.9.9/32 (alias: 'mgmt0:2')
  IPv6 enabled: yes
  Autoconf enabled: no
  Autoconf route: yes
  Autoconf privacy: no
  IPv6 addresses: 1
  IPv6 address: fe80::202:c9ff:fe5e:a5d8/64
  Speed: 1000Mb/s (auto)
  Duplex: full (auto)
  Interface type: ethernet
  Interface ifindex: 2
  Interface source: physical
  MTU: 1500
  HW address: 00:02:C9:5E:A5:D8
  RX bytes: 2970074221
  TX bytes: 468579522
  RX packets: 44983023
  TX packets: 1390539
  RX mcast packets: 0
  TX discards: 0
  RX discards: 0
  TX errors: 0
  RX errors: 0
  TX overruns: 0
  RX overruns: 0
  TX carrier: 0
  RX frame: 0
  TX collisions: 0
  TX queue len: 1000
```

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


**Related Commands**

```
show interfaces <ifname>
```

**Notes**

- Setting the duplex to “auto” also sets the speed to “auto”
- Setting the duplex to one of the settings “half” or “full” also sets the speed to a manual setting which is determined by querying the interface to find out its current auto-detected state
speed

speed <speed>
no speed

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

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>speed</td>
<td>Sets the speed of the interface. The following are the possible values:</td>
</tr>
<tr>
<td></td>
<td>• 10 - fixed to 10Mbps</td>
</tr>
<tr>
<td></td>
<td>• 100 - fixed to 1000Mbps</td>
</tr>
<tr>
<td></td>
<td>• 1000 - fixed to 1000Mbps</td>
</tr>
<tr>
<td></td>
<td>• auto - auto speed sensing (10/100/1000Mbps)</td>
</tr>
</tbody>
</table>

**Default**

auto

**Configuration Mode**

Config Interface Management

**History**

3.1.0000

**Role**

admin

**Example**

switch (config interface mgmt0) # speed auto
switch (config interface mgmt0) # show interfaces mgmt0
Interface mgmt0 state
  Admin up: yes
  Link up: yes
  IP address: 172.30.2.2
  Netmask: 255.255.0.0
  Secondary address: 9.9.9.92 (alias: 'mgmt0:2')
  IPv6 enabled: yes
  Autoconf enabled: no
  Autoconf route: yes
  Autoconf privacy: no
  IPv6 addresses: 1
  IPv6 address: fe80::202:9ff:fe56:a5d8/64
  Speed: 1000Mb/s (auto)
  Duplex: full (auto)
  Interface type: ethernet
  Interface ifindex: 2
  Interface source: physical
  MTU: 1500
  HW address: 00:02:C9:5E:A5:D8
  Comment:
    RX bytes: 2970074221 TX bytes: 468579522
    RX packets: 44983023 TX packets: 1390539
    RX mcast packets: 0 TX discards: 0
    RX discards: 0 TX errors: 0
    RX errors: 0 TX overruns: 0
    RX overruns: 0 TX carrier: 0
    RX frame: 0 TX collisions: 0
    TX queue len: 1000

switch (config interface mgmt0) #
Related Commands

```
show interfaces <ifname>
```

Notes

- Setting the speed to “auto” also sets the duplex to “auto”
- Setting the speed to one of the manual settings (generally “10”, “100”, or “1000”) also sets the duplex to a manual setting which is determined by querying the interface to find out its current auto-detected state
**dhcp**

```bash
dhcp [renew]
no dhcp
```

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

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>renew</td>
<td>Forces a renewal of the IP address. A restart on the DHCP client for the specified interface will be issued.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Default</th>
<th>Could be enabled or disabled (per part number) manufactured with 3.2.0500</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Configuration Mode</th>
<th>Config Interface Management</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>History</th>
<th>3.1.0000</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Role</th>
<th>admin</th>
</tr>
</thead>
</table>

**Example**

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

**Related Commands**

- show interfaces <ifname> configured

**Notes**

- When enabling DHCP, the IP address and netmask are received via DHCP hence, the static IP address configuration is ignored.
- Enabling DHCP disables zeroconf and vice versa.
- Setting a static IP address and netmask does not disable DHCP. DHCP is disabled using the “no” form of this command, or by enabling zeroconf.
### dhcp hostname

**dhcp hostname**

**no dhcp hostname**

Enables fetching the hostname from DHCP for this interface. The no form of the command disables fetching the hostname from DHCP for this interface.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>Enabled</td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Config Interface Management</td>
</tr>
<tr>
<td>History</td>
<td>3.5.1000</td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
</tr>
</tbody>
</table>
| Example            | switch (config interface mgmt0) # dhcp hostname
switch (config interface mgmt0) # |
| Related Commands   | hostname <hostname>
show interfaces <ifname> configured |
| Notes              | • If a hostname is configured manually by the user, that configuration would override the “dhcp hostname” configuration
• After upgrading to version 3.5.1000 when a default hostname is not configured, the DHCP server assigns the new hostname for your machine
• These commands do not work on in-band interfaces |
**shutdown**

```
shutdown
no shutdown
```

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

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>no shutdown</td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Config Interface Management</td>
</tr>
<tr>
<td>History</td>
<td>3.1.0000</td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
</tr>
</tbody>
</table>

**Example**

```
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) #
```

**Related Commands**

`show interfaces <ifname> configured`

**Notes**
### zeroconf

**zeroconf**

**no zeroconf**

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

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

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>no zeroconf</td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Config Interface Management</td>
</tr>
<tr>
<td>History</td>
<td>3.1.0000</td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
</tr>
</tbody>
</table>

#### Example

```
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:
```

#### Related Commands

- `show interfaces <ifname> configured`

#### Notes

Enabling zeroconf disables DHCP and vice versa.
**comment**

**Syntax Description**

comment

A free-form string that has no semantics other than being displayed when the interface records are listed.

**Default**

no comment

**Configuration Mode**

Config Interface Management

**Example**

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

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

```
switch (config interface mgmt0) #
```
<table>
<thead>
<tr>
<th>Related Commands</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Notes</td>
<td></td>
</tr>
</tbody>
</table>
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.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>IPv6 addressing is disabled</td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Config Interface Management</td>
</tr>
<tr>
<td>History</td>
<td>3.1.0000</td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
</tr>
</tbody>
</table>

Example

```
switch (config interface mgmt0) # ipv6 enable
switch (config interface mgmt0) # show interfaces mgmt0
Interface mgmt0 state
    Admin up: yes
    Link up: yes
    IP address: 172.30.2.2
    Netmask: 255.255.0.0
    IPv6 enabled: yes
    Autoconf enabled: no
    Autoconf route: yes
    Autoconf privacy: no
    IPv6 addresses: 1
    IPv6 address: fe80::202:c9ff:fe5e:a5d8/64
    Speed: 1000Mb/s (auto)
    Duplex: full (auto)
    Interface type: ethernet
    Interface ifindex: 2
    Interface source: physical
    MTU: 1500
    HW address: 00:02:C9:5E:A5:D8
    Comment: my-interface
    RX bytes: 962067812
    TX bytes: 40658219
    RX packets: 3738865
    TX packets: 142345
    RX mcast packets: 0
    TX mcast packets: 0
    RX discards: 0
    TX discards: 0
    RX errors: 0
    TX errors: 0
    RX overruns: 0
    TX overruns: 0
    RX frame: 0
    TX carrier: 0
    RX collisions: 0
    TX collisions: 0
    RX queue len: 1000

switch (config interface mgmt0) #
```
**Related Commands**

- ipv6 address
- show interface <ifname>

**Notes**

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

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

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

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPv6 address/netmask</td>
<td>Configures a static IPv6 address and netmask. Format example: 2001:db8:1234::5678/64.</td>
</tr>
<tr>
<td>autoconfig</td>
<td>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.</td>
</tr>
<tr>
<td>autoconfig default</td>
<td>Enables default learning routes. The default route will be discovered automatically, if the autoconfig is enabled.</td>
</tr>
<tr>
<td>autoconfig privacy</td>
<td>Uses privacy extensions for SLAAC to construct the autoconfig address, if the autoconfig is enabled.</td>
</tr>
</tbody>
</table>

Default: No IP address available, auto config is enabled

Configuration Mode: Config Interface Management

History: 3.1.0000

Role: admin
Example

```
switch (config interface mgmt0) # ipv6 fe80::202:c9ff:fe5e:a5d8/64
switch (config interface mgmt0) # show interfaces mgmt0
```

Interface mgmt0 state
```
Admin up: yes
Link up: yes
IP address: 172.30.2.2
Netmask: 255.255.0.0
IPv6 enabled: yes
Autoconf enabled: no
Autoconf route: yes
Autoconf privacy: no
IPv6 addresses: 1
IPv6 address: fe80::202:c9ff:fe5e:a5d8/64
Speed: 1000Mb/s (auto)
Duplex: full (auto)
Interface type: ethernet
Interface ifindex: 2
Interface source: physical
MTU: 1500
HW address: 00:02:C9:5E:A5:D8
Comment: my-interface
RX bytes: 962067812 TX bytes: 40658219
RX packets: 3738865 TX packets: 142345
RX mcast packets: 0 TX discards: 0
RX discards: 0 TX errors: 0
RX errors: 0 TX overruns: 0
RX overruns: 0 TX carrier: 0
RX frame: 0 TX collisions: 0
TX queue len: 1000
```

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.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>if-name</th>
<th>Interface name:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>• lo</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• mgmt0</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• mgmt1</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Default</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuration Mode</td>
<td>Config</td>
</tr>
<tr>
<td>History</td>
<td>3.1.0000</td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
</tr>
</tbody>
</table>

#### Example

```bash
switch (config) # ipv6 dhcp primary-intf mgmt0
switch (config) #
```

#### Related Commands

- ipv6 enable
- ipv6 address
- show interface <ifname>

#### Notes
# ipv6 dhcp stateless

ipv6 dhcp stateless  
no ipv6 dhcp stateless

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

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

*show interface <ifname> brief*

Displays a brief info on the interface configuration and status.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>ifname</th>
<th>The interface name e.g., “mgmt0”, “mgmt1”, “lo” (loopback), etc.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>N/A</td>
<td></td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Any Command Mode</td>
<td></td>
</tr>
<tr>
<td>History</td>
<td>3.1.0000</td>
<td></td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
<td></td>
</tr>
</tbody>
</table>

**Example**

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

switch (config) #
```

**Related Commands**

N/A

**Notes**

N/A
### show interface configured

**show interface <ifname> configured**

Displays configuration information about the specified interface.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ifname</td>
<td>The interface name e.g., “mgmt0”, “mgmt1”, “lo” (loopback), etc.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Default</th>
<th>N/A</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Configuration Mode</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Any Command Mode</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>History</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.1.0000</td>
<td></td>
</tr>
<tr>
<td>3.5.1000</td>
<td>Updated Example with “DHCP Hostname”</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Role</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>admin</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Example</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>switch (config) # show interfaces mgmt0 configured</td>
<td>Interface mgmt0 configuration</td>
</tr>
<tr>
<td>Enabled: yes</td>
<td></td>
</tr>
<tr>
<td>DHCP: yes</td>
<td></td>
</tr>
<tr>
<td>DHCP Hostname: yes</td>
<td></td>
</tr>
<tr>
<td>Zeroconf: no</td>
<td></td>
</tr>
<tr>
<td>IP address:</td>
<td></td>
</tr>
<tr>
<td>Netmask:</td>
<td></td>
</tr>
<tr>
<td>IPV6 enabled: yes</td>
<td></td>
</tr>
<tr>
<td>Autoconf enabled: no</td>
<td></td>
</tr>
<tr>
<td>Autoconf route: yes</td>
<td></td>
</tr>
<tr>
<td>Autoconf privacy: no</td>
<td></td>
</tr>
<tr>
<td>IPV6 addresses: 0</td>
<td></td>
</tr>
<tr>
<td>Speed: auto</td>
<td></td>
</tr>
<tr>
<td>Duplex: auto</td>
<td></td>
</tr>
<tr>
<td>MTU: 1500</td>
<td></td>
</tr>
<tr>
<td>Comment: my-interface</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Related Commands</th>
<th>N/A</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Notes</th>
<th></th>
</tr>
</thead>
</table>
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.

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>hostname</td>
<td>A free-form string.</td>
</tr>
</tbody>
</table>

**Default**

Default hostname

**Configuration Mode**

Config

**History**

3.1.0000
3.6.3004 Added support for the character “.”

**Role**

admin

**Example**

switch (config) # hostname my-switch-hostname
my-switch-hostname (config) #

**Related Commands**

show hosts

**Notes**

- Hostname may contain letters, numbers, and hyphens ('-'), in any combination
- Hostname may not contain other characters, such as “%”, “_” etc.
- The character “.” is supported
- Hostname may not begin with a hyphen
- Hostname may be 1-63 characters long
- Changing hostname stamps a new HTTPS certificate
### ip name-server

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

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

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>IPv4/v6 address</th>
<th>IPv4 or IPv6 address.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>No server name</td>
<td></td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Config</td>
<td></td>
</tr>
<tr>
<td>History</td>
<td>3.1.0000</td>
<td></td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
<td></td>
</tr>
</tbody>
</table>
| Example            | switch (config) # ip name-server 9.9.9.9  
switch (config) # show hosts  
Hostname: switch  
Name server: 9.9.9.9 (configured)  
Name server: 10.211.0.121 (dynamic)  
Name server: 172.30.0.126 (dynamic)  
Name server: 10.4.0.135 (dynamic)  
Domain name: lab.mtl.com (dynamic)  
Domain name: vmlab.mtl.com (dynamic)  
Domain name: yok.mtl.com (dynamic)  
Domain name: mtl.com (dynamic)  
IP 127.0.0.1 maps to hostname localhost  
IPv6 ::1 maps to hostname localhost6  
Automatically map hostname to loopback address: yes  
Automatically map hostname to IPv6 loopback address: no  
switch (config) # | show hosts | show hosts |
ip domain-list

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

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

### Syntax Description

<table>
<thead>
<tr>
<th>Domain Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>domain-name</td>
<td>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).</td>
</tr>
</tbody>
</table>

### Default

No static domain name

### Configuration Mode

Config

### History

3.1.0000

### Role

admin

### Example

```plaintext
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
```

### Related Commands

- show hosts

### Notes
ip/ipv6 host

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

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

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>hostname</td>
<td>The hostname in a string form.</td>
</tr>
<tr>
<td>IP Address</td>
<td>The IPv4 or IPv6 address.</td>
</tr>
</tbody>
</table>

| Default | No static domain name. |
| Configuration Mode | Config |
| History | 3.1.0000 |
| Role | admin |

Example

switch (config) # ip host my-host 2.2.2.2
switch (config) # ipv6 host my-ipv6-host 2001::8f9
switch (config) # show hosts
Hostname: switch
Name server: 9.9.9.9 (configured)
Name server: 10.211.0.121 (dynamic)
Name server: 172.30.0.126 (dynamic)
Name server: 10.4.0.135 (dynamic)
Domain name: mydomain.com (configured)
Domain name: lab.mtl.com (dynamic)
Domain name: vmlab.mtl.com (dynamic)
Domain name: yok.mtl.com (dynamic)
Domain name: mtl.com (dynamic)
IP 1.1.1.1 maps to hostname p
IP 127.0.0.1 maps to hostname localhost
IP 2.2.2.2 maps to hostname my-host
IPv6 2001::8f9 maps to hostname my-ipv6-host
IPv6 ::1 maps to hostname localhost6
Automatically map hostname to loopback address: yes
Automatically map hostname to IPv6 loopback address: yes
switch (config) #

Related Commands

show hosts

Notes
**ip/ipv6 map-hostname**

```
ip [ipv6] map-hostname
no [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.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>N/A</th>
</tr>
</thead>
</table>
| Default             | IPv4 mapping is enabled by default
|                     | IPv6 mapping is disabled by default |
| Configuration Mode  | Config |
| History             | 3.1.0000 |
| Role                | admin |

**Example**

```
switch (config) # ip map-hostname
switch (config) # # show hosts
Hostname: switch
Name server: 9.9.9.9 (configured)
Name server: 10.211.0.121 (dynamic)
Name server: 172.30.0.126 (dynamic)
Name server: 10.4.0.135 (dynamic)
Domain name: mydomain.com (configured)
Domain name: lab.mtl.com (dynamic)
Domain name: vmlab.mtl.com (dynamic)
Domain name: yok.mtl.com (dynamic)
Domain name: mtl.com (dynamic)
IP 1.1.1.1 maps to hostname p
IP 127.0.0.1 maps to hostname localhost
IP 2.2.2.2 maps to hostname my-host
IPv6 2001::8f9 maps to hostname my-ipv6-host
IPv6 ::1 maps to hostname localhost6
Automatically map hostname to loopback address: yes
Automatically map hostname to IPv6 loopback address: yes
switch (config) #
switch (config) # ping my-host-name
PING localhost (127.0.0.1) 56(84) bytes of data.
64 bytes from localhost (127.0.0.1): icmp_seq=1 ttl=64 time=0.078 ms
64 bytes from localhost (127.0.0.1): icmp_seq=2 ttl=64 time=0.052 ms
64 bytes from localhost (127.0.0.1): icmp_seq=3 ttl=64 time=0.058 ms
```
### Related Commands

- show hosts

### Notes

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

Displays hostname, DNS configuration, and static host mappings.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>N/A</td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Any Command Mode</td>
</tr>
<tr>
<td>History</td>
<td>3.1.0000</td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
</tr>
</tbody>
</table>

**Example**

```
switch (config) # show hosts
Hostname: my-host-name
Name server: 9.9.9.9 (configured)
Name server: 10.211.0.121 (dynamic)
Name server: 172.30.0.126 (dynamic)
Name server: 10.4.0.135 (dynamic)
Domain name: mydomain.com (configured)
Domain name: lab.mtl.com (dynamic)
Domain name: vmlab.mtl.com (dynamic)
Domain name: yok.mtl.com (dynamic)
Domain name: mtl.com (dynamic)
IP 1.1.1.1 maps to hostname p
IP 127.0.0.1 maps to hostname localhost
IP 2.2.2.2 maps to hostname my-host
IPv6 ::1 maps to hostname localhost6
Automatically map hostname to loopback address: yes
Automatically map hostname to IPv6 loopback address: no
switch (config) #
```
### 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.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>network-prefix</th>
<th>IPv4 or IPv6 network prefix.</th>
</tr>
</thead>
<tbody>
<tr>
<td>netmask</td>
<td></td>
<td>IPv4 netmask formats are:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• /24</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• 255.255.255.0</td>
</tr>
<tr>
<td></td>
<td></td>
<td>IPv6 netmask format is:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• /48 (as a part of the network prefix)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>nexthop-address</th>
<th>The IPv4 or IPv6 address of the next hop router for this route.</th>
</tr>
</thead>
<tbody>
<tr>
<td>ifname</td>
<td>The interface name (e.g., mgmt0, mgmt1).</td>
</tr>
</tbody>
</table>

| Default                       | N/A                                                             |
| Configuration Mode            | Config                                                          |
| History                       | 3.1.0000                                                        |
| Role                          | admin                                                           |

**Example**

```
switch (config) # ip route 20.20.0.0 255.255.255.0 mgmt0
switch (config) # show ip route
```

**Related Commands**

- show ip route

**Notes**
ipv6 default-gateway

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

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

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip address</td>
<td>The default gateway IP address (IPv6).</td>
</tr>
<tr>
<td>ifname</td>
<td>The interface name (e.g., mgmt0, mgmt1).</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Default</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuration Mode</td>
<td>Config</td>
</tr>
<tr>
<td>History</td>
<td>3.1.0000</td>
</tr>
<tr>
<td></td>
<td>3.2.0500</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Role</th>
<th>admin</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>switch (config) # ipv6 default-gateway ::1</td>
</tr>
<tr>
<td>switch (config) # show ipv6 default-gateway static</td>
</tr>
<tr>
<td>Configured default gateways:</td>
</tr>
<tr>
<td>::1</td>
</tr>
<tr>
<td>switch (config) #</td>
</tr>
</tbody>
</table>

| Related Commands | show ip route |

<table>
<thead>
<tr>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>• The configured default gateway will not be used if DHCP is enabled.</td>
</tr>
<tr>
<td>• In order to configure ipv4 default-gateway use ‘ip route’ command.</td>
</tr>
</tbody>
</table>
show ip/ipv6 route

show {ip | ipv6} route [static]

Displays the routing table in the system.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Default</th>
<th>Configuration Mode</th>
<th>History</th>
<th>Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>static</td>
<td>N/A</td>
<td>Any Command Mode</td>
<td>3.1.0000</td>
<td>admin</td>
</tr>
</tbody>
</table>

**Example**

```
switch (config) # show ip route
Destination       Mask              Gateway           Interface   Source  
default           0.0.0.0           172.30.0.1        mgmt0       DHCP  
10.10.10.10       255.255.255.255 0.0.0.0           mgmt0       static
20.10.10.10       255.255.255.255 172.30.0.1        mgmt0       static
20.20.20.0        255.255.255.0     0.0.0.0           mgmt0       static
172.30.0.0        255.255.0.0       0.0.0.0           mgmt0       interface
```

```
switch (config) # show ipv6 route
Destination prefix
Gateway                                  Interface  Source
-----------------------------------------------------------------------
::/0                                      
::1/128                                  lo       local
::                                 mgmt0       static
2222:2222:2222::/64                       
::                                 mgmt1       interface
```

Related Commands

show ip default-gateway

Notes
show ipv6 default-gateway

show ipv6 default-gateway [static]

Displays the default gateway.

Syntax Description

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>static</td>
<td>Displays the static configuration of the default gateway</td>
</tr>
</tbody>
</table>

Default: N/A

Configuration Mode: Any Command Mode

History: 3.1.0000

Role: admin

Example

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

Related Commands

ipv6 default-gateway

Notes

The configured IPv4 default gateway will not be used if DHCP is enabled.
### 4.1.7.4 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.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>IP address</th>
<th>IPv4 address.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>MAC address</td>
<td>MAC address.</td>
</tr>
</tbody>
</table>

**Default**

N/A

**Configuration Mode**

Config Interface Management

**History**

3.2.0500

**Role**

admin

**Example**

```
switch (config interface mgmt0) #ip arp 20.20.20.20 aa:aa:aa:aa:aa:aa
switch (config interface mgmt0) # show ip arp
```

```
Total number of entries: 6

<table>
<thead>
<tr>
<th>Address</th>
<th>Type</th>
<th>MAC Address</th>
<th>Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.209.1.103</td>
<td>Dynamic</td>
<td>00:02:C9:11:A1:78</td>
<td>mgmt0</td>
</tr>
<tr>
<td>10.209.1.168</td>
<td>Dynamic</td>
<td>00:02:C9:5E:C3:28</td>
<td>mgmt0</td>
</tr>
<tr>
<td>10.209.1.104</td>
<td>Dynamic</td>
<td>00:02:C9:11:A1:E6</td>
<td>mgmt0</td>
</tr>
<tr>
<td>10.209.1.153</td>
<td>Dynamic</td>
<td>00:02:C9:11:A1:86</td>
<td>mgmt0</td>
</tr>
<tr>
<td>10.209.1.105</td>
<td>Dynamic</td>
<td>00:02:C9:5E:0B:56</td>
<td>mgmt0</td>
</tr>
<tr>
<td>10.209.0.1</td>
<td>Dynamic</td>
<td>00:00:5E:00:01:01</td>
<td>mgmt0</td>
</tr>
</tbody>
</table>
```

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

**Related Commands**

- `show ip arp`
- `ip route`

**Notes**
ip arp timeout

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

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

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>timeout-value</td>
<td>Time (in seconds) that an entry remains in the ARP cache. Range: 60-28800.</td>
</tr>
<tr>
<td>vrf-name</td>
<td>VRF session name</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Default</th>
<th>1500 seconds</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Configuration Mode</th>
<th>Config</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>History</th>
<th>Added VRF parameter and updated Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.2.0230</td>
<td>3.5.1000</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Role</th>
<th>admin</th>
</tr>
</thead>
</table>

| Example | switch (config) # ip arp timeout 2000  
switch (config) # |
|---------|----------------|

| Related Commands | ip arp  
show ip arp |
|------------------|----------|

<table>
<thead>
<tr>
<th>Notes</th>
<th></th>
</tr>
</thead>
</table>
| • This value is used as the default ARP timeout whenever a new IP interface is created  
• The time interval after which each ARP entry becomes stale may actually vary from 50-150% of the configured value |
show ip arp

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

Displays ARP table.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>interface type</td>
<td>Filters the table according to a specific interface (i.e. mgmt0)</td>
</tr>
<tr>
<td>ip-address</td>
<td>Filters the table to the specific ip-address</td>
</tr>
<tr>
<td>count</td>
<td>Shows ARP statistics</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Default</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuration Mode</td>
<td>Any Command Mode</td>
</tr>
<tr>
<td>History</td>
<td>3.3.3000</td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
</tr>
<tr>
<td>Example</td>
<td>switch-626a54 [standalone: master] (config) # show ip arp</td>
</tr>
<tr>
<td></td>
<td>Total number of entries: 3</td>
</tr>
<tr>
<td></td>
<td>Address</td>
</tr>
<tr>
<td></td>
<td>--------</td>
</tr>
<tr>
<td></td>
<td>10.209.0.1</td>
</tr>
<tr>
<td></td>
<td>10.209.1.120</td>
</tr>
<tr>
<td></td>
<td>10.209.1.121</td>
</tr>
<tr>
<td></td>
<td>switch (config) # show ip arp count</td>
</tr>
<tr>
<td></td>
<td>ARP Table size: 3 (inband: 0, out of band: 3)</td>
</tr>
<tr>
<td></td>
<td>switch (config) #</td>
</tr>
</tbody>
</table>

Related Commands

Notes
**ipv6 neighbor**

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

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

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPv6 address</td>
<td>The IPv6 address.</td>
</tr>
<tr>
<td>ifname</td>
<td>The management interface (i.e. mgmt0, mgmt1).</td>
</tr>
<tr>
<td>MAC address</td>
<td>The MAC address.</td>
</tr>
</tbody>
</table>

| Default                  | N/A                                  |
| Configuration Mode       | Config                               |
| History                  | 3.1.0000                             |
| Role                     | admin                                |

**Example**

```plaintext
switch (config) # ipv6 neighbor 2001:db8:701f::8f9 mgmt0 00:11:22:33:44:55
switch (config) #
```

**Related Commands**

- show ipv6 neighbor
- ipv6 route
- arp
- clear ipv6 neighbors

**Notes**

- ARP is used only with IPv4. In IPv6 networks, Neighbor Discovery Protocol (NDP) is used similarly.
- Use The no form of the command to remove static entries. Dynamic entries can be cleared via the “clear ipv6 neighbors” command.
## clear ipv6 neighbors

**clear ipv6 neighbors**

Clears the dynamic neighbors cache.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>N/A</td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Config</td>
</tr>
<tr>
<td>History</td>
<td>3.1.0000</td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
</tr>
</tbody>
</table>
| Example            | switch (config) # clear ipv6 neighbors  
                   | switch (config) # |
| Related Commands   | ipv6 neighbor  
                   | show ipv6 neighbor  
                   | arp |
| Notes              | • Clearing Neighbor Discovery Protocol (NDP) cache removes only the dynamic entries learned and not the static entries configured  
                   | • Use the no form of the command to remove static entries |
**show ipv6 neighbors**

`show ipv6 neighbors [static]`

Displays the Neighbor Discovery Protocol (NDP) table.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>static</td>
<td>Filters only the table of the static entries.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Default</th>
<th>N/A</th>
</tr>
</thead>
</table>

**Configuration Mode**

Config

**History**

3.1.0000

**Role**

admin

**Example**

```
switch (config) # show ipv6 neighbors
IPv6 Address                            Age MAC Address       State      Interf
------------------------------------- ----- ----------------- ---------- ---
switch (config) #
```

**Related Commands**

ipv6 neighbor

clear ipv6 neighbor

show ipv6

**Notes**
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-hostname}
```

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

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>yield-to-static</td>
<td>Does not allow you to install a default gateway from DHCP if there is already a statically configured one.</td>
</tr>
<tr>
<td>hostname</td>
<td>Specifies the hostname to be sent during DHCP client negotiation if send-hostname is enabled.</td>
</tr>
<tr>
<td>primary-intf &lt;ifname&gt;</td>
<td>Sets the interface from which a non-interface-specific configuration (resolver and routes) will be accepted via DHCP.</td>
</tr>
<tr>
<td>send-hostname</td>
<td>Enables the DHCP client to send a hostname during negotiation.</td>
</tr>
</tbody>
</table>

| Default             | no ip dhcp yield-to-static
| no ip dhcp hostname
| ip ip dhcp primary-intf mgmt0
| no ip dhcp send-hostname |

| Configuration Mode | Config |
| History            | 3.1.0000 |
| Role               | admin |
Example

switch (config) # ip dhcp default-gateway yield-to-static
switch (config) # show ip dhcp

| DHCP | Enabled | Running | lease |
|-------------------------------------|
| lo | no | no | no |
| mgmt0 | yes | yes | yes |
| mgmt1 | yes | yes | no |

DHCP primary interface:
  Configured: mgmt0
  Active: mgmt0

DHCP default gateway yields to static configuration: yes

DHCP client options:
  Send Hostname: no
  Client Hostname: switch (using system hostname)

switch (config) #

Related Commands

show ip dhcp
dhcp [renew]

Notes

DHCP is supported for IPv4 networks only.
show ip dhcp

Displays the DHCP configuration and status.

**Syntax Description**

N/A

**Default**

N/A

**Configuration Mode**

Any Command Mode

**History**

3.1.0000

**Role**

admin

**Example**

```
switch (config) # show ip dhcp
DHCP primary interface:
    Configured: mgmt0
    Active:     mgmt0

DHCP: yield default gateway to static configuration: yes

DHCP Client Options:
    Send Hostname: no
    Client Hostname: switch (using system hostname)
```

**Related Commands**

ip dhcp
dhcp [renew]

**Notes**
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.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>IPv6 is disabled</td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Config</td>
</tr>
<tr>
<td>History</td>
<td>3.1.0000</td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
</tr>
</tbody>
</table>
| Example            | switch (config) # ipv6 enable
|                    | switch (config) # show ipv6
|                    | IPv6 summary
|                    |   IPv6 supported: yes
|                    |   IPv6 admin enabled: yes
|                    |   IPv6 interface count: 2
|                    | switch (config) # |

**Related Commands** - ipv6 default-gateway, ipv6 host, ipv6 map-hostname, ipv6 neighbor, ipv6 route, show ipv6, show ipv6 default-gateway, show ipv6 route

**Notes**
### 4.1.7.7 IP Diagnostic Tools

**ping**

```
```

Sends ICMP echo requests to a specified host.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Linux Ping options</th>
<th><a href="http://linux.about.com/od/commands/l/blcm-d18_ping.htm">http://linux.about.com/od/commands/l/blcm-d18_ping.htm</a></th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>N/A</td>
<td></td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Config</td>
<td></td>
</tr>
<tr>
<td>History</td>
<td>3.1.0000</td>
<td></td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
<td></td>
</tr>
</tbody>
</table>

**Example**

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

**Related Commands**

traceroutes

**Notes**
traceroute


Traces the route packets take to a destination.
<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>-4</td>
<td>Uses IPv4.</td>
</tr>
<tr>
<td></td>
<td>-6</td>
<td>Uses IPv6.</td>
</tr>
<tr>
<td></td>
<td>-d</td>
<td>Enables socket level debugging.</td>
</tr>
<tr>
<td></td>
<td>-F</td>
<td>Sets DF (do not fragment bit) on.</td>
</tr>
<tr>
<td></td>
<td>-I</td>
<td>Uses ICMP ECHO for tracerouting.</td>
</tr>
<tr>
<td></td>
<td>-T</td>
<td>Uses TCP SYN for tracerouting.</td>
</tr>
<tr>
<td></td>
<td>-U</td>
<td>Uses UDP datagram (default) for tracerouting.</td>
</tr>
<tr>
<td></td>
<td>-n</td>
<td>Does not resolve IP addresses to their domain names.</td>
</tr>
<tr>
<td></td>
<td>-r</td>
<td>Bypasses the normal routing and send directly to a host on an attached network.</td>
</tr>
<tr>
<td></td>
<td>-A</td>
<td>Performs AS path lookups in routing registries and print results directly after the corresponding addresses.</td>
</tr>
<tr>
<td></td>
<td>-V</td>
<td>Prints version info and exit.</td>
</tr>
<tr>
<td></td>
<td>-f</td>
<td>Starts from the first_ttl hop (instead from 1).</td>
</tr>
<tr>
<td></td>
<td>-g</td>
<td>Routes packets throw the specified gateway (maximum 8 for IPv4 and 127 for IPv6).</td>
</tr>
<tr>
<td></td>
<td>-i</td>
<td>Specifies a network interface to operate with.</td>
</tr>
<tr>
<td></td>
<td>-m</td>
<td>Sets the max number of hops (max TTL to be reached). Default is 30.</td>
</tr>
<tr>
<td></td>
<td>-N</td>
<td>Sets the number of probes to be tried simultaneously (default is 16).</td>
</tr>
<tr>
<td></td>
<td>-p</td>
<td>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).</td>
</tr>
<tr>
<td></td>
<td>-t</td>
<td>Sets the TOS (IPv4 type of service) or TC (IPv6 traffic class) value for outgoing packets.</td>
</tr>
<tr>
<td></td>
<td>-l</td>
<td>Uses specified flow_label for IPv6 packets.</td>
</tr>
<tr>
<td></td>
<td>-w</td>
<td>Sets the number of seconds to wait for response to a probe (default is 5.0). Non-integer (float point) values allowed too.</td>
</tr>
<tr>
<td></td>
<td>-q</td>
<td>Sets the number of probes per each hop. Default is 3.</td>
</tr>
<tr>
<td>Default</td>
<td>N/A</td>
<td></td>
</tr>
<tr>
<td>----------</td>
<td>------------------------------------------</td>
<td></td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Config</td>
<td></td>
</tr>
<tr>
<td>History</td>
<td>3.1.0000</td>
<td></td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
<td></td>
</tr>
</tbody>
</table>
| Example  | switch (config) # traceroute 192.168.10.70  
traceroute to 192.168.10.70 (192.168.10.70), 30 hops max, 40 byte packets  
1 172.30.0.1 (172.30.0.1) 3.632 ms 2.849 ms 3.544 ms  
2 10.222.128.46 (10.222.128.46) 3.176 ms 3.289 ms 3.656 ms  
3 10.158.128.30 (10.158.128.30) 15.331 ms 15.819 ms 16.388 ms  
4 10.158.128.65 (10.158.128.65) 20.468 ms 7.893 ms 12.27 ms  
5 10.7.34.115 (10.7.34.115) 16.405 ms 11.985 ms 12.264 ms  
6 192.168.10.70 (192.168.10.70) 16.377 ms 16.091 ms 20.475 ms  
switch (config) #                                      |
| Related Commands |                                             |
| Notes     |                                           |
**tcpdump**

```
tcpdump [-aAdDeflNOpqRStuxX] [-c count] [-C file_size]
    [-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.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>N/A</td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Config</td>
</tr>
<tr>
<td>History</td>
<td>3.1.0000</td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
</tr>
</tbody>
</table>

**Example**

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

**Related Commands**

N/A

**Notes**

N/A
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**

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

Sets the time and date.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>hh:mm:ss</td>
<td>Time.</td>
</tr>
<tr>
<td>yyyy/mm/dd</td>
<td>Date.</td>
</tr>
</tbody>
</table>

**Default**

N/A

**Configuration Mode**

Config

**History**

3.1.0000

**Role**

admin

**Example**

```
switch (config) # clock set 23:23:23 2010/08/19
switch (config) # show clock
Time: 23:23:26
Date: 2010/08/19
Time zone: UTC
(Etc/UTC)
UTC offset: same as UTC
switch (config) #
```

**Related Commands**

show clock

**Notes**

If not specified, the date will be left the same.
clock timezone

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

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

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

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

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>zone word</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>The possible forms this could take include: continent, city, continent, country, city, continent, region, country, city, ocean, and/or island.</td>
</tr>
</tbody>
</table>

- **Default**: GMT
- **Configuration Mode**: Config
- **History**: 3.1.0000
- **Role**: admin

**Example**

```
switch (config) # clock timezone America North United_States Other New_York
switch (config) # show clock
Time: 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) #
```

**Related Commands**: show clock

**Notes**
ntp

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

Configures NTP. The no form of the command negates NTP options.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>disable</th>
<th>enable</th>
<th>peer or server</th>
<th>IP address</th>
<th>version &lt;number&gt;</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Disables NTP</td>
<td>Enables NTP</td>
<td>Configures an NTP peer or server node</td>
<td>IPv4 or IPv6 address</td>
<td>Specifies the NTP version number of this peer</td>
</tr>
<tr>
<td>Default</td>
<td>NTP is enabled</td>
<td>NTP version number is 4</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Configuration Mode</th>
<th>Config</th>
</tr>
</thead>
<tbody>
<tr>
<td>History</td>
<td>3.1.0000</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Role</th>
<th>admin</th>
</tr>
</thead>
</table>

| Example |         | switch (config) # no ntp peer 192.168.10.24 disable  
|---------|---------| switch (config) # |

| Related Commands | N/A |

| Notes | |

**ntpdate**

```
ntpdate <IP address>
```

Sets the system clock using the specified SNTP server.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>IP address</th>
<th>IP.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>N/A</td>
<td></td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Config</td>
<td></td>
</tr>
<tr>
<td>History</td>
<td>3.1.0000</td>
<td></td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
<td></td>
</tr>
</tbody>
</table>

**Example**

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

<table>
<thead>
<tr>
<th>Related Commands</th>
<th>N/A</th>
</tr>
</thead>
</table>

**Notes**

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

**ntp authenticate**  
**no ntp authenticate**

Enables NTP authentication.  
The no form of the command disables NTP authentication.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>N/A</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>Disabled</td>
<td></td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Config</td>
<td></td>
</tr>
<tr>
<td>History</td>
<td>3.5.0200</td>
<td></td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
<td></td>
</tr>
<tr>
<td>Example</td>
<td>switch (config) # ntp authenticate</td>
<td></td>
</tr>
<tr>
<td>Related Commands</td>
<td>N/A</td>
<td></td>
</tr>
<tr>
<td>Notes</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### 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.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>key_id</td>
<td>Specifies a key ID, whether existing or a new one to be added. Range: 1-65534.</td>
</tr>
<tr>
<td>encrypt_type</td>
<td>Specifies encryption type to use (md5, or sha1)</td>
</tr>
<tr>
<td>password</td>
<td>Password string</td>
</tr>
</tbody>
</table>

| Default                  | Disabled                                                                   |
| Configuration Mode       | Config                                                                     |
| History                  | 3.5.0200                                                                   |
| Role                     | admin                                                                     |

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

**Related Commands**
N/A

**Notes**
If a password is not entered, a prompt appears requiring that a password is introduced.
# ntp peer disable

```
npt 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.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip_address</td>
<td>IP address of the peer (IPv4 and IPv6 are acceptable)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Default</th>
<th>Disabled</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuration Mode</td>
<td>Config</td>
</tr>
<tr>
<td>History</td>
<td>3.5.0200</td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
</tr>
</tbody>
</table>
| Example       | switch (config) # ntp peer 10.10.10.10 disable  
                | switch (config) # |
| Related Commands | N/A     |
| Notes         |         |
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.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>ip_address</th>
<th>IP address of the peer (IPv4 and IPv6 are acceptable)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>key_id</td>
<td>Range: 1-65534</td>
</tr>
</tbody>
</table>

Default: Disabled

Configuration Mode: Config

History: 3.5.0200

Role: admin

Example: switch (config) # ntp peer 10.10.10.10 keyID 120

Related Commands: N/A

Notes:
### 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.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip_address</td>
<td>IP address of the peer (IPv4 and IPv6 are acceptable)</td>
</tr>
<tr>
<td>ver_num</td>
<td>NTP version (3 or 4)</td>
</tr>
</tbody>
</table>

| Default | 4 |
| Configuration Mode | Config |
| History | 3.5.0200 |
| Role | admin |

#### Example
```
switch (config) # ntp peer 10.10.10.10 version 4
```

#### Related Commands
N/A

#### Notes

---

Mellanox Technologies Confidential  
Rev 4.60
ftp server disable

ftp server <ip_address> disable
no ftp server <ip_address> disable

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

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>ip_address</th>
<th>IP address of the server (IPv4 and IPv6 are acceptable)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>Disabled</td>
<td></td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Config</td>
<td></td>
</tr>
<tr>
<td>History</td>
<td>3.5.0000</td>
<td></td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
<td></td>
</tr>
</tbody>
</table>
| Example            | switch (config) # ntp server 10.10.10.10 disable
switch (config) # |
| Related Commands   | N/A         |                                                        |
| Notes              |             |                                                        |
**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.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip_address</td>
<td>IP address of the server (IPv4 and IPv6 are acceptable)</td>
</tr>
<tr>
<td>key_id</td>
<td>Range: 1-65534</td>
</tr>
</tbody>
</table>

Default Disabled

Configuration Mode Config

History 3.5.0200

Role admin

Example switch (config) # ntp server 10.10.10.10 keyID 120

Related Commands N/A

Notes
**ntp server trusted-enable**

```plaintext
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.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip_address</td>
<td>IP address of NTP server</td>
</tr>
</tbody>
</table>

**Default**

N/A

**Configuration Mode**

Config

**History**

3.6.2002

**Role**

admin

**Example**

```
switch (config) # ntp server 10.10.10.10 trusted-enable
```

**Related Commands**

N/A

**Notes**

NTP trusted servers can be used as a mitigation for Sybil attacks which is a vulnerability caused by NTP peers sharing the same NTP key base. This mitigation adds the concept of trusted servers which if enabled in conjunction with NTP authentication ensures that time information will only be obtained from trusted servers.
### ntp server version

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

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

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip_address</td>
<td>IP address of the server (IPv4 and IPv6 are acceptable)</td>
</tr>
<tr>
<td>ver_num</td>
<td>NTP version (3 or 4)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Configuration Mode</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Config</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>History</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.5.0200</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Role</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>admin</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Example</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>switch (config) # ntp server 10.10.10.10 version 4</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Related Commands</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>N/A</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
</tr>
</tbody>
</table>
**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.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>key(s)</th>
<th>Range: 1-65534.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>Disabled</td>
<td></td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Config</td>
<td></td>
</tr>
<tr>
<td>History</td>
<td>3.5.0200</td>
<td></td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
<td></td>
</tr>
</tbody>
</table>
| Example            | switch (config) # ntp trusted-key 1,3,5  
switch (config) # ntp trusted-key 1-5  |                 |
| Related Commands   | ntp authentication-key | |
| Notes              | Keys may be separated with commas without any space, or they may be set as a range using a hyphen. |
show clock

show clock

Displays the current system time, date and time zone.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>N/A</td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Any Command Mode</td>
</tr>
<tr>
<td>History</td>
<td>3.1.0000</td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
</tr>
</tbody>
</table>
| Example            | switch (config) # show clock
     Time: 04:21:44
     Date: 2012/02/26
     Time zone: America North United_States Other New_York |
| Related Commands   | N/A |
| Notes              |     |
show ntp

show ntp
Displays the current NTP settings.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>N/A</td>
</tr>
</tbody>
</table>

**Configuration Mode**: Any Command Mode

**History**
3.1.0000
3.5.0200 Updated Example

**Role**: admin

**Example**
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) #

**Related Commands**
N/A

**Notes**
**show ntp configured**

Displays NTP configuration.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>N/A</td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Any Command Mode</td>
</tr>
<tr>
<td>History</td>
<td>3.5.0200</td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
</tr>
</tbody>
</table>

**Example**

```plaintext
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) #
```

<table>
<thead>
<tr>
<th>Related Commands</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Notes</td>
<td></td>
</tr>
</tbody>
</table>
### show ntp keys

#### show ntp configured

Displays NTP keys.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>N/A</td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Any Command Mode</td>
</tr>
<tr>
<td>History</td>
<td>3.5.0200</td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
</tr>
</tbody>
</table>

#### Example

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

#### Related Commands

N/A

#### Notes
4.3 Software Management

4.3.1 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 4.3.2, “Upgrading MLNX-OS HA Groups,” on page 207.

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:
```

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

```
switch (config) # image delete image-PPC_M460EX-3.0.1224.img
switch (config) #
```

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

Step 4. Fetch the new software image.

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

Step 5. Display the available images.

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

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

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

  Partition 2:
     SX <new ver> 2013-04-28 16:52:50
```
Step 6. Install the new image.

```bash
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:

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

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

```bash
switch (config) # show images
Images available to be installed:
  new_image.img
  SX <new ver> 2013-04-28 16:52:50

Installed images:
Partition 1:
  SX <old ver> 2011-04-28 16:02:50
```
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 4.3.1, “Upgrading MLNX-OS Software,” on page 204.

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

### 4.3.2 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
```

<table>
<thead>
<tr>
<th>Hostname</th>
<th>VIP-State</th>
<th>IP Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>SwitchA</td>
<td>master</td>
<td>10.10.10.1</td>
</tr>
<tr>
<td>SwitchB</td>
<td>standby</td>
<td>10.10.10.2</td>
</tr>
</tbody>
</table>

Step 2. Upgrade standby nodes in the HA group according to steps 1-10 in section Section 4.3.1, on page 204.

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 4.3.1, on page 204.

4.3.3 Deleting Unused Images

➢ To delete unused images:

Step 1. Enter Config mode. Run:

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

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

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

Last boot partition: 1
Next boot partition: 1
Boot manager password is set.
No image install currently in progress.
Require trusted signature in image being installed: yes
switch (config) #
```
Step 3. Delete the unused images. Run:

```
switch (config) # image delete image-PPC_M460EX-3.1.1224.img
switch (config) #
```

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

4.3.4 Downgrading MLNX-OS Software

**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.

4.3.4.1 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](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 delete image=EFM_PPC_M405EX-ppc-m405ex 20090531-190132.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>
```

### 4.3.4.2 Downgrading Image

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

Step 1. Log in as admin.

Step 2. Enter config mode. Run:

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

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

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

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

```
switch (config) # image install <image_name>
Step 1 of 4: Verify Image
100.0% [###############################]
Step 2 of 4: Uncompress Image
100.0% [###############################]
Step 3 of 4: Create Filesystems
100.0% [###############################]
Step 4 of 4: Extract Image
100.0% [###############################]
switch (config) #
```
Step 5. Show all image files on the system. Run:

```plaintext
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.
```

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

```plaintext
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:

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

Step 7. Reload the switch. Run:

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

4.3.4.3 Switching to Partition with Older Software Version

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

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

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

- The user has run “reset factory” command, which clears all configuration files in the system
- The user has run “configuration switch-to” to a configuration file with different name then the backup file
Note that the configuration file becomes empty if the switch is downgraded to a software version which has never been installed yet.

To allow switching partition to the older software version for the 2 aforementioned cases only, follow the steps below:

**Step 1.** Run the command:

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

**Step 2.** Set the boot partition. Run:

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

**Step 3.** Save the configuration. Run:

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

**Step 4.** Reload the system. Run:

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

### 4.3.5 Upgrading System Firmware

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

#### 4.3.5.1 After Updating MLNX-OS Software

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

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

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

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

Some subsystems are not updated with a default firmware.

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

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

4.3.5.2.1 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.
```

Step 2. Save the configuration. Run:

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

Step 3. Reboot the system to enable auto update.

4.3.6 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 a 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.

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
```
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.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>location ID</td>
<td>Specifies the default destination location. There can be up to 2 images on the system. The possible values are 1 or 2.</td>
</tr>
<tr>
<td>next</td>
<td>Sets the boot location to be the next once after the one currently booted from, thus avoiding a cycle through all the available locations.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Default</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuration Mode</td>
<td>enable/config</td>
</tr>
<tr>
<td>History</td>
<td>3.1.0000</td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
</tr>
</tbody>
</table>

**Example**

```plaintext
switch (config) # image boot location 2
switch (config) #
```

**Related Commands**

- show images

**Notes**
### boot next

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

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

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

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

```
boot system {location | next}
no boot system next
```

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

### Syntax Description

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>location</td>
<td>Specifies location from which to boot system</td>
</tr>
<tr>
<td>next</td>
<td>Boots system from next location after one currently booted</td>
</tr>
<tr>
<td>location</td>
<td>• 1 – installs to location 1</td>
</tr>
<tr>
<td></td>
<td>• 2 – installs to location 2</td>
</tr>
</tbody>
</table>

### Default

N/A

### Configuration Mode

Config

### History

3.2.0506

### Role

admin

### Example

```
switch (config) # boot system location 2
switch (config) #
```

### Related Commands

show images

### Notes
### image default-chip-fw

image default-chip-fw <file name>

Sets the default firmware package to be installed.

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

Notes
### image delete

**image delete <image name>**

Deletes the specified image file.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>image name</td>
<td>Specifies the image name.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Default</th>
<th>N/A</th>
</tr>
</thead>
</table>

**Configuration Mode**

<table>
<thead>
<tr>
<th>Configuration Mode</th>
<th>Config</th>
</tr>
</thead>
</table>

**History**

3.1.0000

**Role**

admin

**Example**

```bash
switch (config) # image delete image=MLNXNX-OS-201140526-010145.img
switch (config) #
```

**Related Commands**

- show images

**Notes**
### image fetch

**image fetch** `<URL> [<filename>]`  
Downloads an image from the specified URL or via SCP.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>URL</td>
<td>HTTP, HTTPS, FTP, TFTP, SCP and SFTP are supported. Example: scp://username:[password]@hostname/path/filename.</td>
</tr>
<tr>
<td>filename</td>
<td>Specifies a filename for this image to be stored locally.</td>
</tr>
</tbody>
</table>

**Default**  
N/A

**Configuration Mode**  
Config

**History**  
3.1.0000

**Role**  
admin

**Example**

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

Other options:

```bash
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.ima
switch (config) # image fetch ftp://user:mypassword@[fd4f:13:cc00:1::40]/foo/bar.ima
switch (config) # image fetch ftp://hostname/dir/filename
switch (config) # image fetch ftp://[fd4f:13:cc00:1::40]/dir/filename
switch (config) # image fetch scp://user@myhost/dir/filename
switch (config) # image fetch scp://user@myhost:[1022]/dir/filename
switch (config) # image fetch scp://user:pass@[fd4f:13:cc00:1::40]/dir/filename
switch (config) # image fetch sftp://user@myhost/dir/filename
switch (config) # image fetch sftp://user@[fd4f:13:cc00:1::40]:1022/dir/filename
switch (config) # image fetch sftp://user:pass@[fd4f:13:cc00:1::40]/dir/filename
```
### Related Commands

- show images

### Notes

- Please delete the previously available image, prior to fetching the new image.
- The path to the file in the case of TFTP depends on the server configuration. Therefore, it may not be an absolute path but a relative one.
- See section “Upgrading MLNX-OS SX Software,” in the *Mellanox SwitchX® User Manual* for a full upgrade example.
image install

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

Installs the specified image file.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>description</th>
</tr>
</thead>
<tbody>
<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>
</tbody>
</table>
| prog-options        | • “no-track” overrides CLI default and does not track the installation progress  
                     • “track” overrides CLI default and tracks the installation progress |
| ver-options         | • “check-sig” requires an image to have either a valid signature or no signature  
                     • “ignore-sig” allows unsigned or invalidly signed images to be installed  
                     • “require-sig” requires from the installed image to have a valid signature. If a valid signature is not found on the image, the image cannot be installed |

| Default             | N/A |
| Configuration Mode  | Config |
| History             | 3.1.0000 |
| Role                | admin |
| Example             | switch (config) # image install SX_PPC_M460EX 3.0.0000-dev-HA 2012-01-22 08:47:59 ppc  
                     Step 1 of 4: Verify Image  
                     100.0%  
                     [################################################################]  
                     Step 2 of 4: Uncompress Image  
                     100.0%  
                     [################################################################]  
                     Step 3 of 4: Create Filesystems  
                     100.0%  
                     [################################################################]  
                     Step 4 of 4: Extract Image  
                     100.0%  
                     [################################################################]  
                     switch (config) # |
<table>
<thead>
<tr>
<th>Related Commands</th>
<th>show images</th>
</tr>
</thead>
</table>
| Notes             | • The image cannot be installed on the “active” location (the one which is currently being booted)  
• On a two-location system, the location is chosen automatically if no location is specified |
# image move

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

Renames the specified image file.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>src image name</th>
<th>Specifies the old image name.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>dest image name</td>
<td>Specifies the new image name.</td>
</tr>
</tbody>
</table>

**Default**

N/A

**Configuration Mode**

Config

**History**

3.1.0000

**Role**

admin

**Example**

```
switch (config) # image move image1.img image2.img
switch (config) #
```

**Related Commands**

show images

**Notes**
image options

image options {require-sig | serve 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.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>require-sig</th>
<th>Requires images to be signed by a trusted signature</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>serve all</td>
<td>Specifies that the image files present on this appliance should be made available for HTTP and/or HTTPS download</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Default</th>
<th>N/A</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Configuration Mode</th>
<th>Config</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>History</th>
<th>3.1.0000</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Role</th>
<th>admin</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Example</th>
<th>switch (config) # image options require-sig</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Related Commands</th>
<th>show images</th>
</tr>
</thead>
</table>

| Notes | The parameter “serve all” affects not only the files currently present, but also any files that are later downloaded. It only applies to image files, not the installed images, which are not themselves in a downloadable format. After running “serve all” the URLs where the images will be available are:  
• http://<HOSTNAME>/system_images/<FILENAME>  
• https://<HOSTNAME>/system_images/<FILENAME> |
|--------|----------------------------------------------------------|
show bootvar

show bootvar

Displays the installed system images and the boot parameters.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>N/A</td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Config</td>
</tr>
<tr>
<td>History</td>
<td>3.1.0000</td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
</tr>
</tbody>
</table>

**Example**

```
switch (config) # show bootvar
Installed images:
    Partition 1:
      SX_PPC_M460EX 3.0.0000-dev-HA 2012-01-22 08:47:59 ppc
      Last dobincp: 2012/01/23 14:54:23

    Partition 2:
      SX_PPC_M460EX 3.0.0000-dev-HA 2012-01-18 09:52:41 ppc
      Last dobincp: 2012/01/19 16:48:23

Last boot partition: 1
Next boot partition: 1

Boot manager password is set.

No image install currently in progress.

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

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

switch (config) #
```
show images

show image

Displays information about the system images and boot parameters.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>N/A</td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Any Command Mode</td>
</tr>
<tr>
<td>History</td>
<td>3.1.0000</td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
</tr>
</tbody>
</table>

**Example**

```
switch (config) # show images
Images available to be installed:
  image=SX_PPC_M460EX-ppc-m460ex-20120122-084759.img
SX_PPC_M460EX 3.0.0000-dev-HA 2012-01-22 08:47:59 ppc

 Installed images:
  Partition 1:
  SX_PPC_M460EX 3.0.0000-dev-HA 2012-01-22 08:47:59 ppc
  Last dobincp: 2012/01/23 14:54:23

  Partition 2:
  SX_PPC_M460EX 3.0.0000-dev-HA 2012-01-18 09:52:41 ppc
  Last dobincp: 2012/01/19 16:48:23

 Last boot partition: 1
 Next boot partition: 1

 Boot manager password is set.

 No image install currently in progress.

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

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

**Related Commands**

N/A

**Notes**


4.4  Configuration Management

4.4.1  Saving a Configuration File

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

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

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

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

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

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

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

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

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

4.4.2  Loading a Configuration File

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

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

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

4.4.3  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:

  Step 1. Run the command `reset factory [reboot] [keep-basic] [keep-all-config]:`

  ```
  switch (config) # reset factory keep-basic
  ```
4.4.4 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.

4.4.4.1 BIN Configuration Files

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

- **To create a new BIN configuration file:**
  ```
  switch (config) # configuration new my-filename
  ```

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

- **To upload a BIN configuration file from a switch to an external file server:**
  ```
  switch (config) # configuration upload my-filename scp://myusername@my-server/path/to/my/<file>
  ```

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

- **To see the available configuration files:**
  ```
  switch (config) # show configuration files
  initial (active)
  my-filename
  ```

  Active configuration: initial
  Unsaved changes: no

  ```
  switch (config) #
  ```

- **To load a BIN configuration file:**
  ```
  switch (config) # configuration switch-to my-filename
  ```
  This requires a reboot.
  Type 'yes' to confirm: yes

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

  A binary configuration file uploaded from the switch is encrypted and has integrity verification. If the file is modified in any manner, the fetch to the switch fails.
4.4.4.2 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 4.4.4.1) 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.
### 4.4.5 Commands

#### 4.4.5.1 File System

**debug generate dump**

```
debug generate dump
```

Generates a debug dump.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>N/A</td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Config</td>
</tr>
<tr>
<td>History</td>
<td>3.1.0000</td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
</tr>
</tbody>
</table>
| Example            | switch (config) # debug generate dump  
Generated dump syadump-switch-112104-201140526-091707.tgz  
switch (config) # |
| Related Commands   | file debug-dump |
| Notes              | The dump can then be manipulated using the “file debug-dump...” commands. |
**file debug-dump**

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

Manipulates debug dump files.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>delete {&lt;filename&gt;</td>
<td>latest}</td>
</tr>
<tr>
<td>email {&lt;filename&gt;</td>
<td>latest}</td>
</tr>
<tr>
<td>upload {{&lt;filename&gt;</td>
<td>latest} &lt;URL&gt;}}</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Default</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuration Mode</td>
<td>Config</td>
</tr>
<tr>
<td>History</td>
<td>3.1.0000 Initial release</td>
</tr>
<tr>
<td></td>
<td>3.3.4000 Added “latest” parameter</td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
</tr>
</tbody>
</table>
| Example | switch (config) # file debug-dump email sysdump-switch-112104-20114052-091707.tgz  
switch (config) # |
| Related Commands | show files debug-dump |
| Notes | |
## file stats

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

Manipulates statistics report files.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>delete &lt;filename&gt;</th>
<th>Deletes a stats report file.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>move &lt;source filename&gt; &lt;destination filename&gt;</td>
<td>Renames a stats report file.</td>
</tr>
<tr>
<td></td>
<td>upload &lt;filename&gt; &lt;URL&gt;</td>
<td>Uploads a stats report file. URL - HTTP, HTTPS, FTP, TFTP, SCP and SFTP are supported. Example: scp://username[:password]@hostname/path/filename.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Default</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuration Mode</td>
<td>Config</td>
</tr>
<tr>
<td>History</td>
<td>3.1.0000</td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
</tr>
</tbody>
</table>
| Example | switch (config) # file stats move memory-1.csv memory-2.csv  
switch (config) # |
| Related Commands | show files stats  
show files stats <filename> |
| Notes | |
**file tcpdump**

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

Manipulates tcpdump output files.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>delete &lt;filename&gt;</td>
<td>Deletes the specified tcpdump output file.</td>
</tr>
<tr>
<td>upload &lt;filename&gt;</td>
<td>Uploads the specified tcpdump output file to the specified URL.</td>
</tr>
<tr>
<td>&lt;URL&gt;</td>
<td>URL - HTTP, HTTPS, FTP, TFTP, SCP and SFTP are supported. Example: scp://username[:password]@hostname/path/filename.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Default</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuration Mode</td>
<td>Config</td>
</tr>
<tr>
<td>History</td>
<td>3.1.0000</td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
</tr>
</tbody>
</table>

**Example**

```
switch (config) # file tcpdump delete my-tcpdump-file.txt
switch (config) #
```

**Related Commands**

- `show files stats`
- `tcpdump`

**Notes**
# reload

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

Reboots or shuts down the system.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>force immediate</th>
<th>Forces an immediate reboot of the system even if the system is busy.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>halt</td>
<td>Shuts down the system.</td>
</tr>
<tr>
<td></td>
<td>noconfirm</td>
<td>Reboots the system without asking about unsaved changes.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Default</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuration Mode</td>
<td>Config</td>
</tr>
<tr>
<td>History</td>
<td>3.1.0000</td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
</tr>
</tbody>
</table>

**Example**

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

**Related Commands**

reset factory

**Notes**
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.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>keep-all-config</th>
<th>keep-basic</th>
<th>keep-virt-vols</th>
<th>only-config</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>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”.</td>
<td>Preserves licenses in the running configuration file</td>
<td>Preserve all virtual disk volumes</td>
<td>Removes configuration files only. The logs, stats, images, snapshots, history, and known hosts are preserved.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Default</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuration Mode</td>
<td>Config</td>
</tr>
<tr>
<td>History</td>
<td>3.1.0000</td>
</tr>
<tr>
<td></td>
<td>3.4.0000 Added notes and “keep-virt-vols” parameter</td>
</tr>
<tr>
<td></td>
<td>3.6.2002 Updated Example and Notes</td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
</tr>
</tbody>
</table>
| Example | switch (config) # reset factory  
Warning - confirming will cause system reboot.  
Type 'YES' to confirm reset: YES  
Resetting and rebooting the system -- please wait...  
... |
<table>
<thead>
<tr>
<th><strong>Related Commands</strong></th>
<th>reload</th>
</tr>
</thead>
</table>
| **Notes**            | • Effects of parameter “keep-all-config”: Licenses – not deleted; profile – no change; configuration – unchanged; management IP – unchanged  
• Effects of parameter “keep-basic”: Licenses – not deleted; profile – reset; configuration – reset; management IP – reset 
• Effects of parameter “keep-virt-vols”: Licenses – deleted; profile – reset; configuration – reset; management IP – unchanged 
• Confirming the command causes system reboot |
### show files debug-dump

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

Displays a list of debug dump files.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>filename</th>
<th>Displays a summary of the contents of a particular debug dump file.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>N/A</td>
<td></td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Config</td>
<td></td>
</tr>
<tr>
<td>History</td>
<td>3.1.0000</td>
<td></td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
<td></td>
</tr>
<tr>
<td>Example</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

```
switch (config) # show files debug-dump sysdump-switch-112104-2011052-091707.tgz
System information:

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

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

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

==================================================================

```

### Related Commands

file debug-dump

### Notes
show files stats

show files stats <filename>

Displays a list of statistics report files.

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

**show files system [detail]**

Displays usage information of the file systems on the system.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>detail</th>
<th>Displays more detailed information on file-system.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>N/A</td>
<td></td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Config</td>
<td></td>
</tr>
<tr>
<td>History</td>
<td>3.1.0000</td>
<td></td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
<td></td>
</tr>
</tbody>
</table>

**Example**

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

Statistics for /var filesystem:
  Bytes Total          860 MB
  Bytes Used           209 MB
  Bytes Free           651 MB
  Bytes Percent Free   75%
  Bytes Available      651 MB
  Inodes Total         0
  Inodes Used          0
  Inodes Free          0
  Inodes Percent Free  0%
```

**Related Commands**

N/A

**Notes**


### show files tcpdump

*Syntax Description:* Displays a list of statistics report files.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Default</th>
<th>Configuration Mode</th>
<th>History</th>
<th>Role</th>
<th>Example</th>
<th>Related Commands</th>
</tr>
</thead>
<tbody>
<tr>
<td>N/A</td>
<td>N/A</td>
<td>Config</td>
<td>3.1.0000</td>
<td>admin</td>
<td></td>
<td>file tcpdump</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>tcpdump</td>
</tr>
</tbody>
</table>

**Notes:**

### 4.4.5.2 Configuration Files

#### configuration audit

*Syntax Description:* Chooses settings related to configuration change auditing.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Default</th>
<th>Configuration Mode</th>
<th>History</th>
<th>Role</th>
<th>Example</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>max-changes Set maximum number of audit messages to log per change.</td>
<td>1000</td>
<td>Config</td>
<td>3.1.0000</td>
<td>admin</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Example:**

```bash
switch (config) # configuration audit max-changes 100
switch (config) # show configuration audit
Maximum number of changes to log: 100
switch (config) #
```
<table>
<thead>
<tr>
<th>Related Commands</th>
<th>show configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>Notes</td>
<td>N/A</td>
</tr>
</tbody>
</table>
configuration copy

configuration copy <source name> <dest name>

Copies a configuration file.

Syntax Description

<table>
<thead>
<tr>
<th>Source Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>source name</td>
<td>Name of source file.</td>
</tr>
<tr>
<td>dest name</td>
<td>Name of destination file. If the file of specified filename does not exist a new file will be created with said filename.</td>
</tr>
</tbody>
</table>

Default

N/A

Configuration Mode

Config

History

3.1.0000

Role

admin

Example

switch (config) # configuration copy initial.bak example
switch (config) #

Related Commands

Notes

- This command does not affect the current running configuration
- The active configuration file may not be the target of a copy. However, it may be the source of a copy in which case the original remains active.
**configuration delete**

**configuration delete <filename>**

Deletes a configuration file.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>filename</td>
<td>Name of file to delete.</td>
</tr>
</tbody>
</table>

| Default            | N/A                          |
| Configuration Mode | Config                       |
| History            | 3.1.0000                     |
| Role               | admin                        |

**Example**

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

**Related Commands**

- show configuration

**Notes**

- This command does not affect the current running configuration
- The active configuration file may not be deleted
### configuration fetch

**command:** configuration fetch `<URL>` `[<name>]`

Downloads a configuration file from a remote host.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>URL</th>
<th>HTTP, HTTPS, FTP, TFTP, SCP and SFTP are supported. Example: scp://username[:password]@hostname/path/filename.</th>
</tr>
</thead>
<tbody>
<tr>
<td>name</td>
<td>The configuration file name.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Default</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuration Mode</td>
<td>Config</td>
</tr>
<tr>
<td>History</td>
<td>3.1.0000</td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
</tr>
</tbody>
</table>

**Example**

```
switch (config) # configuration fetch scp://root:password@192.168.10.125/tmp/conf1
switch (config) #
```

**Related Commands**

- configuration switch-to

**Notes**

- The downloaded file should not override the active configuration file, using the `<name>` parameter
- If no name is specified for a configuration fetch, it is given the same name as it had on the server
- No configuration file may have the name “active”
configuration jump-start

configuration jump-start

Runs the initial-configuration wizard.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>N/A</td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Config</td>
</tr>
<tr>
<td>History</td>
<td>3.1.0000</td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
</tr>
</tbody>
</table>

**Example**

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

**Related Commands**

N/A

**Notes**

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

configuration merge <filename>

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

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>filename</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>N/A</td>
<td>Name of file from which to merge settings.</td>
</tr>
<tr>
<td>Configuration Mode</td>
<td></td>
<td>Config</td>
<td></td>
</tr>
<tr>
<td>History</td>
<td></td>
<td>3.1.0000</td>
<td></td>
</tr>
<tr>
<td>Role</td>
<td></td>
<td>admin</td>
<td></td>
</tr>
</tbody>
</table>
| Example             |          |          | switch (config) # configuration merge new-config-file  
|                     |          |          | switch (config) #                                  |
| Related Commands    |          |          |                                                  |
| Notes               |          |          | • No configuration files are modified during this process  
|                     |          |          | • The configuration name must be a non-active configuration file |
configuration move

configuration move <source name> <dest name>

Moves a configuration file.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>source name</th>
<th>Old name of file to move.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>dest name</td>
<td>New name for moved file.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Default</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuration Mode</td>
<td>Config</td>
</tr>
<tr>
<td>History</td>
<td>3.1.0000</td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
</tr>
</tbody>
</table>

Example

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

Related Commands

- show configuration

Notes

- This command does not affect the current running configuration
- The active configuration file may not be the target of a move
configuration new

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

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

Syntax Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>filename</td>
<td>Names for new configuration file.</td>
</tr>
<tr>
<td>factory</td>
<td>Creates new file with only factory defaults.</td>
</tr>
<tr>
<td>keep-basic</td>
<td>Keeps licenses and host keys.</td>
</tr>
<tr>
<td>keep-connect</td>
<td>Keeps configuration necessary for connectivity (interfaces, routes, and ARP).</td>
</tr>
</tbody>
</table>

Default: Keeps licenses and host keys

Configuration Mode: Config

History: 3.1.0000

Role: admin

Example

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

Related Commands

- show configuration

Notes
configuration switch-to

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

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

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>no-reboot</th>
<th>Forces configuration change without rebooting the switch</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>N/A</td>
<td></td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Config</td>
<td></td>
</tr>
<tr>
<td>History</td>
<td>3.1.0000</td>
<td></td>
</tr>
<tr>
<td></td>
<td>3.6.1002</td>
<td>Added “no-reboot” option</td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
<td></td>
</tr>
<tr>
<td>Example</td>
<td>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) #</td>
<td></td>
</tr>
<tr>
<td>Related Commands</td>
<td>show configuration files</td>
<td></td>
</tr>
<tr>
<td>Notes</td>
<td>• The current running configuration is lost and not automatically saved to the previous active configuration file. • When running the command without the “no-reboot” parameter, the user is prompted to OK a reboot. If the answer is “yes”, the configuration is replaced and the switch is rebooted immediately.</td>
<td></td>
</tr>
</tbody>
</table>
configuration text fetch

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

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

Syntax Description

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>apply</th>
<th>Applies the file to the running configuration (i.e. executes the commands in it). This option has the following parameters:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>• discard: Does not keep downloaded configuration text file after applying it to the system</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• fail-continue: If applying commands, continues execution even if one of them fails</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• overwrite: If saving the file and the filename already exists, replaces the old file</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• verbose: Displays all commands being executed and their output instead of just those that get errors</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>filename</th>
<th>Specifies filename for saving downloaded text file.</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>overwrite</th>
<th>Downloads the file and saves it using the same name it had on the server. This option has the following parameters:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>• apply: Applies the downloaded configuration to the running system</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• filename: Specifies filename for saving downloaded text file</td>
</tr>
</tbody>
</table>

Default N/A

Configuration Mode Config

History

<table>
<thead>
<tr>
<th>History</th>
<th>3.2.1000</th>
<th>First version</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>3.2.3000</td>
<td>Updated command</td>
</tr>
</tbody>
</table>

Role admin

Example

switch (config) # configuration fetch text scp://username[:password]@hostname/path/filename

Related Commands N/A

Notes
configuration text file

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

Performs operations on text-based configuration files.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>filename &lt;file&gt;</td>
<td>Specifies the filename.</td>
</tr>
<tr>
<td>apply</td>
<td>Applies the configuration on the system.</td>
</tr>
<tr>
<td>fail-continue</td>
<td>Continues execution of the commands even if some commands fail.</td>
</tr>
<tr>
<td>verbose</td>
<td>Displays all commands being executed and their output, instead of just those that get errors.</td>
</tr>
<tr>
<td>delete</td>
<td>Deletes the file.</td>
</tr>
<tr>
<td>rename &lt;filename&gt;</td>
<td>Renames the file.</td>
</tr>
<tr>
<td>upload &lt;URL&gt;</td>
<td>Supported types are HTTP, HTTPS, FTP, TFTP, SCP and SFTP. For example: scp://user-name[:password]@hostname/path/filename.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Default</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuration Mode</td>
<td>Config</td>
</tr>
<tr>
<td>History</td>
<td>3.1.0000</td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
</tr>
</tbody>
</table>

Example

```
switch (config) # configuration text file my-config-file delete
switch (config) #
```

Related Commands

show configuration files

Notes
configuration text generate

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

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

### Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>active</td>
<td>Generates from currently active configuration.</td>
</tr>
<tr>
<td>running</td>
<td>Uses running configuration.</td>
</tr>
<tr>
<td>saved</td>
<td>Uses saved configuration.</td>
</tr>
<tr>
<td>file &lt;filename&gt;</td>
<td>Generates from inactive saved configuration.</td>
</tr>
<tr>
<td>save</td>
<td>Saves new file to local persistent storage.</td>
</tr>
<tr>
<td>upload &lt;URL&gt;</td>
<td>Supported types are HTTP, HTTPS, FTP, TFTP, SCP and SFTP. For example: scp://username[;password]@hostname/path/filename.</td>
</tr>
</tbody>
</table>

### Default

N/A

### Configuration Mode

Config

### History

3.1.0000

### Role

admin

### Example

```
switch (config) # configuration text generate file initial.prev save example
switch (config) # show configuration files
initial (active)
initial.prev
initial.bak
Active configuration: initial
Unsaved changes: yes
switch (config) #
```

### Related Commands

show configuration files

### Notes
configuration upload

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

Uploads a configuration file to a remote host.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>active</th>
<th>Upload the active configuration file.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>N/A</td>
<td></td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Config</td>
<td></td>
</tr>
<tr>
<td>History</td>
<td>3.1.0000</td>
<td></td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
<td></td>
</tr>
</tbody>
</table>

Example

```
switch (config) # configuration upload active scp://root:password@192.168.10.125/tmp/conf1
switch (config) #
```

<table>
<thead>
<tr>
<th>Related Commands</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Notes</td>
<td>No configuration file may have the name “active”.</td>
</tr>
</tbody>
</table>
configuration write

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

Saves the running configuration to the active configuration file.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>local</td>
<td>Saves the running configuration locally (same as “write memory local”)</td>
</tr>
<tr>
<td>to &lt;filename&gt;</td>
<td>Saves the running configuration to a new file under a different name and makes it the active file</td>
</tr>
<tr>
<td>no-switch</td>
<td>Saves the running configuration to this file but keep the current one active</td>
</tr>
</tbody>
</table>

Default: N/A

Configuration Mode: Config

History: 3.1.0000

Role: admin

Example:

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

Related Commands: write

Notes
### write

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

Saves or displays the running configuration.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<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>
</tbody>
</table>

**Default**  
N/A

**Configuration Mode**  
Config

**History**  
3.1.0000

**Role**  
admin

**Example**

```bash
switch (config) # write terminal  
## Running database "initial"  
## Generated at 2014/05/27 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) #
```
<table>
<thead>
<tr>
<th><strong>Related Commands</strong></th>
<th>show running-config</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>configuration write</td>
</tr>
</tbody>
</table>

**Notes**
**show configuration**

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

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

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>audit</td>
<td>Displays settings for configuration change auditing.</td>
<td></td>
</tr>
<tr>
<td>files [&lt;filename&gt;]</td>
<td>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.</td>
<td></td>
</tr>
<tr>
<td>running</td>
<td>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.</td>
<td></td>
</tr>
<tr>
<td>text files</td>
<td>Displays names of available text-based configuration files.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Default</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuration Mode</td>
<td>Config</td>
</tr>
<tr>
<td>History</td>
<td>3.1.0000</td>
</tr>
<tr>
<td></td>
<td>3.3.5006</td>
</tr>
<tr>
<td>Role</td>
<td>monitor/admin</td>
</tr>
</tbody>
</table>
switch (config) # show configuration
##
## Active saved database "newcon"
## Generated at 20114/05/25 10:18:52 +0000
## Hostname: switch-3cc29c
##
##
## Network interface configuration
##
interface mgmt0 comment ""
interface mgmt0 create
interface mgmt0 dhcp
interface mgmt0 display
interface mgmt0 duplex auto
interface mgmt0 mtu 1500
no interface mgmt0 shutdown
interface mgmt0 speed auto
no interface mgmt0 zeroconf
switch (config) #
# show running-config

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

Displays commands to recreate current running configuration.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>expanded</th>
<th>Displays commands in expanded format without compressing ranges</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>protocol</td>
<td>Only displays commands relating to the specified protocol</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Default</th>
<th>N/A</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Configuration Mode</th>
<th>Config</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>History</th>
<th>3.1.0000</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>3.3.4402 Removed “full” parameter</td>
</tr>
<tr>
<td></td>
<td>3.6.2002 Updated Example and added parameters</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Role</th>
<th>monitor/admin</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Example</th>
</tr>
</thead>
</table>

```
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
## ...
switch (config) #
```
4.5  Logging

4.5.1  Monitor

➢  To print logging events to the terminal:

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

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

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

```
Wed Jul 10 11:30:42 2013: Interface IB1/17 changed state to DOWN
Wed Jul 10 11:30:43 2013: Interface IB1/18 changed state to DOWN
```

To see a list of the events, refer to Table 25, “Supported Event Notifications and MIB Mapping,” on page 307.

4.5.2  Remote Logging

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

   Step 1.  Enter Config mode. Run:

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

   Step 2.  Set remote syslog server. Run

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

logging port

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

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

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>destination-port</th>
<th>Range: 1-65535</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hostname</td>
<td>Max 64 characters</td>
<td></td>
</tr>
</tbody>
</table>

**Default**

514 (UDP)

**Configuration Mode**

Config

**History**

3.6.2002

**Role**

admin

**Example**

switch (config) # logging 10.0.0.1 port 105

**Related Commands**

logging <syslog IPv4 address/hostname> trap

**Notes**
logging trap

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

Enables (by setting the IPv4 address/hostname) sending logging messages, with ability to filter the logging messages according to their classes. The no form of the command stops sending messages to the remote syslog server.
<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>syslog IPv4 address/hostname</th>
<th>IPv4 address/hostname of the remote syslog server. Hostname is limited to 64 characters</th>
</tr>
</thead>
</table>

**log-level**

- alert - alert notification, action must be taken immediately
- crit - critical condition
- debug - debug level messages
- emerg - system is unusable (emergency)
- err - error condition
- info - informational condition
- none - disables the logging locally and remotely
- notice - normal, but significant condition
- warning - warning condition

**class**

Sets or removes a per-class override on the logging level. All classes which do not have an override set will use the global logging level set with “logging local <log level>”. Classes that do have an override will do as the override specifies. If “none” is specified for the log level, MLNX-OS will not log anything from this class.

Classes available:

- iss-modules - protocol stack
- mgmt-back - system management back-end
- mgmt-core - system management core
- mgmt-front - system management front-end
- mlx-daemons - management daemons
- sx-sdk - switch SDK

**log-level**

- alert - alert notification, action must be taken immediately
- crit - critical condition
- debug - debug level messages
- emerg - system is unusable (emergency)
- err - error condition
- info - informational condition
- none - disables the logging locally and remotely
- notice - normal, but significant condition
- warning - warning condition

**Default**

Remote logging is disabled

**Configuration Mode**

Config

**History**

3.1.0000
Role

admin

Example

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

Related Commands

  show logging
  logging local override
  logging <syslog IPv4 address/hostname> port

Notes
### logging debug-files

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

Configures settings for debug log files.

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

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

| update \{<number> \| current\} | Uploads a local debug-log file to a remote host.  
|• current: Uploads log file “messages” to a remote host  
|• number: Uploads compressed log file “debug.<number>.gz” to a remote host. Range is 1-10  

| upload | Uploads debug log file to a remote host  

| log-file | Possible values: 1-7, or current  

| upload URL | HTTP, HTTPS, FTP, TFTP, SCP and SFTP are supported (e.g.: scp://username[:password]@hostname/path/filename)  

| Default | N/A  

| Configuration Mode | Config  

| History | 3.3.4150  

| Role | admin  

---

### Syntax Description

- **delete \{current \| oldest\}**
  - Deletes certain debug-log files.
  - **current**: Deletes the current active debug-log file.
  - **oldest**: Deletes some of the oldest debug-log files.

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

- **update \{<number> \| current\}**
  - Uploads a local debug-log file to a remote host.
  - **current**: Uploads log file “messages” to a remote host.
  - **number**: Uploads compressed log file “debug.<number>.gz” to a remote host. Range is 1-10.

- **upload**
  - Uploads debug log file to a remote host.

- **log-file**
  - Possible values: 1-7, or current.

- **upload URL**
  - HTTP, HTTPS, FTP, TFTP, SCP and SFTP are supported (e.g.: scp://username[:password]@hostname/path/filename).

| Default | N/A  

| Configuration Mode | Config  

| History | 3.3.4150  

| Role | admin  

---

### Configuration Mode

- **Config**

### History

- **3.3.4150**

### Role

- **admin**
### Example

```
switch (config) # logging debug-files delete current
switch (config) #
```

### Related Commands

### Notes
### logging local override

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

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

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

**Default** Override is disabled.

**Configuration Mode** Config
### History

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.1.0000</td>
<td>Added debug-module class</td>
</tr>
<tr>
<td>3.3.4150</td>
<td>Changed iss-modules with protocol-stack</td>
</tr>
</tbody>
</table>

### Role

- **admin**

### Example

```plaintext
test (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.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>enable</th>
<th>Specifies whether to include an additional field in each log message that shows the number of seconds since the Epoch or not.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>f-digit</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>w-digit</td>
<td>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.</td>
</tr>
</tbody>
</table>

Default disabled
Configuration Mode Config
History 3.1.0000
Role admin
Example

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

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

Deletes the current or oldest log files.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>current</td>
<td>Deletes current log file.</td>
</tr>
<tr>
<td>oldest</td>
<td>Deletes oldest log file.</td>
</tr>
<tr>
<td>number of files</td>
<td>Sets the number of files to be deleted.</td>
</tr>
</tbody>
</table>

**Default**
CLI commands and audit message are set to notice logging level

**Configuration Mode**
Config

**History**
3.1.0000

**Role**
admin

**Example**
```
switch (config) # logging files delete current
switch (config) #
```

**Related Commands**
- show logging
- show log files

**Notes**
logging files rotation

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

Sets the rotation criteria of the logging files.

| Syntax Description | freq | Sets rotation criteria according to time. Possible options are:
| | | • Daily
| | | • Weekly
| | | • Monthly

| | size-mb | Sets rotation criteria according to size in megabytes. The range is 1-9999.

| | size-percentage | Sets rotation criteria according to size in percentage of the partition where the logging files are kept in. The percentage given is truncated to three decimal points (thousandths of a percent).

| | force | Forces an immediate rotation of the log files. This does not affect the schedule of auto-rotation if it was done based on time: the next automatic rotation will still occur at the same time for which it was previously scheduled. Naturally, if the auto-rotation was based on size, this will delay it somewhat as it reduces the size of the active log file to zero.

| | number-of-files | The number of log files will be kept. If the number of log files ever exceeds this number (either at rotation time, or when this setting is lowered), the system will delete as many files as necessary to bring it down to this number, starting with the oldest.

| Default | 10 files are kept by default with rotation criteria of 5% of the log partition size

| Configuration Mode | Config
| History | 3.1.0000
| Role | admin
Example

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

Related Commands

- show logging
- show log files

Notes
# logging files upload

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

Uploads a log file to a remote host.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>current</th>
<th>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.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>file-number</td>
<td>An archived log file. The archived log file will have the name “messages&lt;n&gt;.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.</td>
</tr>
<tr>
<td></td>
<td>url</td>
<td>Uploads URL path. FTP, TFTP, SCP, and SFTP are supported. For example: scp://username[:password]@hostname/path/filename.</td>
</tr>
</tbody>
</table>

**Default**

10 files are kept by default with rotation criteria of 5% of the log partition size

**Configuration Mode**

Config

**History**

3.1.0000

**Role**

admin

**Example**

switch (config) # logging files upload 1 scp://admin@scpserver

**Related Commands**

show logging

show log files

**Notes**
### logging format

`logging format {standard | welf [fw-name <hostname>]}`

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

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

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>standard</th>
<th>Standard format.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>welf</td>
<td>WebTrends Enhanced Log file (WELF) format.</td>
</tr>
<tr>
<td></td>
<td>hostname</td>
<td>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.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Default</th>
<th>standard</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Configuration Mode</th>
<th>Config</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>History</th>
<th>3.1.0000</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Role</th>
<th>admin</th>
</tr>
</thead>
</table>

**Example**

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

**Related Commands**

- show logging

**Notes**
logging level

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

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

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>cli commands</th>
<th>Sets the severity level at which CLI commands which the user executes are logged.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>audit mgmt</td>
<td>Sets the severity level at which all network management audit messages are logged.</td>
</tr>
</tbody>
</table>

| log-level | • alert - alert notification, action must be taken immediately  
|           | • crit - critical condition  
|           | • debug - debug level messages  
|           | • emerg - system is unusable (emergency)  
|           | • err - error condition  
|           | • info - informational condition  
|           | • none - disables the logging locally and remotely  
|           | • notice - normal, but significant condition  
|           | • warning - warning condition |

Default: CLI commands and audit message are set to notice logging level

Configuration Mode: Config

History: 3.1.0000

Role: admin

Example:

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

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

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

Syntax Description

facility
- mgmt-front
- mgmt-back
- mgmt-core
- events
- sx-sdk
- mlnx-daemons
- iss-modules

priority-level
- none
- emerg
- alert
- crit
- err
- warning
- notice
- info
- debug

Default
no logging monitor

Configuration Mode
Config

History
3.3.4000

Role
admin

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

Related Commands

Notes
logging receive

logging receive
no logging receive

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

Syntax Description | N/A
--- | ---
Default | Receiving logging is disabled
Configuration Mode | Config
History | 3.1.0000
Role | admin

Example

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

Related Commands

show logging
logging local
logging local override

Notes

- This does not log to the console TTY port
- In-band management should be enabled in order to open a channel from the host to the CPU
- If enabled, only log messages matching or exceeding the minimum severity specified with the “logging local” command will be logged, regardless of what is sent from the remote host
logging trap

logging trap <log-level>
no logging trap

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

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>log-level</td>
<td>The minimum severity level for all configured syslog servers:</td>
</tr>
<tr>
<td></td>
<td>• none – disable logging</td>
</tr>
<tr>
<td></td>
<td>• emerg – emergency: system is unusable</td>
</tr>
<tr>
<td></td>
<td>• alert – action must be taken immediately</td>
</tr>
<tr>
<td></td>
<td>• crit – critical conditions</td>
</tr>
<tr>
<td></td>
<td>• err – error conditions</td>
</tr>
<tr>
<td></td>
<td>• warning – warning conditions</td>
</tr>
<tr>
<td></td>
<td>• notice – normal but significant condition</td>
</tr>
<tr>
<td></td>
<td>• info – informational messages</td>
</tr>
<tr>
<td></td>
<td>• debug – debug-level messages</td>
</tr>
</tbody>
</table>

Default: Receiving logging is disabled

Configuration Mode: Config

History: 3.1.0000

Role: admin

Example:
```
switch (config) # logging trap info
switch (config) #
```

Related Commands

Notes
**show logging**

**show logging**

Displays the logging configurations.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>N/A</td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Any Command Mode</td>
</tr>
<tr>
<td>History</td>
<td>3.1.0000</td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
</tr>
</tbody>
</table>

**Example**

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

**Related Commands**

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

**Notes**
show log

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

Displays the log file with optional filter criteria.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>continues</td>
<td>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.</td>
</tr>
<tr>
<td>files</td>
<td>Displays the list of log files.</td>
</tr>
<tr>
<td>&lt;file-number&gt;</td>
<td>Displays an archived log file, where the number may range from 1 up to the number of archived log files available.</td>
</tr>
<tr>
<td>[not] matching &lt;reg-exp&gt;</td>
<td>The file is piped through a LINUX “grep” utility to only include lines either matching, or not matching, the provided regular expression.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Default</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuration Mode</td>
<td>Any Command Mode</td>
</tr>
<tr>
<td>History</td>
<td>3.1.0000</td>
</tr>
<tr>
<td>3.3.4402</td>
<td>Updated example and added note</td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
</tr>
</tbody>
</table>
| Example | switch (config) # show log matching "Executing|Action"
Jan 19 10:55:38 arc-switch14 cli28202: [cli.NOTICE]: user admin: Executing command: en
Jan 19 11:19:32 arc-switch14 cli28202: [cli.NOTICE]: user admin: Executing command: image install image=SX_PPC_M460EX-ppc-m460ex-20140119-115026.img
Jan 19 11:19:32 arc-switch14 mgmtd4064: [mgmtd.NOTICE]: Action ID 326: requested by: user admin (System Administrator) via CLI
Jan 19 11:19:32 arc-switch14 mgmtd4064: [mgmtd.NOTICE]: Action ID 326: descr: install system software image
Jan 19 11:19:32 arc-switch14 mgmtd4064: [mgmtd.NOTICE]: Action ID 326: param: switch next boot location after install: no
switch (config) # |
<table>
<thead>
<tr>
<th>Related Commands</th>
<th>logging fields</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>logging files rotation</td>
</tr>
<tr>
<td></td>
<td>logging level</td>
</tr>
<tr>
<td></td>
<td>logging local</td>
</tr>
<tr>
<td></td>
<td>logging receive</td>
</tr>
<tr>
<td></td>
<td>logging <code>&lt;syslog IPv4 address/hostname&gt;</code></td>
</tr>
<tr>
<td></td>
<td>show logging</td>
</tr>
</tbody>
</table>

| Notes | When using a regular expression containing | (OR), the expression should be surrounded by quotes (“<expression>”), otherwise it is parsed as filter (PIPE) command. |
4.6 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}
```
4.6.1 Commands

**debug ethernet all**

d 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.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>N/A</td>
</tr>
<tr>
<td><strong>Configuration Mode</strong></td>
<td>Config</td>
</tr>
<tr>
<td>History</td>
<td>3.3.4150</td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
</tr>
</tbody>
</table>
| **Example**         | switch (config) # debug ethernet all  
switch (config) # |

**Related Commands**

**Notes**
debug ethernet dcbx

ddebug 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.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>all</th>
<th>Enables all traces.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>management</td>
<td>Management messages.</td>
</tr>
<tr>
<td></td>
<td>fail-all</td>
<td>All failure traces.</td>
</tr>
<tr>
<td></td>
<td>control-panel</td>
<td>Control plane traces.</td>
</tr>
<tr>
<td></td>
<td>tlv</td>
<td>TLV related trace configuration.</td>
</tr>
</tbody>
</table>

Default: N/A
Configuration Mode: Config
History: 3.3.4150
Role: admin
Example:

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

Related Commands

Notes
debug ethernet ip all

debug ethernet ip all

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

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>N/A</td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Config</td>
</tr>
<tr>
<td>History</td>
<td>3.3.4150</td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
</tr>
</tbody>
</table>
| Example            | switch (config) # debug ethernet ip all  
switch (config) # |

Related Commands

Notes
debug ethernet ip arp all

debug ethernet ip arp all
no debug ethernet ip arp all

Enables the trace level for ARP.
The no form of the command disables the trace level for ARP.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>N/A</td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Config</td>
</tr>
<tr>
<td>History</td>
<td>3.3.4150</td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
</tr>
</tbody>
</table>
| Example             | switch (config) # debug ethernet ip arp all
switch (config) # |

Related Commands

Notes
**debug ethernet ip bgp**

```
debug ethernet ip bgp {all | control-path | dampening | graceful-restart | internal | keep-alive | receive | resources | rtm | transmit | update}
no debug ethernet ip bgp {all | control-path | dampening | graceful-restart | internal | keep-alive | receive | resources | rtm | transmit | update}
```

Enables the trace level for BGP. The no form of the command disables tracking a specified level.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>all</td>
<td>Enable track traces</td>
</tr>
<tr>
<td>control-path</td>
<td>Control path dump trace</td>
</tr>
<tr>
<td>dampening</td>
<td>Dampening information</td>
</tr>
<tr>
<td>graceful-restart</td>
<td>Graceful-restart events</td>
</tr>
<tr>
<td>internal</td>
<td>Internal events</td>
</tr>
<tr>
<td>keep-alive</td>
<td>Keep-alive packets exchange</td>
</tr>
<tr>
<td>neighbor</td>
<td>Peer connection/state changes traces</td>
</tr>
<tr>
<td>receive</td>
<td>All received packets</td>
</tr>
<tr>
<td>resources</td>
<td>OS Resource trace</td>
</tr>
<tr>
<td>rtm</td>
<td>Route change notifications</td>
</tr>
<tr>
<td>transmit</td>
<td>All transmitted packets</td>
</tr>
<tr>
<td>update</td>
<td>Update packets exchange</td>
</tr>
</tbody>
</table>

**Default**  
N/A

**Configuration Mode**  
Config

**History**  
3.3.4150

**Role**  
admin

**Example**
```
switch (config) # debug ethernet ip arp all
switch (config) #
```

**Related Commands**

**Notes**
debug ethernet ip dhcp-relay

\[\text{debug ethernet ip dhcp-relay \{all | error\}}\]
\[\text{no debug ethernet ip dhcp-relay \{all | error\}}\]

Configures the trace level for DHCP.
The no form of the command disables tracking a specified level.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>all</th>
<th>Enables track traces</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>error</td>
<td>Error code debug messages</td>
</tr>
</tbody>
</table>

**Default**
N/A

**Configuration Mode**
Config

**History**
3.3.4150

**Role**
admin

**Example**
switch (config) # debug ethernet ip dhcp-relay all
switch (config) #

**Related Commands**

**Notes**
```plaintext
debugethernet ip igmp-l3

debugethernet ip igmp-l3 {all | control-plane | data-path | fail-all | init-shut | management | memory | packet-path | resources}
no debugethernet ip igmp-l3 {all | control-plane | data-path | fail-all | init-shut | management | memory | packet-path | resources}

Configures the trace level for IGMP.
The no form of the command disables tracking a specified level.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<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>
</tbody>
</table>

**Default**: N/A

**Configuration Mode**: Config

**History**: 3.3.4150

**Role**: admin

**Example**

```
switch (config) # debugethernet ip igmp-l3 all
switch (config) #
```

**Related Commands**

**Notes**

**debug ethernet ip igmp-snooping**

```
depth 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.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>all</td>
<td>Enable track traces</td>
</tr>
<tr>
<td>forward-db-messages</td>
<td>Forwarding database messages</td>
</tr>
<tr>
<td>group-info</td>
<td>Group information messages</td>
</tr>
<tr>
<td>init-shut</td>
<td>Init and shutdown messages</td>
</tr>
<tr>
<td>packet-dump</td>
<td>Packet dump messages</td>
</tr>
<tr>
<td>query</td>
<td>Query related messages</td>
</tr>
<tr>
<td>source-info</td>
<td>Source information messages</td>
</tr>
<tr>
<td>system-resources-management</td>
<td>System resources management messages</td>
</tr>
<tr>
<td>timer</td>
<td>Timer messages</td>
</tr>
<tr>
<td>vlan-info</td>
<td>VLAN information messages</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Default</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuration Mode</td>
<td>Config</td>
</tr>
<tr>
<td>History</td>
<td>3.3.4150</td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
</tr>
</tbody>
</table>

**Example**

```
switch (config) # debug ethernet ip igmp-snooping all
switch (config) #
```

**Related Commands**

**Notes**
debug ethernet ip interface

debbug 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.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>all</td>
<td>Enable track traces</td>
</tr>
<tr>
<td>arp-packet-dump</td>
<td>ARP packet dump trace</td>
</tr>
<tr>
<td>buffer</td>
<td>Buffer trace</td>
</tr>
<tr>
<td>enet-packet-dump</td>
<td>ENET packet dump trace</td>
</tr>
<tr>
<td>error</td>
<td>Trace error messages</td>
</tr>
<tr>
<td>fail-all</td>
<td>All failures including Packet Validation Trace</td>
</tr>
<tr>
<td>filter</td>
<td>Lower layer traces</td>
</tr>
<tr>
<td>trace-error</td>
<td>Trace error messages</td>
</tr>
<tr>
<td>trace-event</td>
<td>Trace event messages</td>
</tr>
</tbody>
</table>

Default: N/A

Configuration Mode: Config

History: 3.3.4150

Role: admin

Example:
switch (config) # debug ethernet ip interface all
switch (config) #
debug ethernet ip ospf

debug ethernet ip ospf \{adjacency \| all \| configuration \| ddp-packet \| helper \| Interface \| ism \| lrq-packet \| lsa_packet \| lsu-packet\}

Configures the trace level for OSPF.
The no form of the command disables tracking a specified level.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>adjacency</th>
<th>Adjacency formation debug messages</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>all</td>
<td>Enable track traces</td>
</tr>
<tr>
<td></td>
<td>configuration</td>
<td>Configuration debug messages</td>
</tr>
<tr>
<td></td>
<td>ddp-packet</td>
<td>DDP packet debug messages</td>
</tr>
<tr>
<td></td>
<td>helper</td>
<td>Helper debug messages</td>
</tr>
<tr>
<td></td>
<td>Interface</td>
<td>Interface debug messages</td>
</tr>
<tr>
<td></td>
<td>ism</td>
<td>Interface State Machine debug messages</td>
</tr>
<tr>
<td></td>
<td>lrq-packet</td>
<td>Link State Request Packet debug messages</td>
</tr>
<tr>
<td></td>
<td>lsa_packet</td>
<td>Link State Acknowledge Packet debug messages</td>
</tr>
<tr>
<td></td>
<td>lsu-packet</td>
<td>Link State Update Packet debug messages</td>
</tr>
<tr>
<td></td>
<td>nsm</td>
<td>Neighbor State Machine debug messages</td>
</tr>
</tbody>
</table>

**Default**: N/A

**Configuration Mode**: Config

**History**: 3.3.4150

**Role**: admin

**Example**:  
```
switch (config) # debug ethernet ip ospf all
switch (config) #
```

**Related Commands**

**Notes**
debug ethernet lacp

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

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

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>all</th>
<th>all-resource</th>
<th>data-path</th>
<th>fail-all</th>
<th>init-shut</th>
<th>management</th>
<th>memory</th>
<th>packet</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Enables all traces.</td>
<td>BPDU related messages.</td>
<td>Init and shutdown traces.</td>
<td>Management messages.</td>
<td>Memory related messages.</td>
<td>IP packet dump trace.</td>
<td>All failure traces.</td>
<td>OS resource trace.</td>
</tr>
</tbody>
</table>

**Default**

N/A

**Configuration Mode**

Config

**History**

3.3.4150

**Role**

admin

**Example**

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

**Related Commands**

- 

**Notes**

- 

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.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>all</th>
<th>Enables all traces.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>control-panel</td>
<td>Control plane traces.</td>
</tr>
<tr>
<td></td>
<td>critical-event</td>
<td>Critical traces.</td>
</tr>
<tr>
<td></td>
<td>data-path</td>
<td>IP packet dump trace.</td>
</tr>
<tr>
<td></td>
<td>fail-all</td>
<td>All failure traces.</td>
</tr>
<tr>
<td></td>
<td>init-shut</td>
<td>Init and shutdown traces.</td>
</tr>
<tr>
<td></td>
<td>management</td>
<td>Management messages.</td>
</tr>
<tr>
<td></td>
<td>memory</td>
<td>Memory related messages.</td>
</tr>
<tr>
<td></td>
<td>neigh-add</td>
<td>Neighbor add traces.</td>
</tr>
<tr>
<td></td>
<td>neigh-age-out</td>
<td>Neighbor ageout traces.</td>
</tr>
<tr>
<td></td>
<td>neigh-del</td>
<td>Neighbor delete traces.</td>
</tr>
<tr>
<td></td>
<td>neigh-drop</td>
<td>Neighbor drop traces.</td>
</tr>
<tr>
<td></td>
<td>neigh-updt</td>
<td>Neighbor update traces.</td>
</tr>
<tr>
<td></td>
<td>tlv</td>
<td>TLV related trace configuration</td>
</tr>
</tbody>
</table>

**Default**
N/A

**Configuration Mode**
Config

**History**
3.3.4150

**Role**
admin

**Example**
```
switch (config) # debug ethernet lldp all
switch (config) #
```
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.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>N/A</td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Config</td>
</tr>
<tr>
<td>History</td>
<td>3.3.4150</td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
</tr>
</tbody>
</table>
| Example            | switch (config) # debug ethernet port all
switch (config) # |

Related Commands

Notes
**debug ethernet qos**

```
depth ethernet qos {all | all-resource | control-panel | fail-all | filters | init-shut | management | memory | packet}

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

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

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>all</td>
<td>Enables all traces.</td>
</tr>
<tr>
<td>all-resource</td>
<td>OS resource traces.</td>
</tr>
<tr>
<td>control-panel</td>
<td>Control plane traces.</td>
</tr>
<tr>
<td>fail-all</td>
<td>All failure traces.</td>
</tr>
<tr>
<td>filters</td>
<td>Lower layer traces.</td>
</tr>
<tr>
<td>init-shut</td>
<td>Init and shutdown traces.</td>
</tr>
<tr>
<td>management</td>
<td>Management messages.</td>
</tr>
<tr>
<td>memory</td>
<td>Memory related messages.</td>
</tr>
<tr>
<td>packet</td>
<td>BPDU related messages.</td>
</tr>
</tbody>
</table>

**Default**

N/A

**Configuration Mode**

Config

**History**

3.3.4150

**Role**

admin

**Example**

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

**Related Commands**

**Notes**
debug ethernet spanning-tree


Configures the trace level for spanning-tree.
The no form of the command disables the configured spanning-tree debug traces.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>all</th>
<th>Enables all traces.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>error</td>
<td>Error messages trace.</td>
</tr>
<tr>
<td></td>
<td>event</td>
<td>Events related messages.</td>
</tr>
<tr>
<td></td>
<td>filters</td>
<td>Lower later traces.</td>
</tr>
<tr>
<td></td>
<td>init-shut</td>
<td>Init and shutdown traces.</td>
</tr>
<tr>
<td></td>
<td>management</td>
<td>Management messages.</td>
</tr>
<tr>
<td></td>
<td>memory</td>
<td>Memory related messages.</td>
</tr>
<tr>
<td></td>
<td>packet</td>
<td>BPDU related messages.</td>
</tr>
<tr>
<td></td>
<td>port-info-state-machine</td>
<td>Port information messages.</td>
</tr>
<tr>
<td></td>
<td>port-receive-state-machine</td>
<td>Port received messages.</td>
</tr>
<tr>
<td></td>
<td>port-role-selection-state-machine</td>
<td>Port role selection messages.</td>
</tr>
<tr>
<td></td>
<td>port-transit-state-machine</td>
<td>Port transition messages.</td>
</tr>
<tr>
<td></td>
<td>port-transmit-state-machine</td>
<td>Port transmission messages.</td>
</tr>
<tr>
<td></td>
<td>protocol-migration-state-machine</td>
<td>Protocol migration messages.</td>
</tr>
<tr>
<td></td>
<td>timers</td>
<td>Timer modules message.</td>
</tr>
</tbody>
</table>

**Default**

N/A

**Configuration Mode**

Config
<table>
<thead>
<tr>
<th>History</th>
<th>3.3.4150</th>
</tr>
</thead>
<tbody>
<tr>
<td>Role</td>
<td>admin</td>
</tr>
<tr>
<td>Example</td>
<td></td>
</tr>
</tbody>
</table>
|           | switch (config) # debug ethernet spanning-tree all  
|           | switch (config) # |

**Related Commands**

**Notes**
debug ethernet vlan

debugethernetvlan{all|fwd|priority|filters}
noddebugethernetvlan{all|fwd|priority|filters}

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

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>all</th>
<th>Enables all traces</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>fwd</td>
<td>Forward.</td>
</tr>
<tr>
<td></td>
<td>priority</td>
<td>Priority.</td>
</tr>
<tr>
<td></td>
<td>filters</td>
<td>Lower layer traces.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Default</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuration Mode</td>
<td>Config</td>
</tr>
<tr>
<td>History</td>
<td>3.3.4150</td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
</tr>
</tbody>
</table>

Example

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

Related Commands

Notes
# 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.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>dcbx</td>
<td>Displays the trace level for spanning tree.</td>
</tr>
<tr>
<td>ip</td>
<td>Displays debug trace level for ethernet routing module.</td>
</tr>
<tr>
<td></td>
<td>• arp</td>
</tr>
<tr>
<td></td>
<td>• dhcp-relay</td>
</tr>
<tr>
<td></td>
<td>• igmp-snooping</td>
</tr>
<tr>
<td></td>
<td>• interface</td>
</tr>
<tr>
<td></td>
<td>• ospf</td>
</tr>
<tr>
<td>lacp</td>
<td>Displays the trace level for LACP.</td>
</tr>
<tr>
<td>lldp</td>
<td>Displays the trace level for LLDP.</td>
</tr>
<tr>
<td>port</td>
<td>Displays the trace level for port.</td>
</tr>
<tr>
<td>qos</td>
<td>Displays the trace level for QoS.</td>
</tr>
<tr>
<td>spanning-tree</td>
<td>Displays the trace level for spanning tree.</td>
</tr>
<tr>
<td>vlan</td>
<td>Displays the trace level for VLAN.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Default</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuration Mode</td>
<td>Any Command Mode</td>
</tr>
<tr>
<td>History</td>
<td>3.3.4150</td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
</tr>
</tbody>
</table>

**Example**
```
switch (config) # show debug ethernet dcbx
dcbx protocol:
  management is ON
  fail-all is ON
  control-panel is ON
  tlv is ON
switch (config) #
```

**Related Commands**

**Notes**
show log debug

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

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

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>continuous</th>
<th>Displays new event log messages as they arrive.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>files</td>
<td>Displays archived debug log files.</td>
</tr>
<tr>
<td></td>
<td>matching</td>
<td>Displays event debug logs that match a given regular expression.</td>
</tr>
<tr>
<td></td>
<td>not</td>
<td>Displays event debug logs that do not meet certain criteria.</td>
</tr>
</tbody>
</table>

Default  N/A
Configuration Mode Any Command Mode
History  3.3.4150
Role  admin

Example

```sh
switch (config) # show log debug
Jun 15 16:20:47 switch-627e4c Issd[6509]: TID 1274844336: [Issd.DEBUG]: NPAPI: >>QoSHwQueueDelete i4IfIndex[137]
Jun 15 16:20:47 switch-627e4c Issd[6509]: TID 1274844336: [Issd.DEBUG]: NPAPI: >>QoSHwQueueDelete i4IfIndex[141]
Jun 15 16:20:47 switch-627e4c Issd[6509]: TID 1274844336: [Issd.DEBUG]: NPAPI: ==FsHwSetSpeed ... 16:20:48 switch-627e4c Issd[6509]: TID 1274844336: [Issd.DEBUG]: NPAPI: ==FsHwGetSpeed sx_api_port_speed_oper_get = 0
Jun 15 16:20:49 switch-627e4c Issd[6509]: TID 1274844336: [Issd.DEBUG]: NPAPI: >>CfaGddConfigPort NS u4IfIndex[89], u1ConfigOption[6]
Jun 15 16:20:49 switch-627e4c Issd[6509]: TID 1274844336: [Issd.DEBUG]: NPAPI: >>CfaGddConfigPort NS u4IfIndex[33], u1ConfigOption[6]
Jun 15 16:20:49 switch-627e4c Issd[6509]: TID 1274844336: [Issd.DEBUG]: NPAPI: >>CfaGddConfigPort NS u4IfIndex[73], u1ConfigOption[6]
Jun 15 16:20:49 switch-627e4c Issd[6509]: TID 1274844336: [Issd.DEBUG]: NPAPI: >>CfaGddConfigPort NS u4IfIndex[121], u1ConfigOption[6]
Jun 15 16:20:49 switch-627e4c Issd[6509]: TID 1274844336: [Issd.DEBUG]: NPAPI: >>CfaGddConfigPort NS u4IfIndex[13], u1ConfigOption[6]
Jun 15 16:20:49 switch-627e4c Issd[6509]: TID 1274844336: [Issd.DEBUG]: NPAPI: >>CfaGddConfigPort NS u4IfIndex[81], u1ConfigOption[6]
Jun 15 16:20:49 switch-627e4c Issd[6509]: TID 1274844336: [Issd.DEBUG]: NPAPI: >>CfaGddConfigPort NS u4IfIndex[65], u1ConfigOption[6]
```

Related Commands

Notes
4.7 Event Notifications

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

4.7.1 Supported Events

Table 25 presents the supported events and maps them to their relevant MIB OID.

**Table 25 - Supported Event Notifications and MIB Mapping**

<table>
<thead>
<tr>
<th>Event Name</th>
<th>Event Description</th>
<th>MIB OID</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>asic-chip-down</td>
<td>ASIC (chip) down</td>
<td>Mellanox-EFM-MIB:asicChipDown</td>
<td>Not supported</td>
</tr>
<tr>
<td>cpu-util-high</td>
<td>CPU utilization has risen too high</td>
<td>Mellanox-EFM-MIB:cpuUtilHigh</td>
<td>N/A</td>
</tr>
<tr>
<td>disk-space-low</td>
<td>File system free space has fallen too low</td>
<td>Mellanox-EFM-MIB:diskSpaceLow</td>
<td>N/A</td>
</tr>
<tr>
<td>health-module-status</td>
<td>Health module status changed</td>
<td>Mellanox-EFM-MIB:systemHealthStatus</td>
<td>N/A</td>
</tr>
<tr>
<td>insufficient-fans</td>
<td>Insufficient amount of fans in system</td>
<td>Mellanox-EFM-MIB:insufficientFans</td>
<td>N/A</td>
</tr>
<tr>
<td>insufficient-fans-recover</td>
<td>Insufficient amount of fans in system recovered</td>
<td>Mellanox-EFM-MIB:insufficientFansRecover</td>
<td>N/A</td>
</tr>
<tr>
<td>insufficient-power</td>
<td>Insufficient power supply</td>
<td>Mellanox-EFM-MIB:insufficientPower</td>
<td>N/A</td>
</tr>
<tr>
<td>interface-down</td>
<td>An interface’s link state has changed to DOWN</td>
<td>RFC1213: linkdown (SNMPv1)</td>
<td>Supported for Ethernet, and management interfaces for 1U and blade systems</td>
</tr>
<tr>
<td>interface-up</td>
<td>An interface’s link state has changed to UP</td>
<td>RFC1213: linkup (SNMPv1)</td>
<td>Supported for Ethernet, and management interfaces for 1U and blade systems</td>
</tr>
<tr>
<td>internal-bus-error</td>
<td>Internal bus (I^2C) error</td>
<td>Mellanox-EFM-MIB:internalBusError</td>
<td>N/A</td>
</tr>
<tr>
<td>liveness-failure</td>
<td>A process in the system is detected as hung</td>
<td>Not implemented</td>
<td>N/A</td>
</tr>
<tr>
<td>low-power</td>
<td>Low power supply</td>
<td>Mellanox-EFM-MIB:lowPower</td>
<td>N/A</td>
</tr>
</tbody>
</table>
4.7.2 Terminal Notifications

➢ To print events to the terminal:

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

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

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

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

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

Step 1. Enter to Config mode. Run:

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

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

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

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

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

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

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

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

```
switch (config) # show email events
```

Failure events for which emails will be sent:
- process-crash: A process in the system has crashed
- unexpected-shutdown: Unexpected system shutdown

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

```
switch (config) #
```

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

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

The last command should generate the following email:

```
-----Original Message-----
From: Admin User [mailto:do-not-reply@switch.]
Sent: Sunday, May 01, 2011 11:17 AM
To: <name>
Subject: System event on switch: Test email for event notification

==== System information:
Hostname: switch
```
... 
Date: 2011/05/01 08:17:29 
Uptime: 17h 8m 28.060s 

This is a test email. 
==== Done.
### 4.7.4 Commands

#### 4.7.4.1 Email Notification

**email autosupport enable**

email autosupport enable
no email autosupport enable

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

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>N/A</td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Config</td>
</tr>
<tr>
<td>History</td>
<td>3.2.3000</td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
</tr>
<tr>
<td>Example</td>
<td>switch (config) # email autosupport enable</td>
</tr>
<tr>
<td>Related Commands</td>
<td>N/A</td>
</tr>
<tr>
<td>Notes</td>
<td>N/A</td>
</tr>
</tbody>
</table>
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.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>event</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>process-crash – a process has crashed</td>
</tr>
<tr>
<td></td>
<td>process-exit – a process unexpectedly exited</td>
</tr>
<tr>
<td></td>
<td>liveness-failure – a process is detected as hung</td>
</tr>
<tr>
<td></td>
<td>cpu-kill-high – CPU utilization has risen too high</td>
</tr>
<tr>
<td></td>
<td>cpu-kill-ok – CPU utilization has fallen back to normal levels</td>
</tr>
<tr>
<td></td>
<td>paging-high – paging activity has risen too high</td>
</tr>
<tr>
<td></td>
<td>paging-ok – paging activity has fallen back to normal levels</td>
</tr>
<tr>
<td></td>
<td>disk-space-low – filesystem free space has fallen too low</td>
</tr>
<tr>
<td></td>
<td>disk-space-ok – filesystem free space is back in the normal range</td>
</tr>
<tr>
<td></td>
<td>memusage-high – memory usage has risen too high</td>
</tr>
<tr>
<td></td>
<td>memusage-ok – memory usage has fallen back to acceptable levels</td>
</tr>
<tr>
<td></td>
<td>netusage-high – network utilization has risen too high</td>
</tr>
<tr>
<td></td>
<td>netusage-ok – network utilization has fallen back to acceptable levels</td>
</tr>
<tr>
<td></td>
<td>disk-td-high – disk I/O per second has risen too high</td>
</tr>
<tr>
<td></td>
<td>disk-td-ok – disk I/O per second has fallen back to acceptable levels</td>
</tr>
<tr>
<td></td>
<td>unexpected-cluster-join – node has unexpectedly joined the cluster</td>
</tr>
<tr>
<td></td>
<td>unexpected-cluster-leave – node has unexpectedly left the cluster</td>
</tr>
<tr>
<td></td>
<td>unexpected-cluster-size – the number of nodes in the cluster is expected</td>
</tr>
<tr>
<td></td>
<td>unexpected-shutdown – unexpected system shutdown</td>
</tr>
<tr>
<td></td>
<td>interface-up – an interface’s link state has changed to up</td>
</tr>
<tr>
<td></td>
<td>interface-down – an interface's link state has changed to down</td>
</tr>
<tr>
<td></td>
<td>user-login – a user has logged into the system</td>
</tr>
<tr>
<td></td>
<td>user-logout – a user has logged out of the system</td>
</tr>
<tr>
<td></td>
<td>health-module-status – health module status</td>
</tr>
<tr>
<td></td>
<td>temperature-too-high – temperature has risen too high</td>
</tr>
<tr>
<td></td>
<td>low-power – low power supply</td>
</tr>
<tr>
<td></td>
<td>low-power-recover – low power supply recover</td>
</tr>
<tr>
<td></td>
<td>insufficient-power – insufficient power supply</td>
</tr>
<tr>
<td></td>
<td>power-redundancy-mismatch – power redundancy mismatch</td>
</tr>
<tr>
<td></td>
<td>insufficient-fans – insufficient amount of fans in system</td>
</tr>
<tr>
<td></td>
<td>insufficient-fans-recover – insufficient amount of fans in system</td>
</tr>
</tbody>
</table>
- asic-chip-down – ASIC (chip) down
- internal-bus-error – internal bus (I2C) error
- internal-link-speed-mismatch – internal links speed mismatch

<table>
<thead>
<tr>
<th>Default</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuration Mode</td>
<td>Config</td>
</tr>
<tr>
<td>History</td>
<td>3.2.3000</td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
</tr>
<tr>
<td>Example</td>
<td>switch (config) # email autosupport event process-crash</td>
</tr>
<tr>
<td>Related Commands</td>
<td>N/A</td>
</tr>
<tr>
<td>Notes</td>
<td></td>
</tr>
</tbody>
</table>
### email autosupport ssl mode

```bash
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.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>none</th>
<th>Does not use TLS to secure auto-support email.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>tls</td>
<td>Uses TLS over the default server port to secure auto-support email and does not send an email if TLS fails.</td>
</tr>
<tr>
<td></td>
<td>tls-none</td>
<td>Attempts TLS over the default server port to secure auto-support email, and falls back on plain-text if this fails.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Default</th>
<th>tls-none</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuration Mode</td>
<td>Config</td>
</tr>
<tr>
<td>History</td>
<td>3.2.3000</td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
</tr>
</tbody>
</table>

**Example**

```bash
switch (config) # email autosupport ssl mode tls
```

**Related Commands**

N/A

**Notes**
email autosupport ssl cert-verify

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

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

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>N/A</td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Config</td>
</tr>
<tr>
<td>History</td>
<td>3.2.3000</td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
</tr>
<tr>
<td>Example</td>
<td>switch (config) # email autosupport ssl cert-verify</td>
</tr>
<tr>
<td>Related Commands</td>
<td>N/A</td>
</tr>
<tr>
<td>Notes</td>
<td></td>
</tr>
</tbody>
</table>
**email autosupport ssl ca-list**

```plaintext
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.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>default_ca_list</td>
<td>Default supplemental CA certificate list.</td>
</tr>
<tr>
<td>none</td>
<td>No supplemental list; uses built-in list only.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Default</th>
<th>Config Mode</th>
<th>History</th>
<th>Role</th>
<th>Example</th>
<th>Related Commands</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>default_ca_list</td>
<td>Config</td>
<td>3.2.3000</td>
<td>admin</td>
<td>switch (config) # email autosupport ssl ca-list default_ca_list</td>
<td>N/A</td>
<td></td>
</tr>
</tbody>
</table>
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.

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

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

email mailhub <hostname or IP address>

no email mailhub

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

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>hostname or IP address</th>
<th>Hostname or IP address.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>N/A</td>
<td></td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Config</td>
<td></td>
</tr>
<tr>
<td>History</td>
<td>3.1.0000</td>
<td></td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
<td></td>
</tr>
</tbody>
</table>

**Example**

```
switch (config) # email mailhub 10.0.8.11
switch (config) # show email
Mail hub: 10.0.8.11
Mail hub port: 25
Domain: (not specified)
Return address: do-not-reply
Include hostname in return address: yes

... switch (config) #
```

**Related Commands**

show email [events]

**Notes**
email mailhub-port

email mailhub-port <hostname or IP address>
no email mailhub-port

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

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

Related Commands

show email

Notes
email notify event

email notify event <event name>
no email notify event <event name>

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

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>event name</th>
<th>Example event names would include “process-crash” and “cpu-util-high”.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>No events are enabled</td>
<td></td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Config</td>
<td></td>
</tr>
<tr>
<td>History</td>
<td>3.1.0000</td>
<td></td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
<td></td>
</tr>
</tbody>
</table>

Example

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

Informational events for which emails will be sent:  
liveness-failure: A process in the system was detected as hung  
process-exit: A process in the system unexpectedly exited  
cpu-util-ok: CPU utilization has fallen back to normal levels  
cpu-util-high: CPU utilization has risen too high  
disk-io-ok: Disk I/O per second has fallen back to acceptable levels  
...  
temperature-too-high: Temperature has risen too high  

All events for which autosupport emails will be sent:  
process-crash: A process in the system has crashed  
liveness-failure: A process in the system was detected as hungswitch  
(config) #  

Related Commands

show email

Notes

This does not affect auto-support emails. Auto-support can be disabled overall, but if it is enabled, all auto-support events are sent as emails.
email notify recipient

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

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

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>email addr</th>
<th>Email address of intended recipient.</th>
</tr>
</thead>
<tbody>
<tr>
<td>class</td>
<td>class</td>
<td>Specifies which types of events are sent to this recipient.</td>
</tr>
<tr>
<td>info</td>
<td>info</td>
<td>Sends informational events to this recipient.</td>
</tr>
<tr>
<td>failure</td>
<td>failure</td>
<td>Sends failure events to this recipient.</td>
</tr>
<tr>
<td>detail</td>
<td>detail</td>
<td>Sends detailed event emails to this recipient.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Default</th>
<th>No recipients are added</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuration Mode</td>
<td>Config</td>
</tr>
<tr>
<td>History</td>
<td>3.1.0000</td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
</tr>
</tbody>
</table>

Example

```
switch (config) # email notify recipient user2@autosupport.mellanox.com
switch (config) # show email
Mail hub: 
Mail hub port: 25
Domain: (not specified)
Return address: user1
Include hostname in return address: no
Dead letter settings:
Save dead.letter files: yes
Dead letter max age: (none)
Email notification recipients:
user2@autosupport.mellanox.com (all events, in detail)
Autosupport emails
Enabled: no
Recipient: autosupport@autosupport.mellanox.com
Mail hub: autosupport.mellanox.com
switch (config) #
```

Related Commands

show email

Notes
**email return-addr**

```
email return-addr <username>
no email domain
```

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

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

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>username</th>
<th>Username.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>do-not-reply</td>
<td></td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Config</td>
<td></td>
</tr>
<tr>
<td>History</td>
<td>3.1.0000</td>
<td></td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
<td></td>
</tr>
</tbody>
</table>

**Example**

```
switch (config) # email return-addr user1
switch (config) # show email
Mail hub:
Mail hub port: 25
Domain: (not specified)
Return address: user1
Include hostname in return address: yes
...
switch (config) #
```

**Related Commands**

show email

**Notes**
**email return-host**

```
email return-host
no email return-host
```

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

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>No return host</td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Config</td>
</tr>
<tr>
<td>History</td>
<td>3.1.0000</td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
</tr>
</tbody>
</table>

**Example**

```
switch (config) # no email return-host
switch (config) # show email
Mail hub:
Mail hub port: 25
Domain: (system domain name)
Return address: my-address
Include hostname in return address: no

Current reply address: host@localdomain

Dead letter settings:
  Save dead.letter files: yes
  Dead letter max age: 5 days

No recipients configured.

Autosupport emails
  Enabled: no
  Recipient: autosupport@autosupport.mellanox.com
  Mail hub: autosupport.mellanox.com
```

**Related Commands**

- show email

**Notes**

This only takes effect if the return address does not contain an “@” character.
email send-test

 email send-test

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

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

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>none</th>
<th>No security mode, operates in plaintext.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>tls</td>
<td>Attempts to use TLS on the regular mailhub port, with STARTTLS. If this fails, it gives up.</td>
</tr>
<tr>
<td></td>
<td>tls-none</td>
<td>Attempts to use TLS on the regular mailhub port, with STARTTLS. If this fails, it falls back on plaintext.</td>
</tr>
</tbody>
</table>

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

**email ssl cert-verify**  
**no email ssl cert-verify**

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

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>N/A</td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Config</td>
</tr>
<tr>
<td>History</td>
<td>3.2.3000</td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
</tr>
<tr>
<td>Example</td>
<td>switch (config) # email ssl cert-verify</td>
</tr>
<tr>
<td>Related Commands</td>
<td>N/A</td>
</tr>
<tr>
<td>Notes</td>
<td>This command has no impact unless TLS is used.</td>
</tr>
</tbody>
</table>
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.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ca-list-name</td>
<td>Specifies CA list name.</td>
</tr>
<tr>
<td>default-ca-list</td>
<td>Uses default supplemental CA certificate list.</td>
</tr>
<tr>
<td>none</td>
<td>Uses no list of supplemental certificates.</td>
</tr>
</tbody>
</table>

Default: default-ca-list

Configuration Mode: Config

History: 3.2.3000

Role: admin

Example

switch (config) # email ssl ca-list none

Related Commands: N/A

Notes: This command has no impact unless TLS is used, and certificate verification is enabled.
show email

show email [events]

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

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

**Related Commands**

show email

**Notes**
4.8 **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** – recording of 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.

### 4.8.1 Commands

**protocol telemetry**

```plaintext
protocol telemetry
no protocol telemetry
```

Unhides telemetry config CLIs.
The no form of the command hides telemetry config CLIs.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>Disabled.</td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Config</td>
</tr>
<tr>
<td>History</td>
<td>3.6.3004</td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
</tr>
</tbody>
</table>
| Example            | switch (config) # protocol telemetry  
<p>|                    | switch (config) # no protocol telemetry |</p>
<table>
<thead>
<tr>
<th>Related Commands</th>
</tr>
</thead>
<tbody>
<tr>
<td>Notes</td>
</tr>
</tbody>
</table>
telemetry shutdown

Disables the telemetry protocol, and histogram fetching for all sampling enabled interfaces without changing any internal configuration. The no form of the command enables telemetry protocol.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>Disabled</td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Config</td>
</tr>
<tr>
<td>History</td>
<td>3.6.3004</td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
</tr>
</tbody>
</table>
| Example            | switch (config) # telemetry shutdown  
switch (config) # no telemetry shutdown |

Related Commands

Notes
telemetry sampling log

telemetry sampling log <time>
no telemetry sampling log <time>

Enables the log interval value (histogram fetching) from device.
The no form of the command disables the log interval value.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>time</th>
<th>Input Range: 100 msec - 1 min</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>1000 msec.</td>
<td></td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Config</td>
<td></td>
</tr>
<tr>
<td>History</td>
<td>3.6.3004</td>
<td></td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
<td></td>
</tr>
</tbody>
</table>
| Example             | switch (config) # telemetry sampling log 1000  
switch (config) # no telemetry sampling log |

Related Commands

Notes
interface ethernet telemetry sampling tc mcast

interface ethernet <slot>/<port>[/<subport>] telemetry sampling tc <tc_id> mcast
no interface ethernet <slot>/<port>[/<subport>] telemetry sampling tc <tc_id> mcast

Enables multicast sampling (histogram fetching) on a tc for a specific Ethernet interface.
The no form of the command disables multicast sampling on a tc for a specific Ethernet interface.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>slot/port</td>
<td>Ethernet port number</td>
</tr>
<tr>
<td>subport</td>
<td>Ethernet subport number to be used in case of split port</td>
</tr>
<tr>
<td>tc_id</td>
<td>Input range: 0-7</td>
</tr>
</tbody>
</table>

| Default            | N/A                                    |
| Configuration Mode | Config-Instance-ID                     |
| History            | 3.6.3004 1/2/4                         |
| Role               | admin                                  |

Example

```
switch (config) # interface ethernet 1/2 telemetry sampling tc 3 mcast
switch (config) # no interface ethernet 1/2 telemetry sampling tc 3 mcast
```

Related Commands

Notes
interface ethernet telemetry sampling tc ucast

interface ethernet <slot>/<port>[/<subport>] telemetry sampling tc <tc_id> ucast
no interface ethernet <slot>/<port>[/<subport>] telemetry sampling tc <tc_id> ucast

Enables unicast sampling (histogram fetching) on a tc for a specific Ethernet interface.
The no form of the command disables unicast sampling on a tc for a specific Ethernet interface.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>slot/port</td>
<td>Ethernet port number</td>
</tr>
<tr>
<td>subport</td>
<td>Ethernet subport number to be used in case of split port</td>
</tr>
<tr>
<td>tc_id</td>
<td>Input range: 0-7</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Default</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Config Mode</td>
<td>Config</td>
</tr>
<tr>
<td>History</td>
<td>3.6.3004</td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
</tr>
</tbody>
</table>

Example

```
switch (config) # interface ethernet 1/2 telemetry sampling tc 3 ucast
switch (config) # no interface ethernet 1/2 telemetry sampling tc 3 ucast
```

Related Commands

Notes
interface ib 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).

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>slot/port</th>
<th>InfiniBand port number</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>N/A</td>
<td></td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Config-Instance</td>
<td></td>
</tr>
<tr>
<td>History</td>
<td>3.6.3004</td>
<td></td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
<td></td>
</tr>
<tr>
<td>Example</td>
<td>switch (config) # interface ib 1/1 telemetry sampling</td>
<td></td>
</tr>
<tr>
<td></td>
<td>switch (config) # no interface ib 1/1 telemetry sampling</td>
<td></td>
</tr>
<tr>
<td>Related Commands</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Notes</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
show telemetry sampling interface ethernet tc ucast

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

Syntax Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>slot/port</td>
<td>Ethernet port number</td>
</tr>
<tr>
<td>subport</td>
<td>Ethernet subport number to be used in case of split port</td>
</tr>
<tr>
<td>tc_id</td>
<td>Input range: 0-7</td>
</tr>
</tbody>
</table>

Default

N/A

Configuration Mode

Any Command Mode

History

3.6.3004

Role

admin

Example

switch (config) # show telemetry sampling interface ethernet 1/2 tc 6 ucast

Telemetry histogram Eth1/2 traffic-class 6 - ucast

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>01/13/17</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</td>
</tr>
<tr>
<td>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>08:18:11.67953</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>

Related Commands

Notes
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.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>slot/port</td>
<td>Ethernet port number</td>
</tr>
<tr>
<td>subport</td>
<td>Ethernet subport number to be used in case of split port</td>
</tr>
<tr>
<td>tc_id</td>
<td>Input range: 0-7</td>
</tr>
</tbody>
</table>

**Default**  
N/A

**Configuration Mode**  
Any Command Mode

**History**  
3.6.3004

**Role**  
admin

**Example**

```
switch (config) # show telemetry sampling interface ethernet 1/2 tc 3 mcast
```

```
Telemetry histogram Eth1/2 traffic-class 3 - mcast
Time  Bin sizes (nsec buffer was occupied in bytes range)
     01/16/17  250ns  500ns  750ns  1000ns  1250ns  1500ns  1750ns  2000ns  2500ns  3000ns  4000ns  5000ns  6000ns  7000ns  8000ns  9000ns  10000ns  12000ns  14000ns  16000ns>
04:09:07.79936  00000000  0  0  0  0  0  0  0  0  0  0  0  0  0  0  0  0  0  0
04:09:09.80355  00000000  0  0  0  0  0  0  0  0  0  0  0  0  0  0  0  0  0  0
04:09:10.80518  00000000  0  0  0  0  0  0  0  0  0  0  0  0  0  0  0  0  0  0
```

**Related Commands**

**Notes**
**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.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>slot/port</td>
<td>Ethernet port number</td>
</tr>
<tr>
<td>subport</td>
<td>Ethernet subport number to be used in case of split port</td>
</tr>
<tr>
<td>tc_id</td>
<td>Input range: 0-7</td>
</tr>
<tr>
<td>num_of_entries</td>
<td>Input range: 0-1000</td>
</tr>
</tbody>
</table>

**Default**

N/A

**Configuration Mode**

Any Command Mode

**History**

3.6.3004

**Role**

admin

**Example**

```
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 (nsec buffer was occupied in bytes range)------------------------------------------------------------------------------------------------------------------------------------------------------
01/16/17                2976<                27552       52128       76704      101280      125856      150432      175008      199584      199584>
04:28:39.81351    1000000000                 0           0           0          0           0           0           0     ...                 0           0           0          0           0           0           0           0           0
04:28:41.81708    1000000000                 0           0           0          0           0           0           0           0           0
```

**Related Commands**

**Notes**

In case requested entries are more than what the DB contains it will print the amount in the table.
**show telemetry sampling interface 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.

**Syntax Description**

<table>
<thead>
<tr>
<th>Description</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>slot/port</td>
<td>slot/port Ethernet port number</td>
</tr>
<tr>
<td>subport</td>
<td>subport Ethernet subport number to be used in case of split port</td>
</tr>
<tr>
<td>tc_id</td>
<td>Input range: 0-7</td>
</tr>
<tr>
<td>num_of_entries</td>
<td>Input range: 0-1000</td>
</tr>
</tbody>
</table>

**Default**

N/A

**Configuration Mode**

Any Command Mode

**History**

3.6.3004

**Role**

admin

**Example**

```
switch (config) # show telemetry sampling interface ethernet 1/2 tc 3 mcast last 4
```

<table>
<thead>
<tr>
<th>Time</th>
<th>Bin sizes (nsec) buffer was occupied in bytes range</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>0000000000</td>
</tr>
<tr>
<td>06:23:39.287939</td>
<td>0000000000</td>
</tr>
<tr>
<td>06:23:40.289393</td>
<td>0000000000</td>
</tr>
</tbody>
</table>

**Related Commands**

**Notes**

In case requested entries are more than what the DB contains it will print the amount in the table.
### show telemetry sampling interface ib

**show telemetry sampling interface ib <slot>/<port>**

Displays telemetry histogram samples for a specific ib interface.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
<th>Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>slot/port</td>
<td>Infiniband port number</td>
<td>switch (config) # show telemetry sampling interface ib 1/32 last 20</td>
</tr>
</tbody>
</table>

**Default**

N/A

**Configuration Mode**

Any Command Mode

**History**

3.6.3004

**Role**

admin

**Example**

```
switch (config) # show telemetry sampling interface ib 1/32 last 20

<table>
<thead>
<tr>
<th>Time</th>
<th>02/19/17 09:49:14</th>
<th>02/19/17 09:50:03</th>
<th>02/19/17 09:51:03</th>
</tr>
</thead>
<tbody>
<tr>
<td>System-time</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Bin sizes</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Bin sizes</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Bin sizes</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Bin sizes</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Bin sizes</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Bin sizes</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Bin sizes</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Bin sizes</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Bin sizes</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Bin sizes</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Bin sizes</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Bin sizes</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Bin sizes</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Bin sizes</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Bin sizes</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Bin sizes</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Bin sizes</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Bin sizes</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Bin sizes</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Bin sizes</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Bin sizes</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Bin sizes</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Bin sizes</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Bin sizes</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Bin sizes</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Bin sizes</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Bin sizes</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>
```

**Related Commands**

**Notes**

In case requested entries are more than what the DB contains it will print the amount in the table.
show telemetry sampling interface ib last

Displays fetched unicast histogram details for tc_id of an Ethernet interface.

Syntax Description

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>slot/port</th>
<th>Infiniband port number</th>
</tr>
</thead>
<tbody>
<tr>
<td>num_of_entries</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Default

N/A

Configuration Mode

Any Command Mode

History

3.6.3004

Role

admin

Example

switch (config) # show telemetry sampling interface ethernet 1/2 tc 6 ucast

------------------------------------------------------------------------------------------------------------------------------------------------------
Telemetry histogram: Eth1/2 traffic-class 6 - ucast        Time                                            Bin sizes (nsec buffer was occupied in bytes range)
------------------------------------------------------------------------------------------------------------------------------------------------------
01/13/17               2976<       27552       52128       76704      101280      125856      150432      175008      ...        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

Related Commands

Notes

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>] [filename *] [after *] [before *]`

Exports histograms collected by stats to a csv file.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>slot/port</td>
<td>Ethernet Infiniband port number</td>
</tr>
<tr>
<td>subport</td>
<td>Ethernet Infiniband subport number to be used in case of split port</td>
</tr>
</tbody>
</table>

**Default**

N/A

**Configuration Mode**

Any Command Mode

**History**

3.6.3004

**Role**

admin

**Example**

```
switch (config) # stats export csv telemetry 1/1
```

Generated report file: telemetry-20170119-102715.csv

**Related Commands**


**Notes**
file stats telemetry upload

file stats telemetry upload <filename> <upload URL>

Uploads file created by stats export command to user directory.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>N/A</td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Any Command Mode</td>
</tr>
<tr>
<td>History</td>
<td>3.6.3004</td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
</tr>
<tr>
<td>Example</td>
<td>switch (config) # file stats telemetry upload telemetry-20170119-102715.csv scp://username:password@server//directory</td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>N/A</td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Any Command Mode</td>
</tr>
<tr>
<td>History</td>
<td>3.6.3004</td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
</tr>
</tbody>
</table>

**Example**

```
switch (config) # show files stats telemetry
telemetry-20170119-102715.csv
```

**Related Commands**

**Notes**
4.9 User Management and Security

4.9.1 User Accounts

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

Table 26 - User Roles (Accounts) and Default Passwords

<table>
<thead>
<tr>
<th>User Role</th>
<th>Default Password</th>
</tr>
</thead>
<tbody>
<tr>
<td>admin</td>
<td>admin</td>
</tr>
<tr>
<td>monitor</td>
<td>monitor</td>
</tr>
<tr>
<td>xmladmin</td>
<td>xmladmin</td>
</tr>
<tr>
<td>xmluser</td>
<td>xmluser</td>
</tr>
</tbody>
</table>

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

4.9.2 Authentication, Authorization and Accounting (AAA)

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

- **Authentication** - authentication provides the initial method of identifying each individual user, typically by entering a valid username and password before access is granted. The AAA server compares a user's authentication credentials with the user credentials stored in a database. If the credentials match, the user is granted access to the network or devices. If the credentials do not match, authentication fails and network access is denied.

- **Authorization** - following the authentication, a user must gain authorization for performing certain tasks. After logging into a system, for instance, the user may try to issue commands. The authorization process determines whether the user has the authority to issue such commands. Simply put, authorization is the process of enforcing policies: determining what types or qualities of activities, resources, or services a user is permitted. Usually, authorization occurs within the context of authentication. Once you have authenticated a user, they may be authorized for different types of access or activity.

- **Accounting** - the last level is accounting, which measures the resources a user consumes during access. This includes the amount of system time or the amount of data a user has sent and/or received during a session. Accounting is carried out by logging of session
statistics and usage information, and is used for authorization control, billing, trend analysis, resource utilization, and capacity planning activities.

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

4.9.2.1 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.

4.9.2.2 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

4.9.2.3 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

4.9.2.4 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
```

### 4.9.3 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:**

1. **Step 1.** Disable SNMPv1 and v2. Run:

   ```
   switch (config) # no snmp-server enable communities
   ```

2. **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>
   ```

3. **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>
   ```

4. **Step 4.** Only allow SSHv2. Run:

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

5. **Step 5.** Enable SSH server strict security mode. Run:

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

6. **Step 6.** Disable HTTP access. Run:

   ```
   switch (config) # no web http enable
   ```
Step 7. Enable HTTPS strict cyphers. Run:

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

Step 8. Disable router BGP neighbor password configuration. Run:

```
switch (config) # no router bgp <as-number> neighbor <ip-address> password
```

Step 9. Disable router BGP peer group password configuration. Run:

```
switch (config) # no router bgp <as-number> peer-group <peer-group-name> password
```

Step 10. Disable BGP password configuration. Run:

```
switch (config) # no neighbor <ip-address> password
```

Step 11. Disable MD5 password hashing on for users. Run:

```
switch (config) # username <username> password <password>
```

If a necessary prerequisite is not fulfilled the system does not activate secure mode and issues an advisory message accordingly.

Secure mode is not supported on director switch systems.

- **To activate secure mode:**

```
switch (config) # system secure-mode enable
```

Warning! Configuration is about to be saved and the system will be reloaded. Type 'YES' to confirm the change in secure mode: YES

- **To deactivate secure mode:**

```
switch (config) # no system secure-mode enable
```

Warning! Configuration is about to be saved and the system will be reloaded. Type 'YES' to confirm the change in secure mode: YES

- **To verify secure mode configuration and state:**

```
switch (config)# show system secure-mode
```

Secure mode configured: yes
Secure mode enabled: yes

```
4.9.4 Commands

4.9.4.1 User Accounts

**username**

```
username <username> [capability <cap> | disable [login | password] | disconnect | full-name <name> | nopassword | password [0 | 7] <password>]
```

```
o 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.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>username</td>
<td>Specifies a username and creates a user account. New users are created initially with admin privileges but is disabled.</td>
</tr>
<tr>
<td>capability &lt;cap&gt;</td>
<td>Defines user capabilities.</td>
</tr>
<tr>
<td></td>
<td>• admin - full administrative capabilities</td>
</tr>
<tr>
<td></td>
<td>• monitor - read only capabilities, can not change the running configuration</td>
</tr>
<tr>
<td></td>
<td>• unpriv – can only query the most basic information, and cannot take any actions or change any configuration</td>
</tr>
<tr>
<td></td>
<td>• v_admin – basic administrator capabilities</td>
</tr>
<tr>
<td>disable [login</td>
<td>password]</td>
</tr>
<tr>
<td></td>
<td>• Disable login - disable all logins to this account</td>
</tr>
<tr>
<td></td>
<td>• Disable password - disable login to this account using a local password</td>
</tr>
<tr>
<td>disconnect</td>
<td>Logs out the specified user from the system</td>
</tr>
<tr>
<td>name</td>
<td>Full name of the user</td>
</tr>
<tr>
<td>nopassword</td>
<td>The next login of the user will not require password.</td>
</tr>
<tr>
<td>0</td>
<td>7</td>
</tr>
<tr>
<td></td>
<td>• 7: specifies a login password in encrypted text</td>
</tr>
<tr>
<td>password</td>
<td>Specifies a password for the user in string form. If [0</td>
</tr>
</tbody>
</table>

**Default**

The following usernames are available by default:

- admin
- monitor
- xmladmin
- xmluser
**Configuration Mode**  
Config

**History**

<table>
<thead>
<tr>
<th>Revision</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.1.0000</td>
<td></td>
</tr>
<tr>
<td>3.4.0000</td>
<td>Updated Example</td>
</tr>
<tr>
<td>3.4.1100</td>
<td>Updated Example</td>
</tr>
<tr>
<td>3.6.2002</td>
<td>Added “disconnect” parameter</td>
</tr>
</tbody>
</table>

**Role**  
admin

**Example**

```bash
switch (config) # username monitor full-name smith
switch (config) # show usernames

<table>
<thead>
<tr>
<th>USERNAME</th>
<th>FULL NAME</th>
<th>CAPABILITY</th>
<th>ACCOUNT STATUS</th>
</tr>
</thead>
<tbody>
<tr>
<td>USERID</td>
<td>System Admin</td>
<td>admin</td>
<td>Password set</td>
</tr>
<tr>
<td>admin</td>
<td>System Admin</td>
<td>admin</td>
<td>Password set</td>
</tr>
<tr>
<td>monitor</td>
<td>smith</td>
<td>monitor</td>
<td>Password set (SHA512)</td>
</tr>
<tr>
<td>xmladmin</td>
<td>XML Admin</td>
<td>admin</td>
<td>Password set (SHA512)</td>
</tr>
<tr>
<td>xmluser</td>
<td>XML Monitor</td>
<td>monitor</td>
<td>Password set (SHA512)</td>
</tr>
</tbody>
</table>
```

**Related Commands**  
show usernames  
show users

**Notes**

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

**show usernames**

Displays list of users and their capabilities.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>N/A</td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Any Command Mode</td>
</tr>
<tr>
<td>History</td>
<td>3.1.0000</td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
</tr>
</tbody>
</table>

### Example

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

### Related Commands

- `username`
- `show users`

### Notes
## show users

**show users [history]**

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

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>history</th>
<th>Displays current and historical sessions.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Default</strong></td>
<td>N/A</td>
<td></td>
</tr>
<tr>
<td><strong>Configuration Mode</strong></td>
<td>Any Command Mode</td>
<td></td>
</tr>
<tr>
<td><strong>History</strong></td>
<td>3.1.0000</td>
<td></td>
</tr>
<tr>
<td><strong>Role</strong></td>
<td>admin</td>
<td></td>
</tr>
</tbody>
</table>

### Example

```
USERNAME   FULL NAME                LINE    HOST               IDLE
admin      System Administrator     pts/0   172.22.237.174     0d0h34m4s
admin      System Administrator     pts/1   172.30.0.127       1d3h30m49s
admin      System Administrator     pts/3   172.22.237.34      0d0h0m0s

switch (config) # show users history
admin    pts/3 172.22.237.34    Wed Feb  1 11:56   still logged in
admin    pts/3 172.22.237.34    Wed Feb  1 11:42 - 11:46  (00:04)

wtmp begins Wed Feb  1 11:38:10 2012
switch (config) #
```

### Related Commands

- username
- show usernames

### Notes
show whoami

show whoami

Displays username and capabilities of user currently logged in.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>N/A</td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Any Command Mode</td>
</tr>
<tr>
<td>History</td>
<td>3.1.0000</td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
</tr>
</tbody>
</table>

**Example**

```
switch (config) # show whoami
Current user: admin
Capabilities: admin
switch (config) #
```

**Related Commands**

username
show usernames
show users

**Notes**
4.9.4.2 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.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>N/A</td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Config</td>
</tr>
<tr>
<td>History</td>
<td>3.1.0000</td>
</tr>
<tr>
<td></td>
<td>3.2.3000</td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
</tr>
</tbody>
</table>
| Example            | `switch (config) # aaa accounting changes default stop-only tacacs+`  
|                    | `switch (config) # show aaa`  
|                    | AAA authorization:  
|                    |   Default User: admin  
|                    |   Map Order: local-only  
|                    |   Authentication method(s):  
|                    |     local  
|                    |     radius  
|                    |     tacacs+  
|                    |     ldap  
|                    | Accounting method(s):  
|                    |     tacacs+  
|                    | `switch (config) #` |
| Related Commands   | `show aaa` |
| Notes              | • TACACS+ is presently the only accounting service method supported  
|                    | • Change accounting covers both configuration changes and system actions that are visible under audit logging, however this feature operates independently of audit logging, so it is unaffected by the “logging level audit mgmt” or “configuration audit” commands  
|                    | • Configured TACACS+ servers are contacted in the order in which they appear in the configuration until one accepts the accounting data, or the server list is exhausted  
|                    | • Despite the name of the “stop-only” keyword, which indicates that this feature logs a TACACS+ accounting “stop” message, and in contrast to configuration change accounting, which happens after configuration database changes, system actions are logged when the action is started, not when the action has completed |
aaa authentication login

aaa authentication login default <auth method> [<auth method> [<auth method> [<auth method>]]]
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.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>auth-method</th>
<th>local</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>radius</td>
</tr>
<tr>
<td></td>
<td></td>
<td>tacacs+</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ldap</td>
</tr>
</tbody>
</table>

Default: local

Configuration Mode: Any Command Mode

History: 3.1.0000

Role: admin

Example:

```
switch (config) # aaa authentication login default local radius tacacs+ ldap
switch (config) # show aaa
AAA authorization:
    Default User: admin
    Map Order: local-only
    Authentication method(s):
        local
        radius
        tacacs+
        ldap
Accounting method(s):
    tacacs+
switch (config) #
```

Related Commands: show aaa

Notes: The order in which the methods are specified is the order in which the authentication is attempted. It is required that “local” is one of the methods selected. It is recommended that “local” be listed first to avoid potential problems logging in to local accounts in the face of network or remote server issues.
## aaa authentication attempts fail-delay

**aaa authentication attempts fail-delay <time>**

**no aaa authentication attempts fail-delay**

Configures delay for a specific period of time after every authentication failure. The no form of the command resets the fail-delay to its default value.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>time</th>
<th>Range: 0-60 seconds</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Config</td>
<td></td>
</tr>
<tr>
<td>History</td>
<td>3.5.0200</td>
<td></td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
<td></td>
</tr>
<tr>
<td>Example</td>
<td>switch (config) # aaa authentication attempts fail-delay 1</td>
<td></td>
</tr>
<tr>
<td>Related Commands</td>
<td>N/A</td>
<td></td>
</tr>
<tr>
<td>Notes</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
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.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>downcase</th>
<th>Does not convert all usernames to lowercase (for authentication failure tracking purposes only).</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>enable</td>
<td>Disables tracking of failed authentication attempts</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Default</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuration Mode</td>
<td>Config</td>
</tr>
<tr>
<td>History</td>
<td>3.2.3000</td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
</tr>
</tbody>
</table>

```
Example
switch (config) # aaa authentication attempts track enable
```

<table>
<thead>
<tr>
<th>Related Commands</th>
<th>N/A</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Notes</th>
</tr>
</thead>
</table>
| • This is required for the lockout functionality described below, but can also be used on its own for informational purposes.  
• Disabling tracking does not clear any records of past authentication failures, or the locks in the database. However, it does prevent any updates to this database from being made: no new failures are recorded. It also disables lockout, preventing new lockouts from being recorded and existing lockouts from being enforced. |
aaa authentication attempts lockout

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

Configures lockout of accounts based on failed authentication attempts. The no form of the command clears configuration for lockout of accounts based on failed authentication attempts.
<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>enable</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enables locking out of user accounts based on authentication failures. This both suspends enforcement of any existing lockouts, and prevents any new lockouts from being recorded. If lockouts are later re-enabled, any lockouts that had been recorded previously resume being enforced; but accounts which have passed the max-fail limit in the meantime are NOT automatically locked at this time. They would be permitted one more attempt, and then locked, because of how the locking is done: lockouts are applied after an authentication failure, if the user has surpassed the threshold at that time. Lockouts only work if tracking is enabled. Enabling lockouts automatically enables tracking. Disabling tracking automatically disables lock-outs.</td>
<td></td>
</tr>
</tbody>
</table>

| lock-time | Sets maximum permitted consecutive authentication failures before locking out users. Unlike the “max-fail” setting, this does take effect immediately for all accounts. If both unlock-time and lock-time are set, the unlock-time must be greater than the lock-time. This is not based on the number of consecutive failures, and is therefore divorced from most of the rest of the tally feature, except for the tracking of the last login failure. |

| max-fail | Sets maximum permitted consecutive authentication failures before locking out users. This setting only impacts what lockouts are imposed while the setting is active; it is not retro-active to previous logins. So if max-fail is disabled or changed, this does not immediately cause any users to be changed from locked to unlocked or vice-versa. |

| unlock-time | Enables the auto-unlock of an account after a specified number of seconds if a user account is locked due to authentication failures, counting from the last valid login attempt. Unlike the “max-fail” setting, this does take effect immediately for all accounts. If both unlock-time and lock-time are set, the unlock-time must be greater than the lock-time. Careful with disabling the unlock-time, particularly if you have max-fail set to something, and have not overridden the behavior for the admin (i.e. they are subject to lockouts also). If the admin account gets locked out, and there are no other administrators who can aid, the user may be forced to boot single-user and use the pam_tallybyname command-line utility to unlock your account normally. For more information about the pam_tallybyname command-line utility, refer to the documentation. |

360 Mellanox Technologies Confidential | Rev 4.60
<table>
<thead>
<tr>
<th><strong>Default</strong></th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Configuration Mode</strong></td>
<td>Config</td>
</tr>
<tr>
<td><strong>History</strong></td>
<td>3.2.3000</td>
</tr>
<tr>
<td><strong>Role</strong></td>
<td>admin</td>
</tr>
<tr>
<td><strong>Example</strong></td>
<td><code>switch (config) # aaa authentication attempts lockout enable</code></td>
</tr>
<tr>
<td><strong>Related Commands</strong></td>
<td>N/A</td>
</tr>
<tr>
<td><strong>Notes</strong></td>
<td>N/A</td>
</tr>
</tbody>
</table>
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.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>admin</th>
<th>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.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>no-lockout</td>
<td>Prevents the admin user from being locked out, though the authentication failure history is still tracked (if tracking is enabled overall).</td>
</tr>
<tr>
<td></td>
<td>unknown</td>
<td>Overrides the global settings for tracking and lockouts for unknown accounts. The “unknown” class here contains the following categories:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Real remote usernames which simply failed authentication</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Mis-typed remote usernames</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Passwords accidentally entered as usernames</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Bogus usernames made up as part of an attack on the system</td>
</tr>
<tr>
<td></td>
<td>hash-username</td>
<td>Applies a hash function to the username, and stores the hashed result in lieu of the original.</td>
</tr>
<tr>
<td></td>
<td>no-track</td>
<td>Does not track authentication for such users (which of course also implies no-lockout).</td>
</tr>
</tbody>
</table>

Default: N/A
Configuration Mode: Config
History: 3.2.3000
Role: admin
Example: switch (config) # aaa authentication attempts class-override admin no-lockout
<table>
<thead>
<tr>
<th>Related Commands</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Notes</td>
<td></td>
</tr>
</tbody>
</table>
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.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>all</td>
<td>Applies function to all users.</td>
</tr>
<tr>
<td>user</td>
<td>Applies function to specified user.</td>
</tr>
<tr>
<td>no-clear-history</td>
<td>Leaves the history of login failures but unlocks the account.</td>
</tr>
<tr>
<td>no-unlock</td>
<td>Leaves the account locked but clears the history of login failures.</td>
</tr>
</tbody>
</table>

Default: N/A

Configuration Mode: Config

History: 3.2.3000

Role: admin

Example:
```
switch (config) # aaa authentication attempts reset user admin all
```

Related Commands: N/A

Notes:
clear aaa authentication attempts

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

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

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>all</th>
<th>Applies function to all users.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>user</td>
<td>Applies function to specified user.</td>
</tr>
<tr>
<td></td>
<td>no-clear-history</td>
<td>Clears the history of login failures.</td>
</tr>
<tr>
<td></td>
<td>no-unlock</td>
<td>Unlocks the account.</td>
</tr>
</tbody>
</table>

Default: N/A

Configuration Mode: Config

History: 3.2.3000

Role: admin

Example: `switch (config) # aaa authentication attempts reset user admin no-clear-history`

Related Commands: N/A

Notes:

---
aaa authorization

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

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

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<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>
</tbody>
</table>
| order <policy>     | Sets the user mapping behavior when authenticating users via RADIUS or TACACS+ to one of three choices. The order determines how the remote user mapping behaves. If the authenticated username is valid locally, no mapping is performed. The setting has the following three possible behaviors:  
  - remote-first – if a local-user mapping attribute is returned and it is a valid local username, it maps the authenticated user to the local user specified in the attribute. Otherwise, it uses the user specified by the default-user command.  
  - remote-only – maps a remote authenticated user if the authentication server sends a local-user mapping attribute. If the attribute does not specify a valid local user, no further mapping is tried.  
  - local-only – maps all remote users to the user specified by the “aaa authorization map default-user <user name>” command. Any vendor attributes received by an authentication server are ignored. |

<table>
<thead>
<tr>
<th>Default</th>
<th>Configuration Mode</th>
<th>History</th>
<th>Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default user - admin</td>
<td>Config</td>
<td>3.1.0000</td>
<td>admin</td>
</tr>
<tr>
<td>Map order - remote-first</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Example

```
switch (config) # aaa authorization map default-user admin
switch (config) # show aaa
AAA authorization:
  Default User: admin
  Map Order: remote-first
Authentication method(s):
  local
Accounting method(s):
  tacacs+
switch (config) #
```

Related Commands

```
show aaa
username
```

Notes

- If, for example, the user is locally defined to have admin permission, but in a remote server such as RADIUS the user is authenticated as monitor and the order is remote-first, then the user is given monitor permissions.
- If AAA authorization order policy is configured to remote-only, then when upgrading to 3.4.3000 or later from an older MLNX-OS version, this policy is changed to remote-first.
- 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.
### show aaa

**show aaa**

Displays the AAA configuration.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>N/A</td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Any Command Mode</td>
</tr>
<tr>
<td>History</td>
<td>3.1.0000</td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
</tr>
</tbody>
</table>

#### Example

```bash
switch (config) # show aaa
AAA authorization:
  Default User: admin
  Map Order: remote-first
Authentication method(s):
  local
Accounting method(s):
  tacacs+
switch (config) #
```

#### Related Commands

- `aaa accounting`
- `aaa authentication`
- `aaa authorization`
- `show aaa`
- `show usernames`
- `username`
**show aaa authentication attempts**

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

Shows the current authentication, authorization and accounting settings.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>authentication attempts</td>
<td>Displays configuration and history of authentication failures.</td>
</tr>
<tr>
<td>configured</td>
<td>Displays configuration of authentication failure tracking.</td>
</tr>
<tr>
<td>status user</td>
<td>Displays status of authentication failure tracking and lockouts for specific user.</td>
</tr>
</tbody>
</table>

**Default**

N/A

**Configuration Mode**

Any Command Mode

**History**

3.2.1000

3.5.0200 Updated Example

**Role**

admin

**Example**

```
switch (config) # show aaa authentication attempts
Configuration for authentication failure tracking and locking:

  Track authentication failures:          yes
  Lock accounts based on authentication failures: yes
  Override treatment of 'admin' user:      (none)
  Override treatment of unknown usernames: hash-usernames
  Convert usernames to lowercase for tracking: no
  Delay after each auth failure (fail delay): none

Configuration for lockouts based on authentication failures:

  Lock account after consecutive auth failures: 5
  Allow retry on locked accounts (unlock time): after 15 second(s)
  Temp lock after each auth failure (lock time): none

<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>0Q72B43EHHT8C95AP5RGRKXU3B3L4CTY3Y3H(*):</td>
<td>no</td>
<td>no</td>
<td>1</td>
<td>2012/08/20 14:29:19</td>
<td>ttyS0</td>
</tr>
</tbody>
</table>

(*) Hashed for security reasons
```

**Related Commands**

N/A

**Notes**

N/A
### 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.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>secret</th>
<th>Sets a secret key (shared hidden text string), known to the system and to the RADIUS server.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>retries</td>
<td>Number of retries (0-5) before exhausting from the authentication.</td>
</tr>
<tr>
<td></td>
<td>seconds</td>
<td>Timeout in seconds between each retry (1-60).</td>
</tr>
</tbody>
</table>

**Default**

3 seconds, 1 retry

**Configuration Mode**

Config

**History**

3.1.0000

**Role**

admin

**Example**

```
switch (config) #radius-server retransmit 3
switch (config) # show radius
RADIUS defaults:
    Key: 3333
    Timeout: 3
    Retransmit: 1
No RADIUS servers configured.
switch (config) #
```

**Related Commands**

- aaa authorization
- radius-server host
- show radius

**Notes**

Each RADIUS server can override those global parameters using the command “radius-server host”.
# radius-server host

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

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

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP address</td>
<td>RADIUS server IP address</td>
</tr>
<tr>
<td>enable</td>
<td>Administrative enable of the RADIUS server</td>
</tr>
<tr>
<td>auth-port</td>
<td>Configures authentication port to use with this RADIUS server</td>
</tr>
<tr>
<td>port</td>
<td>RADIUS server UDP port number</td>
</tr>
<tr>
<td>key</td>
<td>Configures shared secret to use with this RADIUS server</td>
</tr>
<tr>
<td>prompt-key</td>
<td>Prompt for key, rather than entering on command line</td>
</tr>
<tr>
<td>retransmit</td>
<td>Configures retransmit count to use with this RADIUS server</td>
</tr>
<tr>
<td>retries</td>
<td>Number of retries (0-5) before exhausting from the authentication</td>
</tr>
<tr>
<td>timeout</td>
<td>Configures timeout between each try</td>
</tr>
<tr>
<td>seconds</td>
<td>Timeout in seconds between each retry (1-60)</td>
</tr>
</tbody>
</table>

**Default**
- 3 seconds, 1 retry
- Default UDP port is 1812

**Configuration Mode**
- Config

**History**
- 3.1.0000

**Role**
- admin
Example

switch (config) # radius-server host 40.40.40.40
switch (config) # show radius
RADIUS defaults:
  Key:             3333
  Timeout:         3
  Retransmit:      1
RADIUS servers:
  40.40.40.40:1812
     Enabled:         yes
     Key:             3333 (default)
     Timeout:         3 (default)
     Retransmit:      1 (default)
switch (config) #

Related Commands
aaa authorization
radius-server
show radius

Notes
- RADIUS servers are tried in the order they are configured
- If you do not specify a parameter for this configured RADIUS server, the configuration will be taken from the global RADIUS server configuration. Refer to “radius-server” command.
show radius

Displays RADIUS configurations.

**Syntax Description**

<table>
<thead>
<tr>
<th>Default</th>
<th>N/A</th>
</tr>
</thead>
</table>

**Configuration Mode**

Any Command Mode

**History**

3.1.0000

**Role**

admin

**Example**

```
switch (config) # show radius
RADIUS defaults:
  Key:             3333
  Timeout:         3
  Retransmit:      1
RADIUS servers:
  40.40.40.40:1812
    Enabled:         yes
    Key:             3333 (default)
    Timeout:         3 (default)
    Retransmit:      1 (default)
switch (config) #
```

**Related Commands**

- aaa authorization
- radius-server
- radius-server host

**Notes**
### 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.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>secret</td>
<td>Set a secret key (shared hidden text string), known to the system and to the TACACS+ server.</td>
</tr>
<tr>
<td>retries</td>
<td>Number of retries (0-5) before exhausting from the authentication.</td>
</tr>
<tr>
<td>seconds</td>
<td>Timeout in seconds between each retry (1-60).</td>
</tr>
</tbody>
</table>

**Default**

3 seconds, 1 retry

**Configuration Mode**

Config

**History**

3.1.0000

**Role**

admin

**Example**

```bash
switch (config) #tacacs-server retransmit 3  
switch (config) # show tacacs  
TACACS+ defaults:  
   Key: 3333  
   Timeout: 3  
   Retransmit: 1  
No TACACS+ servers configured.  
switch (config) #
```

**Related Commands**

- aaa authorization
- show radius
- show tacacs
- tacacs-server host

**Notes**

Each TACACS+ server can override those global parameters using the command “tacacs-server host”.

---

374 Mellanox Technologies Confidential Rev 4.60
### 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.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP address</td>
<td>TACACS+ server IP address</td>
</tr>
<tr>
<td>enable</td>
<td>Administrative enable for the TACACS+ server</td>
</tr>
<tr>
<td>auth-port</td>
<td>Configures authentication port to use with this TACACS+ server</td>
</tr>
<tr>
<td>port</td>
<td>TACACS+ server UDP port number</td>
</tr>
<tr>
<td>auth-type</td>
<td>Configures authentication type to use with this TACACS+ server</td>
</tr>
</tbody>
</table>
| type              | Authentication type. Possible values are:  
|                   | • ASCII  
|                   | • PAP (Password Authentication Protocol) |
| key               | Configures shared secret to use with this TACACS+ server |
| secret            | Sets a secret key (shared hidden text string), known to the system and to the TACACS+ server |
| prompt-key        | Prompts for key, rather than entering key on command line |
| retransmit        | Configures retransmit count to use with this TACACS+ server |
| retries           | Number of retries (0-5) before exhausting from the authentication |
| timeout           | Configures timeout to use with this TACACS+ server |
| seconds           | Timeout in seconds between each retry (1-60) |

**Default**

- 3 seconds, 1 retry
- Default TCP port is 49
- Default auth-type is PAP

**Configuration Mode**

Config
History

3.1.0000

Role

admin

Example

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

Related Commands

aaa authorization
show tacacs
tacacs-server

Notes

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

**show tacacs**

Displays TACACS+ configurations.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>N/A</td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Any Command Mode</td>
</tr>
<tr>
<td>History</td>
<td>3.1.0000</td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
</tr>
</tbody>
</table>

**Example**

```bash
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)
```

**Related Commands**

- aaa authorization
tacacs-server
tacacs-server host

**Notes**
4.9.4.5 LDAP

**ldap base-dn**

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

Sets the base distinguished name (location) of the user information in the schema of the LDAP server.
The no form of the command resets the attribute to its default values.

### Syntax Description

- **string**: A case-sensitive string that specifies the location in the LDAP hierarchy where the server should begin searching when it receives an authorization request.
  
  For example:
  
  “ou=users,dc=example,dc=com”, with no spaces.

### Default

- `ou=users,dc=example,dc=com`

### Configuration Mode

- `Config`

### History

- `3.1.0000`
- `3.4.0000` Updated Example

### Role

- `admin`
Example

```
switch (config) # ldap base-dn ou=department,dc=example,dc=com
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
```

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.

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

```
ldap {group-attribute {<group-att> | member | uniqueMember} | group-dn <group-dn>}
no ldap {group-attribute | group-dn}
```

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

**Syntax Description**

- **group-att**: Specifies a custom attribute name.
- **member**: groupOfNames or group membership attribute.
- **uniqueMember**: groupOfUniqueNames membership attribute.
- **group-dn**: DN of group required for authorization.

**Default**

- **group-att**: member
- **group-dn**: ""

**Configuration Mode**

Config

**History**

3.1.0000

3.4.0000 Updated Example

**Role**

admin

**Example**

```
switch (config) # ldap group-attribute member
switch (config) # ldap group-dn my-group-dn
switch (config) # show ldap
User base DN   : ou=department,dc=example,dc=com
User search scope: subtree
Login attribute: sAMAccountName
Bind DN        : my-dn
Bind password  : my-password
Group base DN  : my-group-dn
Group attribute: member
LDAP version   : 3
Referrals      : yes
Server port    : 389
Search Timeout : 5
Bind Timeout   : 5
SSL mode       : none
Server SSL port: 636 (not active)
SSL ciphers    : TLS1.2 (not active)
SSL cert verify: yes
SSL ca-list    : default-ca-list

LDAP servers:
  1: 10.10.10.10
  2: 10.10.10.12
switch (config) #
```
<table>
<thead>
<tr>
<th>Related Commands</th>
<th>show ldap</th>
</tr>
</thead>
<tbody>
<tr>
<td>Notes</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• 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</td>
</tr>
<tr>
<td></td>
<td>• 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.</td>
</tr>
</tbody>
</table>
**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.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>IP Address</th>
<th>IPv4 or IPv6 address.</th>
</tr>
</thead>
<tbody>
<tr>
<td>number</td>
<td>number</td>
<td>The order of the LDAP server.</td>
</tr>
<tr>
<td>last</td>
<td>last</td>
<td>The LDAP server will be added in the last location.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Default</th>
<th>No hosts configured</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuration Mode</td>
<td>Config</td>
</tr>
<tr>
<td>History</td>
<td>3.1.0000</td>
</tr>
<tr>
<td></td>
<td>3.4.0000</td>
</tr>
<tr>
<td></td>
<td>Updated Example</td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
</tr>
</tbody>
</table>

**Example**

```
switch (config) # ldap host 10.10.10.10
switch (config) # show ldap
User base DN      : ou=department,dc=example,dc=com
User search scope : subtree
Login attribute   : sAMAccountName
Bind DN           : my-dn
Bind password     : my-password
Group base DN     : my-group-dn
Group attribute   : member
LDAP version      : 3
Referrals         : yes
Server port       : 389
Search Timeout    : 5
Bind Timeout      : 5
SSL mode          : none
Server SSL port   : 636 (not active)
SSL ciphers       : TLS1.2 (not active)
SSL cert verify   : yes
SSL ca-list       : default-ca-list

LDAP servers:
  1: 10.10.10.10
  2: 10.10.10.12
```

switch (config) #
| Related Commands | show aaa  
|                 | show ldap |  
| Notes           | • The system will select the LDAP host to try according to its order  
|                 | • New servers are by default added at the end of the list of servers |
ldap login-attribute

ldap login-attribute {<string> | uid | sAMAccountName}
no ldap login-attribute

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

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>string</th>
<th>Custom attribute name.</th>
</tr>
</thead>
<tbody>
<tr>
<td>uid</td>
<td>uid</td>
<td>LDAP login name is taken from the user login username.</td>
</tr>
<tr>
<td>sAMAccountName</td>
<td>sAMAccountName</td>
<td>SAM Account name, active directory login name.</td>
</tr>
</tbody>
</table>

**Default**
sAMAccountName

**Configuration Mode**
Config

**History**
3.1.0000
3.4.0000 Updated Example

**Role**
admin

**Example**
```
switch (config) # ldap login-attribute uid
switch (config) # show ldap
User base DN : ou=department,dc=example,dc=com
User search scope : subtree
Login attribute : uid
Bind DN : my-dn
Bind password : my-password
Group base DN : my-group-dn
Group attribute : member
LDAP version : 3
Referrals : yes
Server port : 389
Search Timeout : 5
Bind Timeout : 5
SSL mode : none
Server SSL port : 636 (not active)
SSL ciphers : TLS1.2 (not active)
SSL cert verify : yes
SSL ca-list : default-ca-list

LDAP servers:
  1: 10.10.10.10
  2: 10.10.10.12
```

**Related Commands**
show aaa
show ldap

**Notes**
**ldap port**

`ldap port <port>`

`no ldap port`

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

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>port</th>
<th>TCP port number.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>389</td>
<td></td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Config</td>
<td></td>
</tr>
<tr>
<td>History</td>
<td>3.1.0000</td>
<td></td>
</tr>
<tr>
<td></td>
<td>3.4.0000</td>
<td>Updated Example</td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
<td></td>
</tr>
</tbody>
</table>
| Example            | switch (config) # ldap port 1111  
switch (config) # show ldap
User base DN        : ou=department,dc=example,dc=com
User search scope   : subtree
Login attribute     : uid
Bind DN             : my-dn
Bind password       : my-password
Group base DN       : my-group-dn
Group attribute     : member
LDAP version        : 3
Referrals           : yes
Server port         : 1111
Search Timeout      : 5
Bind Timeout        : 5
SSL mode            : none
Server SSL port     : 636 (not active)
SSL ciphers         : TLS1.2 (not active)
SSL cert verify     : yes
SSL ca-list         : default-ca-list

LDAP servers:
1: 10.10.10.10
2: 10.10.10.12

Related Commands
show aaa
show ldap

Notes
ldap referrals

ldap referrals
no ldap referrals

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

Syntax Description | N/A
--- | ---
Default | LDAP referrals are enabled
Configuration Mode | Config
History | 3.1.0000
 | 3.4.0000 Updated Example
Role | admin
Example | switch (config) # no ldap referrals
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

Related Commands | show aaa
 | show ldap
Notes | Referral is the process by which an LDAP server, instead of returning a result, will return a referral (a reference) to another LDAP server which may contain further information.
**ldap scope**

`ldap scope <scope>`

`no ldap scope`

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

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

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>scope</th>
</tr>
</thead>
<tbody>
<tr>
<td>- one-level - searches the immediate children of the base dn</td>
<td></td>
</tr>
<tr>
<td>- subtree - searches at the base DN and all its children</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Default</th>
<th>subtree</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Configuration Mode</th>
<th>Config</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>History</th>
<th>3.1.0000</th>
</tr>
</thead>
</table>

3.4.0000 Updated Example

<table>
<thead>
<tr>
<th>Role</th>
<th>admin</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Example</th>
</tr>
</thead>
</table>
| switch (config) # ldap scope subtree  
switch (config) # show ldap  
User base DN : ou=department,dc=example,dc=com  
User search scope : subtree  
Login attribute : uid  
Bind DN : my-dn  
Bind password : my-password  
Group base DN : my-group-dn  
Group attribute : member  
LDAP version : 3  
Referrals : no  
Server port : 1111  
Search Timeout : 5  
Bind Timeout : 5  
SSL mode : none  
Server SSL port : 636 (not active)  
SSL ciphers : TLS1.2 (not active)  
SSL cert verify : yes  
SSL ca-list : default-ca-list  

LDAP servers:  
1: 10.10.10.10  
2: 10.10.10.12  
switch (config) # |

| Related Commands | show aaa  
show ldap |

| Notes | |
**ldap ssl**

*ldap ssl*  
{ca-list <options> | cert-verify | ciphers {all | TLS1.2] | mode <mode> | port <port-number>}

*no ldap ssl* {cert-verify | ciphers | mode | port}

Sets SSL parameter for LDAP.
The no form of the command resets the attribute to its default value.
**Syntax Description**

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

**Default**

cert-verify: enabled  
mode: none (LDAP SSL is not activated)  
port-number: 636  
ciphers: all

**Configuration Mode**

Config
**History**

3.1.0000  First version
3.2.3000  Added ca-list argument.
3.4.0000  Added “ssl ciphers” parameter
Updated Example

**Role**

admin

**Example**

```plaintext
switch (config) # ldap ssl mode ssl
switch (config) # show ldap
User base DN : ou=department,dc=example,dc=com
User search scope : subtree
Login attribute : uid
Bind DN : my-dn
Bind password : my-password
Group base DN : my-group-dn
Group attribute : member
LDAP version : 3
Referrals : no
Server port : 1111
Search Timeout : 5
Bind Timeout : 5
SSL mode : ssl
Server SSL port : 36 (not active)
SSL ciphers : TLS1.2 (not active)
SSL cert verify : yes
SSL ca-list : default-ca-list

LDAP servers:
  1: 10.10.10.10
  2: 10.10.10.12
switch (config) #
```

**Related Commands**

show aaa
show ldap

**Notes**

- If available, the TLS mode is recommended, as it is standardized, and may also be of higher security
- The port number is used only for SSL mode. In case the mode is TLS, the LDAP port number will be used.
**ldap timeout**

```
ldap {timeout-bind | timeout-search} <seconds>
no ldap {timeout-bind | timeout-search}
```

Sets a global communication timeout in seconds for all LDAP servers to specify the extent of the search in the LDAP hierarchy that the server should make when it receives an authorization request. The no form of the command resets the attribute to its default value.

| Syntax Description | timeout-bind | Sets the global LDAP bind timeout for all LDAP servers.
|                    | timeout-search | Sets the global LDAP search timeout for all LDAP servers.
| seconds            | Range: 1-60 seconds. |

| Default | 5 seconds |
| Configuration Mode | Config |
| History | 3.1.0000 |
|          | 3.4.0000 Updated Example |
| Role | admin |

**Example**

```
switch (config) # ldap timeout-bind 10
switch (config) # show ldap
User base DN : ou=department,dc=example,dc=com
User search scope : subtree
Login attribute : uid
Bind DN : my-dn
Bind password : my-password
Group base DN : my-group-dn
Group attribute : member
LDAP version : 3
Referrals : no
Server port : 1111
Search Timeout : 5
Bind Timeout : 10
SSL mode : none
Server SSL port : 636 (not active)
SSL ciphers : TLS1.2 (not active)
SSL cert verify : yes
SSL ca-list : default-ca-list

LDAP servers:
  1: 10.10.10.10
  2: 10.10.10.12
```

switch (config) #
Related Commands

- show aaa
- show ldap

Notes
### ldap version

**ldap version <version>**
**no ldap version**

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

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>version</th>
<th>Sets the LDAP version. Values: 2 and 3.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>3</td>
<td></td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Config</td>
<td></td>
</tr>
<tr>
<td>History</td>
<td>3.1.0000</td>
<td></td>
</tr>
<tr>
<td></td>
<td>3.4.0000</td>
<td>Updated Example</td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
<td></td>
</tr>
</tbody>
</table>

**Example**

```
switch (config) # ldap version 3
switch (config) # show ldap
User base DN : ou=department,dc=example,dc=com
User search scope : subtree
Login attribute : uid
Bind DN : my-dn
Bind password : my-password
Group base DN : my-group-dn
Group attribute : member
LDAP version : 3
Referrals : no
Server port : 1111
Search Timeout : 5
Bind Timeout : 10
SSL mode : none
Server SSL port : 636 (not active)
SSL ciphers : TLS1.2 (not active)
SSL cert verify : yes
SSL ca-list : default-ca-list

LDAP servers:
1: 10.10.10.10
2: 10.10.10.12
```

**Related Commands**

- show aaa
- show ldap

**Notes**
# show ldap

Displays LDAP configurations.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>N/A</td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Any Command Mode</td>
</tr>
<tr>
<td>History</td>
<td>3.1.0000</td>
</tr>
<tr>
<td>3.4.0000</td>
<td>Updated Example</td>
</tr>
</tbody>
</table>

**Role**

`admin`

**Example**

```
switch (config) # show ldap
User base DN       : ou=department,dc=example,dc=com
User search scope  : subtree
Login attribute    : uid
Bind DN            : my-dn
Bind password      : my-password
Group base DN      : my-group-dn
Group attribute    : member
LDAP version       : 3
Referrals          : no
Server port        : 1111
Search Timeout     : 5
Bind Timeout       : 10
SSL mode           : none
Server SSL port    : 636 (not active)
SSL ciphers        : TLS1.2 (not active)
SSL cert verify    : yes
SSL ca-list        : default-ca-list

LDAP servers:
  1: 10.10.10.10
  2: 10.10.10.12
switch (config) #
```

**Related Commands**

- show aaa
- show ldap

**Notes**
4.9.4.6 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.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>Disabled</td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Config</td>
</tr>
<tr>
<td>History</td>
<td>3.5.0200</td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
</tr>
<tr>
<td>Example</td>
<td>switch (config) # system secure-mode enable</td>
</tr>
<tr>
<td></td>
<td>Warning! Configuration is about to be saved and the system will be reloaded.</td>
</tr>
<tr>
<td></td>
<td>Type 'YES' to confirm the change in secure mode: YES</td>
</tr>
<tr>
<td>Related Commands</td>
<td>user &lt;username&gt; password &lt;password&gt;</td>
</tr>
<tr>
<td></td>
<td>ssh server min-version</td>
</tr>
<tr>
<td></td>
<td>ssh server security strict</td>
</tr>
<tr>
<td></td>
<td>snmp-server user</td>
</tr>
<tr>
<td></td>
<td>no neighbor &lt;ip-address&gt; password</td>
</tr>
<tr>
<td></td>
<td>ntp server disable</td>
</tr>
<tr>
<td></td>
<td>ntp server keyID</td>
</tr>
<tr>
<td></td>
<td>router bgp neighbor password</td>
</tr>
<tr>
<td></td>
<td>router bgp peer-group password</td>
</tr>
</tbody>
</table>

Notes
Before enabling secure mode, the command performs the following configuration checks:
- NTP Key ID cannot be MD5 when secure mode is enabled
- SSH min-version cannot be 1 when enabling secure mode
- SSH security must be set to strict security
- SNMPv3 user auth cannot be md5 when enabling secure mode
- SNMPv3 user priv cannot be des when enabling secure mode
- SNMPv3 trap auth cannot be md5 when enabling secure mode
- SNMPv3 trap priv cannot be des when enabling secure mode
- Router BGP neighbor password cannot be set when enabling secure mode
- Router BGP peer-group password cannot be set when enabling with secure mode
- User password hash cannot be MD5 when secure mode is enabled
Only if the check passes, secure mode is enabled on the switch system.
### show system secure-mode

**Description:** Displays the security mode of the switch system.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>N/A</td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Any Command Mode</td>
</tr>
<tr>
<td>History</td>
<td>3.4.2300</td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
</tr>
</tbody>
</table>

**Example**

```bash
switch (config) # show system secure-mode
Secure mode configured: yes
Secure mode enabled : yes
switch (config) #
```

**Related Commands**

- `system secure-mode enable`

**Notes**

- “Secure mode configuration” describes the user configuration
- “Secure mode enabled” describes the system state
4.10 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.

4.10.1 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.
### crypto encrypt-data

```
crypto encrypt-data key-location <local | usb> key <password>
no crypto encrypt-data
```

Enables and configures system file encryption. The no form of the command decrypts sensitive information on the system.

| Syntax Description | key-location | Configures where to store the encryption key:
|                    |              | • local – Stores the key locally
|                    |              | • usb – Stores the key on a USB device
| Default            | N/A          | key
| Configuration Mode | Config       | Configures a key
| History            | 3.6.1002     | 
| Role               | admin        | 
| Example            | switch (config)# crypto encrypt-data key-location usb key mypassword |

**Warning!** All sensitive files are about to be encrypted
- System will perform reset factory, configuration files will be preserved
- System will be rebooted
- Do not power-off, wait for the system to boot

Type 'YES' to confirm this action: YES

**Related Commands**

**Notes**
- It is recommended to store the encryption password on a USB device rather than locally
- Enabling encryption may slightly slow system performance
- If the key is stored on the USB, it must be plugged into the switch in order for the switch to boot. After the switch has booted, the USB key is no longer required and, for security purposes, it is recommended to remove it after running “usb eject”. The USB key may be needed again if the switch is rebooted or if the switch needs to be decrypted.
**crypto ipsec ike**

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

Manage the IKE (ISAKMP) process or database state

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear</td>
<td>Clears IKE (ISAKMP) peering state</td>
</tr>
<tr>
<td>sa</td>
<td>Clears IKE generated ISAKMP and IPSec security associations (remote peers are affected)</td>
</tr>
<tr>
<td>peer</td>
<td>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)</td>
</tr>
<tr>
<td>IPv4 or IPv6 address</td>
<td>Clears security associations for the specified IKE peering (remote peer is affected)</td>
</tr>
<tr>
<td>local</td>
<td>Clear security associations for the specified/all IKE peering (remote peer is affected)</td>
</tr>
<tr>
<td>restart</td>
<td>Restarts the IKE (ISAKMP) daemon (clears all IKE state, peers may be affected)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Default</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuration Mode</td>
<td>Config</td>
</tr>
<tr>
<td>History</td>
<td>3.2.3000</td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
</tr>
</tbody>
</table>

**Example**

```
switch (config)# crypto ipsec ike restart
```

**Related Commands**

N/A

**Notes**

N/A
crypto ipsec peer local

crypto ipsec peer <IPv4 or IPv6 address> local <IPv4 or IPv6 address> {enable | keying {ike [auth {hmac-md5 | hmac-sha1 | hmac-sha256 | null} | dh-group | disable | encrypt | exchange-mode | lifetime | local | mode | peer-identity | pfs-group | preshared-key | prompt-preshared-key | transform-set] | manual [auth | disable | encrypt | local-spi | mode | remote-spi]}}

Configures ipsec in the system.
### Syntax Description

<table>
<thead>
<tr>
<th><strong>Syntax</strong></th>
<th><strong>enable</strong></th>
<th><strong>ike</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>Enables IPSec peering.</td>
<td>Configures IPSec peering using IKE ISAKMP to manage SA keys. It has the following optional parameters:</td>
</tr>
<tr>
<td>ike</td>
<td></td>
<td>• auth: Configures the authentication algorithm for IPSec peering</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• dh-group: Configures the phase1 Diffie-Hellman group proposed for secure IKE key exchange</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• disable: Configures this IPSec peering administratively disabled</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• encrypt: Configures the encryption algorithm for IPSec peering</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• exchange-mode: Configures the IKE key exchange mode to propose for peering</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• lifetime: Configures the SA lifetime to propose for this IPSec peering</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• local-identity: Configures the ISAKMP payload identification value to send as local endpoint's identity</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• mode: Configures the peering mode for this IPSec peering</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• peer-identity: Configures the identification value to match against the peer's ISAKMP payload identification</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• pfs-group: Configures the phase2 PFS (Perfect Forwarding Secrecy) group to propose for Diffie-Hellman exchange for this IPSec peering</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• preshared-key: Configures the IKE pre-shared key for the IPSec peering</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• prompt-preshared-key: Prompts for the pre-shared key, rather than entering it on the command line</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• transform-set: Configures transform proposal parameters</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>keying</strong></th>
<th>Configures key management for this IPSec peering:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• auth: Configures the authentication algorithm for this IPSec peering</td>
</tr>
<tr>
<td></td>
<td>• disable: Configures this IPSec peering administratively disabled</td>
</tr>
<tr>
<td></td>
<td>• encrypt: Configures the encryption algorithm for this IPSec peering</td>
</tr>
<tr>
<td></td>
<td>• local-spi: Configures the local SPI for this manual IPSec peering</td>
</tr>
<tr>
<td></td>
<td>• mode: Configures the peering mode for this IPSec peering</td>
</tr>
<tr>
<td></td>
<td>• remote-spi: Configures the remote SPI for this manual IPSec peering</td>
</tr>
<tr>
<td>Default</td>
<td>N/A</td>
</tr>
<tr>
<td>------------------</td>
<td>----------------------</td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Config</td>
</tr>
<tr>
<td>History</td>
<td>3.2.3000</td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
</tr>
<tr>
<td>Example</td>
<td><code>switch (config)# crypto ipsec peer 10.10.10.10 local 10.7.34.139 enable</code>&lt;br&gt;<code>switch (config)#</code></td>
</tr>
<tr>
<td>Related Commands</td>
<td>N/A</td>
</tr>
<tr>
<td>Notes</td>
<td></td>
</tr>
</tbody>
</table>
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.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>cert-name</td>
<td>The name of the certificate.</td>
</tr>
</tbody>
</table>

| Default         | N/A |
| Configuration Mode | Config |
| History         | 3.2.3000 |
| Role            | admin |

**Example**

switch (config) # crypto certificate default-cert name test

**Related Commands**

N/A

**Notes**

- Two certificates with the same subject and issuer fields cannot both be placed onto the CA list
- The no form of the command does not delete the certificate from the certificate database
- Unless specified otherwise, applications that use CA certificates will still consult the well-known certificate bundle before looking at the default-ca-list
**crypto certificate default-cert**

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

Designates the named certificate as the global default certificate role for authentication of this system to clients.
The no form of the command reverts the default-cert name to “system-self-signed” (the “cert-name” value is optional and ignored).

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>cert-name</td>
<td>The name of the certificate.</td>
</tr>
</tbody>
</table>

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

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

Configures default values for certificate generation.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>country-code</th>
<th>Configures the default certificate value for country code with a two-alphanumeric-character code or -- for none.</th>
</tr>
</thead>
<tbody>
<tr>
<td>days-valid</td>
<td></td>
<td>Configures the default certificate value for days valid.</td>
</tr>
<tr>
<td>email-addr</td>
<td></td>
<td>Configures the default certificate value for email address.</td>
</tr>
<tr>
<td>hash-algorithm {sha1</td>
<td>sha256}</td>
<td></td>
</tr>
<tr>
<td>key-size-bits</td>
<td></td>
<td>Configures the default certificate value for private key size. (Private key length in bits – at least 1024, but 2048 is strongly recommended.)</td>
</tr>
<tr>
<td>locality</td>
<td></td>
<td>Configures the default certificate value for locality.</td>
</tr>
<tr>
<td>org-unit</td>
<td></td>
<td>Configures the default certificate value for organizational unit.</td>
</tr>
<tr>
<td>organization</td>
<td></td>
<td>Configures the default certificate value for the organization name.</td>
</tr>
<tr>
<td>state-or-prov</td>
<td></td>
<td>Configures the default certificate value for state or province.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Default</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuration Mode</td>
<td>Config</td>
</tr>
<tr>
<td>History</td>
<td>3.2.1000</td>
</tr>
<tr>
<td></td>
<td>3.3.4350</td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
</tr>
<tr>
<td>Example</td>
<td>switch (config) # crypto certificate generation default hash-algorithm sha256</td>
</tr>
<tr>
<td>Related Commands</td>
<td>N/A</td>
</tr>
<tr>
<td>------------------</td>
<td>-----</td>
</tr>
<tr>
<td>Notes</td>
<td>The default hashing algorithm used is sha1.</td>
</tr>
</tbody>
</table>
crypto certificate name

crypto certificate name [<cert-name> | system-self-signed] {comment <new
certificate-name-value> | 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.
<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>cert-name</th>
<th>Unique name by which the certificate is identified.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>comment</td>
<td>Specifies a certificate comment.</td>
</tr>
<tr>
<td>generate self-signed</td>
<td>Generates certificates. This option has the following parameters which may be entered sequentially in any order:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• comment: Specifies a certificate comment (free string)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• common-name: Specifies the common name of the issuer and subject (e.g. a domain name)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• country-code: Specifies the country alphanumeric-character country code, or “-” for none)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• days-valid: Specifies the number of days the certificate is valid</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• email-addr: Specifies the email address</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• hash-algorithm: Specifies the hashing function used for signature algorithm</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• 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)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• locality: Specifies the locality name</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• org-unit: Specifies the organizational unit name</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• organization: Specifies the organization name</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• serial-num: Specifies the serial number for the certificate (a lower-case hexadecimal serial number prefixed with “0x”)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• state-or-prov: Specifies the state or province name</td>
<td></td>
</tr>
<tr>
<td>private-key pem</td>
<td>Specifies certificate contents in PEM format.</td>
<td></td>
</tr>
<tr>
<td>prompt-private-key</td>
<td>Prompts for certificate private key with secure echo.</td>
<td></td>
</tr>
<tr>
<td>public-cert</td>
<td>Installs a certificate.</td>
<td></td>
</tr>
<tr>
<td>regenerate</td>
<td>Regenerates the named certificate using configured certificate generation default values for the specified validity period</td>
<td></td>
</tr>
<tr>
<td>rename</td>
<td>Renames the certificate.</td>
<td></td>
</tr>
</tbody>
</table>

**Default**

N/A

**Configuration Mode**

Config
### History

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.2.3000</td>
<td>First version</td>
</tr>
<tr>
<td>3.3.4402</td>
<td>Added “hash-algorithm” parameter</td>
</tr>
</tbody>
</table>

### Role

<table>
<thead>
<tr>
<th>Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>admin</td>
</tr>
</tbody>
</table>

### Example

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

### Related Commands

<table>
<thead>
<tr>
<th>Commands</th>
</tr>
</thead>
<tbody>
<tr>
<td>N/A</td>
</tr>
</tbody>
</table>

### Notes
**crypto certificate system-self-signed**

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

Configures default values for certificate generation.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>days-valid</th>
<th>Specifies the number of days the certificate is valid</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>N/A</td>
<td></td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Config</td>
<td></td>
</tr>
<tr>
<td>History</td>
<td>3.2.1000</td>
<td></td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
<td></td>
</tr>
<tr>
<td>Example</td>
<td>switch (config) # crypto certificate system-self-signed regenerate days-valid 3</td>
<td></td>
</tr>
<tr>
<td>Related Commands</td>
<td>N/A</td>
<td></td>
</tr>
<tr>
<td>Notes</td>
<td>N/A</td>
<td></td>
</tr>
</tbody>
</table>
**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.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>ca-list</th>
<th>Displays the list of supplemental certificates configured for the global default system CA certificate role.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>default-ca-list</td>
<td>Displays information about the currently configured default certificates of the CA list.</td>
</tr>
<tr>
<td></td>
<td>default-cert</td>
<td>Displays information about the currently configured default certificate.</td>
</tr>
<tr>
<td></td>
<td>detail</td>
<td>Displays all attributes related to the certificate.</td>
</tr>
<tr>
<td></td>
<td>name</td>
<td>Displays information about the certificate specified.</td>
</tr>
<tr>
<td></td>
<td>public-pem</td>
<td>Displays the uninterpreted public certificate as a PEM formatted data string</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Default</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuration Mode</td>
<td>Config</td>
</tr>
<tr>
<td>History</td>
<td>3.2.1000</td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
</tr>
</tbody>
</table>
Example

switch (config)# show crypto certificate
Certificate with name 'system-self-signed' (default-cert)
    Comment: system-generated self-signed certificate
    Private Key: present
    Serial Number: 0x546c935511bcac21ac0e8249fbe0844
    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.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>N/A</td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Config</td>
</tr>
<tr>
<td>History</td>
<td>3.6.1002</td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
</tr>
</tbody>
</table>

#### Example

```
switch (config)# show crypto encrypt-data
Sensitive files encryption:
  Status: enabled
  Key location: usb
  Cipher: aes256
switch (config)#
```

#### Related Commands

N/A

#### Notes
**show crypto ipsec**

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

Displays information ipsec configuration.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>N/A</td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Config</td>
</tr>
<tr>
<td>History</td>
<td>3.2.1000</td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
</tr>
</tbody>
</table>
| Example            | switch (config)# show crypto ipsec  
|                    | IPSec Summary  
|                    | ---------------  
|                    | Crypto IKE is using pluto (Openswan) daemon.  
|                    | Daemon process state is stopped.  
|                    | No IPSec peers configured.  
|                    | IPSec IKE Peering State  
|                    | ------------------------  
|                    | Crypto IKE is using pluto (Openswan) daemon.  
|                    | Daemon process state is stopped.  
|                    | No active IPSec IKE peers.  
|                    | IPSec Policy State  
|                    | -----------------  
|                    | No active IPSec policies.  
|                    | IPSec Security Association State  
|                    | --------------------------  
|                    | No active IPSec security associations.  
|                    | switch (config)# |
| Related Commands   | N/A |
| Notes              | N/A |
4.11 Scheduled Jobs

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

4.11.1 Commands

job

```
job <job ID>
no job <job ID>
```

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

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>job ID</th>
<th>An integer.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>N/A</td>
<td></td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Config</td>
<td></td>
</tr>
<tr>
<td>History</td>
<td>3.1.0000</td>
<td></td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
<td></td>
</tr>
</tbody>
</table>
| Example            | switch (config) # job 100
                    switch (config job 100) # |
| Related Commands   | show jobs |
| Notes              | Job state is lost on reboot. |
**command**

**Syntax**

```
command <sequence #> | <command>
no command <sequence #>
```

Adds a CLI command to the job. The no form of the command deletes the command from the job.

**Syntax Description**

<table>
<thead>
<tr>
<th>Sequence #</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>sequence #</td>
<td>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.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>command</td>
<td>A CLI command.</td>
</tr>
</tbody>
</table>

**Default**

N/A

**Configuration Mode**

Config job

**History**

3.1.0000

**Role**

admin

**Example**

```
switch (config)# job 100
switch (config job 100) # command 10 "show power"
switch (config job 100) #
```

**Related Commands**

- show jobs

**Notes**

- The command must be defined with inverted commas (""")
- The command must be added as it was executed from the “config” mode. For example, in order to change the interface description you need to add the command: “interface <type> <number> description my-description”.
**comment**

```
comment <comment>
no comment
```

Adds a comment to the job. The no form of the command deletes the comment.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>comment</th>
<th>The comment to be added (string).</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>&quot;&quot;</td>
<td></td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Config job</td>
<td></td>
</tr>
<tr>
<td>History</td>
<td>3.1.0000</td>
<td></td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
<td></td>
</tr>
</tbody>
</table>
| Example             | switch (config)# job 100  
switch (config job 100) # comment Job_for_example  
switch (config job 100) # |
| Related Commands    | show jobs |                                |
| Notes               |         |                                  |
**enable**

```
enable
no enable
```

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

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

execute

Forces an immediate execution of the job.

<table>
<thead>
<tr>
<th><strong>Syntax Description</strong></th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Default</strong></td>
<td>N/A</td>
</tr>
<tr>
<td><strong>Configuration Mode</strong></td>
<td>Config job</td>
</tr>
<tr>
<td><strong>History</strong></td>
<td>3.1.0000</td>
</tr>
<tr>
<td><strong>Role</strong></td>
<td>admin</td>
</tr>
</tbody>
</table>
| **Example**             | switch (config)# job 100  
                          | switch (config job 100) # execute  
                          | switch (config job 100) # |
| **Related Commands**    | show jobs |
| **Notes**               | • The job timer (if set) is not canceled and the job state is not changed: i.e. the time of the next automatic execution is not affected  
                          • The job will not be run if not currently enabled |
## fail-continue

### Syntax Description

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>N/A</th>
</tr>
</thead>
</table>

### Default

<table>
<thead>
<tr>
<th>Default</th>
<th>A job will halt execution as soon as any of its commands fails</th>
</tr>
</thead>
</table>

### Configuration Mode

<table>
<thead>
<tr>
<th>Configuration Mode</th>
<th>Config job</th>
</tr>
</thead>
</table>

### History

<table>
<thead>
<tr>
<th>History</th>
<th>3.1.0000</th>
</tr>
</thead>
</table>

### Role

<table>
<thead>
<tr>
<th>Role</th>
<th>admin</th>
</tr>
</thead>
</table>

### Example

```
switch (config)# job 100
switch (config job 100) # fail-continue
switch (config job 100) #
```

### Related Commands

<table>
<thead>
<tr>
<th>Related Commands</th>
<th>show jobs</th>
</tr>
</thead>
</table>

### Notes
name

name <job name>
no name

Configures a name for this job.
The no form of the command resets the name to its default.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>name</th>
<th>Specifies a name for the job (string).</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td></td>
<td>&quot;&quot;.</td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Config job</td>
<td></td>
</tr>
<tr>
<td>History</td>
<td>3.1.0000</td>
<td></td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
<td></td>
</tr>
</tbody>
</table>
| Example            | switch (config)# job 100
                  switch (config job 100) # name my-job
                  switch (config job 100) # |
| Related Commands   | show jobs                               |
| Notes              |                                            |
schedule type

schedule type <recurrence type>
no schedule type

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

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>recurrence type</th>
<th>The available schedule types are:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>• daily - the job is executed every day at a specified time</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• weekly - the job is executed on a weekly basis</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• monthly - the job is executed every month on a specified day of the month</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• once - the job is executed once at a single specified date and time</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• periodic - the job is executed on a specified fixed time interval, starting from a fixed point in time.</td>
</tr>
</tbody>
</table>

Default: once

Configuration Mode: Config job

History: 3.1.0000

Role: admin

Example:

switch (config) # job 100
switch (config job 100) # schedule type once
switch (config job 100) #

Related Commands: show jobs

Notes: A schedule type is essentially a structure for specifying one or more future dates and times for a job to execute.
schedule <recurrence type>
schedule <recurrence type> <interval and date>
no schedule

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

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>recurrence type</th>
<th>The available schedule types are:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>• daily - the job is executed every day at a specified time</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• weekly - the job is executed on a weekly basis</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• monthly - the job is executed every month on a specified day of the month</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• once - the job is executed once at a single specified date and time</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• periodic - the job is executed on a specified fixed time interval, starting from a fixed point in time.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Default</th>
<th>once</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuration Mode</td>
<td>Config job</td>
</tr>
<tr>
<td>History</td>
<td>3.1.0000</td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
</tr>
</tbody>
</table>

Example

switch (config)# job 100
switch (config job 100) # schedule monthly interval 10
switch (config job 100) #

Related Commands | show jobs |

Notes

A schedule type is essentially a structure for specifying one or more future dates and times for a job to execute.
show jobs

show jobs [<job-id>]

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

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>job-id</th>
<th>Job ID.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>N/A</td>
<td></td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Config</td>
<td></td>
</tr>
<tr>
<td>History</td>
<td>3.1.0000</td>
<td></td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
<td></td>
</tr>
</tbody>
</table>

Example

```
switch (config) # show jobs 10
Job 10:
    Status:     inactive
    Enabled:    yes
    Continue on failure: no
    Schedule Type: once
    Time and date: 1970/01/01 00:00:00 +0000
    Last Exec Time: Thu 2012/04/05 13:11:42 +0000
    Next Exec Time: N/A
    Commands:
        Command 10: show power
    Last Output:
    ---------------------
    Module    Status
    ---------------------
    PS1       OK
    PS2       NOT PRESENT

switch (config) #
```

Related Commands

show jobs

Notes
4.12 Statistics and Alarms

4.12.1 Commands

**stats alarm <alarm-id> clear**

**stats alarm <alarm ID> clear**

Clears alarm state.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>alarm ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alarms supported by the system, for example:</td>
<td></td>
</tr>
<tr>
<td>• cpu_util_indiv - Average CPU utilization too high: percent utilization</td>
<td></td>
</tr>
<tr>
<td>• disk_io - Operating System Disk I/O per second too high: kilobytes per second</td>
<td></td>
</tr>
<tr>
<td>• fs_mnt - Free filesystem space too low: percent of disk space free</td>
<td></td>
</tr>
<tr>
<td>• intf_util - Network utilization too high: bytes per second</td>
<td></td>
</tr>
<tr>
<td>• memory_pct_used - Too much memory in use: percent of physical memory used</td>
<td></td>
</tr>
<tr>
<td>• paging - Paging activity too high: page faults</td>
<td></td>
</tr>
<tr>
<td>• temperature - Temperature is too high: degrees</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Default</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuration Mode</td>
<td>Config</td>
</tr>
<tr>
<td>History</td>
<td>3.1.0000</td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
</tr>
<tr>
<td>Example</td>
<td>switch (config) # stats alarm cpu_util_indiv clear</td>
</tr>
<tr>
<td>Related Commands</td>
<td>show stats alarm</td>
</tr>
<tr>
<td>Notes</td>
<td></td>
</tr>
</tbody>
</table>


stats alarm <alarm-id> enable

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

**Syntax Description**

<table>
<thead>
<tr>
<th>alarm ID</th>
<th>Alarms supported by the system, for example:</th>
</tr>
</thead>
<tbody>
<tr>
<td>cpu_util_indiv</td>
<td>Average CPU utilization too high: percent utilization</td>
</tr>
<tr>
<td>disk_io</td>
<td>Operating System Disk I/O per second too high: kilobytes per second</td>
</tr>
<tr>
<td>fs_mnt</td>
<td>Free filesystem space too low: percent of disk space free</td>
</tr>
<tr>
<td>intf_util</td>
<td>Network utilization too high: bytes per second</td>
</tr>
<tr>
<td>memory_pct_used</td>
<td>Too much memory in use: percent of physical memory used</td>
</tr>
<tr>
<td>paging</td>
<td>Paging activity too high: page faults</td>
</tr>
<tr>
<td>temperature</td>
<td>Temperature is too high: degrees</td>
</tr>
</tbody>
</table>

**Default**
The default is different per alarm-id

**Configuration Mode**
Config

**History**
3.1.0000

**Role**
admin

**Example**

```
switch (config) # stats alarm cpu_util_indiv enable
switch (config) #
```

**Related Commands**
show stats alarm

**Notes**
stats alarm <alarm-id> event-repeat

stats alarm <alarm ID> event-repeat {single | while-not-cleared}
no stats alarm <alarm ID> event-repeat

Configures repetition of events from this alarm.

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>alarm ID</th>
<th>Alarms supported by the system, for example:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>• cpu_util_indiv - Average CPU utilization too high: percent utilization</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• disk_io - Operating System Disk I/O per second too high: kilobytes per second</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• fs_mnt - Free filesystem space too low: percent of disk space free</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• intf_util - Network utilization too high: bytes per second</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• memory_pct_used - Too much memory in use: percent of physical memory used</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• paging - Paging activity too high: page faults</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• temperature - Temperature is too high: degrees</td>
</tr>
</tbody>
</table>

| Default | single | Does not repeat events: only sends one event whenever the alarm changes state. |
| Default | while-not-cleared | Repeats error events until the alarm clears. |

**Configuration Mode**

<table>
<thead>
<tr>
<th>Configuration Mode</th>
<th>Config</th>
</tr>
</thead>
</table>

**History**

<table>
<thead>
<tr>
<th>History</th>
<th>3.1.0000</th>
</tr>
</thead>
</table>

**Role**

<table>
<thead>
<tr>
<th>Role</th>
<th>monitor/admin</th>
</tr>
</thead>
</table>

**Example**

```
switch (config) # stats alarm cpu_util_indiv event-repeat single
switch (config) #
```

**Related Commands**

show stats alarm

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

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

Configure alarms thresholds.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>alarm ID</th>
<th>Alarms supported by the system, for example:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>• cpu_util_indiv - Average CPU utilization too high: percent utilization</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• disk_io - Operating System Disk I/O per second too high: kilobytes per second</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• fs_mnt - Free filesystem space too low: percent of disk space free</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• intf_util - Network utilization too high: bytes per second</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• memory_pct_used - Too much memory in use: percent of physical memory used</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• paging - Paging activity too high: page faults</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• temperature - Temperature is too high: degrees</td>
</tr>
</tbody>
</table>

falling Configures alarm for when the statistic falls too low.

rising Configures alarm for when the statistic rises too high.

error-threshold Sets threshold to trigger falling or rising alarm.

clear-threshold Sets threshold to clear falling or rising alarm.

threshold-value The desired threshold value, different per alarm.

Default Default is different per alarm-id

Configuration Mode Config

History 3.1.0000

Role admin

Example

```
switch (config) # stats alarm cpu_util_indiv falling clear-threshold 10
switch (config) #
```

Related Commands show stats alarm

Notes Not all alarms support all four thresholds.
**stats alarm <alarm-id> rate-limit**

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

Configures alarms rate limit.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
</table>
| alarm ID           | Alarms supported by the system, for example:  
|                    | - cpu_util_indiv - Average CPU utilization too  
|                    |   high: percent utilization  
|                    | - disk_io - Operating System Disk I/O per sec-
|                    |   ond too high: kilobytes per second  
|                    | - fs_mnt - Free filesystem space too low: percent  
|                    |   of disk space free  
|                    | - intf_util - Network utilization too high: bytes  
|                    |   per second  
|                    | - memory_pct_used - Too much memory in use: percent  
|                    |   of physical memory used  
|                    | - paging - Paging activity too high: page faults  
|                    | - temperature - Temperature is too high: degrees  

<table>
<thead>
<tr>
<th>count-type</th>
<th>Long medium, or short count (number of alarms).</th>
</tr>
</thead>
</table>
| reset              | Set the count and window durations to default val-
|                    | ues for this alarm. |

<table>
<thead>
<tr>
<th>window-type</th>
<th>Long medium, or short count, in seconds.</th>
</tr>
</thead>
</table>

**Default**

- Short window: 5 alarms in 1 hour
- Medium window: 20 alarms in 1 day
- Long window: 50 alarms in 7 days

**Configuration Mode**

Config

**History**

3.1.0000

**Role**

monitor/admin

**Example**

```
switch (config) # stats alarm paging rate-limit window long 2000
switch (config) #
```

**Related Commands**

show stats alarm

**Notes**
## stats chd <chd-id> clear

Clears CHD counters.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>CHD ID</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>CHD supported by the system, for example:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• cpu_util - CPU utilization: percentage of time spent</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• cpu_util_ave - CPU utilization average: percentage of time spent</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• cpu_util_day - CPU utilization average: percentage of time spent</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• disk_device_io_hour - Storage device I/O read/write statistics for the last hour: bytes</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• disk_io - Operating system aggregate disk I/O average (KB/sec)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• eth_day</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• eth_hour</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• eth_ip_day</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• eth_ip_hour</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• fs_mnt_day - Filesystem system usage average: bytes</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• fs_mnt_month - Filesystem system usage average: bytes</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• fs_mnt_week - Filesystem system usage average: bytes</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• ib_day</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• ib_hour</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• intf_day - Network interface statistics aggregation: bytes</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• intf_hour - Network interface statistics (same as “interface” sample)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• intf_util - Aggregate network utilization across all interfaces</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• memory_day - Average physical memory usage: bytes</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• memory_pct - Average physical memory usage</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• paging - Paging activity: page faults</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• paging_day - Paging activity: page faults</td>
</tr>
</tbody>
</table>

### Default
N/A

### Configuration Mode
Config

### History
3.1.0000

### Role
admin
| Example   | switch (config) # stats chd memory_day clear  
|-----------|---------------------------------------------
|           | switch (config) #                          |
| Related Commands | show stats chd |
stats chd <chd-id> enable

no stats chd <chd-id> enable

Enables the CHD.
The no form of the command disables the CHD.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>chd-id</th>
<th>CHD supported by the system, for example:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>• cpu_util - CPU utilization: percentage of time spent</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• cpu_util_ave - CPU utilization average: percentage of time spent</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• cpu_util_day - CPU utilization average: percentage of time spent</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• disk_device_io_hour - Storage device I/O read/write statistics for the last hour: bytes</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• disk_io - Operating system aggregate disk I/O average: KB/sec</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• eth_day</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• eth_hour</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• fs_mnt_day - Filesystem system usage average: bytes</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• fs_mnt_month - Filesystem system usage average: bytes</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• fs_mnt_week - Filesystem system usage average: bytes</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• ib_day</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• ib_hour</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• intf_day - Network interface statistics aggregation: bytes</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• intf_hour - Network interface statistics (same as “interface” sample)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• intf_util - Aggregate network utilization across all interfaces</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• memory_day - Average physical memory usage: bytes</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• memory_pct - Average physical memory usage</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• paging - Paging activity: page faults</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• paging_day - Paging activity: page faults</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Default</th>
<th>Enabled</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuration Mode</td>
<td>Config</td>
</tr>
<tr>
<td>History</td>
<td>3.1.0000</td>
</tr>
<tr>
<td>Role</td>
<td>monitor/admin</td>
</tr>
</tbody>
</table>
### Example

```plaintext
switch (config) # stats chd memory_day enable
switch (config) #
```

### Related Commands

`show stats chd`

### Notes
### stats chd <chd-id> compute time

```
stats chd <CHD ID> compute time [interval | range] <number of seconds>
```

Sets parameters for when this CHD is computed.

#### Syntax Description

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>CHD ID</th>
<th>Possible IDs:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>- cpu_util - CPU utilization: percentage of time spent</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- cpu_util_ave - CPU utilization average: percentage of time spent</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- cpu_util_day - CPU utilization average: percentage of time spent</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- disk_device_io_hour - Storage device I/O read/write statistics for the last hour: bytes</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- disk_io - Operating system aggregate disk I/O average: KB/sec</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- eth_day</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- eth_hour</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- fs_mnt_day - Filesystem system usage average: bytes</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- fs_mnt_month - Filesystem system usage average: bytes</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- fs_mnt_week - Filesystem system usage average: bytes</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- ib_day</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- ib_hour</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- intf_day - Network interface statistics aggregation: bytes</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- intf_hour - Network interface statistics (same as &quot;interface&quot; sample)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- intf_util - Aggregate network utilization across all interfaces</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- memory_day - Average physical memory usage: bytes</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- memory_pct - Average physical memory usage</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- paging - Paging activity: page faults</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- paging_day - Paging activity: page faults</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Possible IDs:</th>
</tr>
</thead>
<tbody>
<tr>
<td>- cpu_util - CPU utilization: percentage of time spent</td>
</tr>
<tr>
<td>- cpu_util_ave - CPU utilization average: percentage of time spent</td>
</tr>
<tr>
<td>- cpu_util_day - CPU utilization average: percentage of time spent</td>
</tr>
<tr>
<td>- disk_device_io_hour - Storage device I/O read/write statistics for the last hour: bytes</td>
</tr>
<tr>
<td>- disk_io - Operating system aggregate disk I/O average: KB/sec</td>
</tr>
<tr>
<td>- eth_day</td>
</tr>
<tr>
<td>- eth_hour</td>
</tr>
<tr>
<td>- fs_mnt_day - Filesystem system usage average: bytes</td>
</tr>
<tr>
<td>- fs_mnt_month - Filesystem system usage average: bytes</td>
</tr>
<tr>
<td>- fs_mnt_week - Filesystem system usage average: bytes</td>
</tr>
<tr>
<td>- ib_day</td>
</tr>
<tr>
<td>- ib_hour</td>
</tr>
<tr>
<td>- intf_day - Network interface statistics aggregation: bytes</td>
</tr>
<tr>
<td>- intf_hour - Network interface statistics (same as &quot;interface&quot; sample)</td>
</tr>
<tr>
<td>- intf_util - Aggregate network utilization across all interfaces</td>
</tr>
<tr>
<td>- memory_day - Average physical memory usage: bytes</td>
</tr>
<tr>
<td>- memory_pct - Average physical memory usage</td>
</tr>
<tr>
<td>- paging - Paging activity: page faults</td>
</tr>
<tr>
<td>- paging_day - Paging activity: page faults</td>
</tr>
</tbody>
</table>

#### interval

Specifies calculation interval (how often to do a new calculation) in number of seconds.

#### range

Specifies calculation range, in number of seconds.

#### number of seconds

Number of seconds.

### Default

Different per CHD
<table>
<thead>
<tr>
<th>Configuration Mode</th>
<th>Config</th>
</tr>
</thead>
<tbody>
<tr>
<td>History</td>
<td>3.1.0000</td>
</tr>
<tr>
<td>Role</td>
<td>monitor/admin</td>
</tr>
</tbody>
</table>
| 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              |        |
```markdown
**stats sample <sample-id> clear**

Clears sample history.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>sample ID</th>
<th>Possible sample IDs are:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>• congested</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• cpu_util - CPU utilization: milliseconds of time spent</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• disk_device_io - Storage device I/O statistics</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• disk_io - Operating system aggregate disk I/O: KB/sec</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• eth</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• eth-abc</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• eth_ip</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• fan - Fan speed</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• fs_mnt_bytes - Filesystem usage: bytes</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• fs_mnt_inodes - Filesystem usage: inodes</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• ib</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• interface - Network interface statistics</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• intf_util - Network interface utilization: bytes</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• memory - System memory utilization: bytes</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• paging - Paging activity: page faults</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• power - Power supply usage</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• power-consumption</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• temperature - Modules temperature</td>
</tr>
</tbody>
</table>

**Default**

N/A

**Configuration Mode**

Config

**History**

3.1.0000

**Role**

admin

**Example**

```
switch (config) # stats sample temperature clear
switch (config) #
```

**Related Commands**

show stats sample

**Notes**

---

Rev 4.60   Mellanox Technologies Confidential  437
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

Sets the amount of time between samples for the specified group of sample data.

Syntax Description

<table>
<thead>
<tr>
<th>Sample ID</th>
<th>Possible sample IDs are:</th>
</tr>
</thead>
<tbody>
<tr>
<td>congested</td>
<td>• congested</td>
</tr>
<tr>
<td>cpu_util</td>
<td>• cpu_util - CPU utilization: milliseconds of time spent</td>
</tr>
<tr>
<td>disk_device_io</td>
<td>• disk_device_io - Storage device I/O statistics</td>
</tr>
<tr>
<td>disk_io</td>
<td>• disk_io - Operating system aggregate disk I/O: KB/sec</td>
</tr>
<tr>
<td>eth</td>
<td>• eth</td>
</tr>
<tr>
<td>fan</td>
<td>• fan - Fan speed</td>
</tr>
<tr>
<td>fs_mnt_bytes</td>
<td>• fs_mnt_bytes - Filesystem usage: bytes</td>
</tr>
<tr>
<td>fs_mnt_inodes</td>
<td>• fs_mnt_inodes - Filesystem usage: inodes</td>
</tr>
<tr>
<td>ib</td>
<td>• ib</td>
</tr>
<tr>
<td>interface</td>
<td>• interface - Network interface statistics</td>
</tr>
<tr>
<td>intf_util</td>
<td>• intf_util - Network interface utilization: bytes</td>
</tr>
<tr>
<td>memory</td>
<td>• memory - System memory utilization: bytes</td>
</tr>
<tr>
<td>paging</td>
<td>• paging - Paging activity: page faults</td>
</tr>
<tr>
<td>power</td>
<td>• power - Power supply usage</td>
</tr>
<tr>
<td>power-consumption</td>
<td>• power-consumption</td>
</tr>
<tr>
<td>temperature</td>
<td>• temperature - Modules temperature</td>
</tr>
</tbody>
</table>

number of seconds | Interval in seconds.

Default | Different per sample

Configuration Mode | Config

History | 3.1.0000

Role | admin

Example

```
switch (config) # stats sample temperature interval 1
switch (config) # show stats sample temperature
Sample "temperature" (Modules temperature):
  Enabled: yes
  Sampling interval: 1 second
```

Related Commands | show stats sample

Notes
## stats clear-all

**stats clear all**

Clears data for all samples, CHDs, and status for all alarms.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>N/A</td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Config</td>
</tr>
<tr>
<td>History</td>
<td>3.1.0000</td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
</tr>
</tbody>
</table>

**Example**

```
switch (config) # stats clear-all
switch (config) #
```

**Related Commands**

N/A

**Notes**
stats export

stats export <format> <report name> [{after | before} <yyyy/mm/dd> <hh:mm:ss>] [filename <filename>]

Exports statistics to a file.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>format</th>
<th>Currently the only supported value for &lt;format&gt; is “csv” (comma-separated value).</th>
</tr>
</thead>
<tbody>
<tr>
<td>report name</td>
<td>report name</td>
<td>Determines dataset to be exported. Possible report names are:</td>
</tr>
<tr>
<td></td>
<td>memory</td>
<td>Memory utilization</td>
</tr>
<tr>
<td></td>
<td>paging</td>
<td>Paging I/O</td>
</tr>
<tr>
<td></td>
<td>cpu_util</td>
<td>CPU utilization</td>
</tr>
<tr>
<td>after</td>
<td>before</td>
<td>Only includes stats collected after or before a specific time.</td>
</tr>
<tr>
<td>yyyy/mm/dd</td>
<td>Date: It must be between 1970/01/01 and 2038/01/19.</td>
<td></td>
</tr>
<tr>
<td>hh:mm:ss</td>
<td>Time: It must be between 00:00:00 and 03:14:07 UTC and is treated as local time.</td>
<td></td>
</tr>
<tr>
<td>filename</td>
<td>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.</td>
<td></td>
</tr>
</tbody>
</table>

Default: N/A

Configuration Mode: Config

History: 3.1.0000

Role: admin

Example:

```
switch (config) # stats export csv memory filename mellanoxexample before 2000/08/14 15:59:50 after 2000/08/14 15:01:50
Generated report file: mellanoxexample.csv
switch (config) # show files stats
mellanoxexample.csv
switch (config) #
```
### Related Commands
- show files stats

### Notes
## show stats alarm

`show stats alarm [<Alarm ID> [rate-limit]]`

Displays status of all alarms or the specified alarm.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Alarm ID</th>
<th>May be:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>• cpu_util_indiv - Average CPU utilization too high: percent utilization</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• disk_io - Operating System Disk I/O per second too high: kilobytes per second</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• fs_mnt - Free filesystem space too low: percent of disk space free</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• intf_util - Network utilization too high: bytes per second</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• memory_pct_used - Too much memory in use: percent of physical memory used</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• paging - Paging activity too high: page faults</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• temperature - Temperature is too high: degrees</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th>rate-limit</th>
<th>Displays rate limit parameters.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>N/A</td>
<td></td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Config</td>
<td></td>
</tr>
<tr>
<td>History</td>
<td>3.1.0000</td>
<td></td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
<td></td>
</tr>
</tbody>
</table>

### Example

```
switch (config) # show stats alarm
Alarm cpu_util_indiv (Average CPU utilization too high): ok
Alarm disk_io (Operating System Disk I/O per second too high): (disabled)
Alarm fs_mnt (Free filesystem space too low): ok
Alarm intf_util (Network utilization too high): (disabled)
Alarm memory_pct_used (Too much memory in use): (disabled)
Alarm paging (Paging activity too high): ok
Alarm temperature (Temperature is too high): ok
switch (config) #
```

### Related Commands

- stats alarm

### Notes
**show stats chd**

```
show stats chd [<CHD ID>]
```

Displays configuration of all statistics CHDs.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>CHD ID</th>
<th>May be:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>- cpu_util_indiv - Average CPU utilization too high: percent utilization</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- disk_io - Operating System Disk I/O per second too high: kilobytes per second</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- fs_mnt - Free filesystem space too low: percent of disk space free</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- intf_util - Network utilization too high: bytes per second</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- memory_pct_used - Too much memory in use: percent of physical memory used</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- paging - Paging activity too high: page faults</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- temperature - Temperature is too high: degrees</td>
</tr>
</tbody>
</table>

| Default           | N/A    |
| Configuration Mode| Config |
| History           | 3.1.0000 |
| Role              | admin  |

**Example**

```
switch (config) # show stats chd disk_device_io_hour

CHD "disk_device_io_hour" (Storage device I/O read/write statistics for the last hour: bytes):
   Enabled: yes
   Source dataset: sample "disk_device_io"
   Computation basis: data points
   Interval: 1 data point(s)
   Range: 1 data point(s)
```

**Related Commands**

stats chd

**Notes**
show stats cpu

show stats cpu

Displays some basic stats about CPU utilization:
• the current level
• the peak over the past hour
• the average over the past hour

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>N/A</td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Config</td>
</tr>
<tr>
<td>History</td>
<td>3.1.0000</td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
</tr>
</tbody>
</table>
| Example            | switch (config) # show stats cpu
CPU 0
  Utilization: 6%
  Peak Utilization Last Hour: 16% at 2012/02/28 08:47:32
  Avg. Utilization Last Hour: 8%
switch (config) # |

Related Commands | N/A |

Notes
show stats sample

show stats sample [<sample ID>]

Displays sampling interval for all samples, or the specified one.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>sample ID</th>
<th>Possible sample IDs are:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>• congested</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• cpu_util - CPU utilization: milliseconds of time spent</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• disk_device_io - Storage device I/O statistics</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• disk_io - Operating system aggregate disk I/O: KB/sec</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• eth</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• fan - Fan speed</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• fs_mnt_bytes - Filesystem usage: bytes</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• fs_mnt_inodes - Filesystem usage: inodes</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• ib</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• interface - Network interface statistics</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• intf_util - Network interface utilization: bytes</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• memory - System memory utilization: bytes</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• paging - Paging activity: page faults</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• power - Power supply usage</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• power-consumption</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• temperature - Modules temperature</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Default</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuration Mode</td>
<td>Config</td>
</tr>
<tr>
<td>History</td>
<td>3.1.0000</td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
</tr>
</tbody>
</table>

Example

```
switch (config) # show stats sample fan
Sample "fan" (Fan speed):
   Enabled: yes
   Sampling interval: 1 minute 11 seconds
switch (config) #
```

Related Commands

N/A

Notes

N/A
4.13 **Chassis Management**

The chassis manager provides the user access to the following information:

*Table 27 - Chassis Manager Information*

<table>
<thead>
<tr>
<th>Accessible Parameters</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>switch temperatures</td>
<td>Displays system’s temperature</td>
</tr>
<tr>
<td>power supply voltages</td>
<td>Displays power supplies’ voltage levels</td>
</tr>
<tr>
<td>fan unit</td>
<td>Displays system fans’ status</td>
</tr>
<tr>
<td>power unit</td>
<td>Displays system power consumers</td>
</tr>
<tr>
<td>Flash memory</td>
<td>Displays information about system memory utilization.</td>
</tr>
</tbody>
</table>

Additionally, it monitors:
- AC power to the PSUs
- DC power out from the PSUs
- Chassis failures

### 4.13.1 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

### 4.13.1.1 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.
### 4.13.1.2 System Health Monitor Alerts Scenarios

- System Health Monitor sends notification alerts in the following cases:

**Table 28 - System Health Monitor Alerts Scenarios** (Sheet 1 of 7)

<table>
<thead>
<tr>
<th>Alert Message</th>
<th>Scenario</th>
<th>Notification Indicator</th>
<th>Recovery Action</th>
<th>Recovery Message</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;fan_name&gt;</code> speed is below minimal range</td>
<td>A chassis fan speed is below minimal threshold: 15% of maximum speed</td>
<td>Email, fan LED and system status LED set red, log alert, SNMP.</td>
<td>Check the fan and replace it if required</td>
<td>“&lt;fan_name&gt; has been restored to its normal state”</td>
</tr>
<tr>
<td>Fan <code>&lt;fan_number&gt;</code> speed in spine number <code>&lt;spine_number&gt;</code> is below minimal range</td>
<td>A spine fan speed is below minimal threshold: 30% of maximum speed</td>
<td>Email, fan LED and system status LED set red, log alert, SNMP</td>
<td>Check the fan and replace it if required</td>
<td>“Fan speed <code>&lt;fan_number&gt;</code> in spine number <code>&lt;spine_number&gt;</code> has been restored to its normal state”</td>
</tr>
<tr>
<td><code>&lt;fan_name&gt;</code> is unresponsive</td>
<td>A chassis fan is not responsive on MLNX-OS systems</td>
<td>Email, fan LED and system status LED set red, log alert, SNMP</td>
<td>Check fan connectivity and replace it if required</td>
<td>“&lt;fan_name&gt; has been restored to its normal state”</td>
</tr>
<tr>
<td>Fan <code>&lt;fan_number&gt;</code> in spine number <code>&lt;spine_number&gt;</code> is unresponsive</td>
<td>A spine fan is not responsive on MLNX-OS systems</td>
<td>Email, fan LED and system status LED set red, log alert, SNMP</td>
<td>Check fan connectivity and replace it if required</td>
<td>“Fan <code>&lt;fan_number&gt;</code> in spine number <code>&lt;spine_number&gt;</code> has been restored to its normal state”</td>
</tr>
<tr>
<td><code>&lt;fan_name&gt;</code> is not present</td>
<td>A chassis fan is missing</td>
<td>Email, fan LED and system status LED set red, log alert, SNMP</td>
<td>Insert a fan unit</td>
<td>“&lt;fan_name&gt; has been restored to its normal state”</td>
</tr>
<tr>
<td>Fan <code>&lt;fan_number&gt;</code> in spine number <code>&lt;spine_number&gt;</code> is not present.</td>
<td>A spine fan is missing</td>
<td>Email, fan LED and system status LED set red, log alert, SNMP</td>
<td>Insert a fan unit</td>
<td>“Fan <code>&lt;fan_number&gt;</code> in spine number <code>&lt;spine_number&gt;</code> has been restored to its normal state”</td>
</tr>
<tr>
<td>Insufficient number of working fans in the system</td>
<td>Insufficient number of working fans in the system</td>
<td>Email, fan LED and system status LED set red, log alert, SNMP</td>
<td>Plug in additional fans or change faulty fans</td>
<td>“The system currently has sufficient number of working fans”</td>
</tr>
<tr>
<td>Alert Message</td>
<td>Scenario</td>
<td>Notification Indicator</td>
<td>Recovery Action</td>
<td>Recovery Message</td>
</tr>
<tr>
<td>---------------------------------------------------</td>
<td>--------------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------------------------</td>
<td>---------------------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Power Supply <code>&lt;ps_number&gt;</code> voltage is out of range</td>
<td>The power supply voltage is out of range.</td>
<td>Email, power supply LED and system status LED set red, log alert, SNMP</td>
<td>Check the power connection of the PS</td>
<td>“Power Supply <code>&lt;ps_number&gt;</code> voltage is in range”</td>
</tr>
<tr>
<td>Power supply <code>&lt;ps_number&gt;</code> temperature is too hot</td>
<td>A power supply unit temperature is higher than the maximum threshold of 70 Celsius on MLNX-OS systems</td>
<td>Email, power supply LED and system status LED set red, log alert, SNMP</td>
<td>Check chassis fans connections. On MLNX-OS systems, check system fan connections.</td>
<td>“Power supply <code>&lt;ps_number&gt;</code> temperature is back to normal”</td>
</tr>
<tr>
<td>Power Supply <code>&lt;number&gt;</code> is unresponsive</td>
<td>A power supply is malfunctioning or disconnected</td>
<td>Email, system status LED set red, log alert, SNMP</td>
<td>Connect power cable or replace malfunctioning PS</td>
<td>“Power supply has been removed” or “PS has been restored to its normal state”</td>
</tr>
<tr>
<td>Unit/leaf/spine <code>&lt;leaf/spine number&gt;</code> is unresponsive</td>
<td>A leaf/spine is not responsive</td>
<td>Email, system status LED set red, log alert, SNMP</td>
<td>Check leaf/spine connectivity and replace it if required</td>
<td>“Leaf/spine number <code>&lt;leaf/spine number&gt;</code> has been restored to its normal state”</td>
</tr>
<tr>
<td>Unit/leaf/spine voltage is out of range</td>
<td>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</td>
<td>Email, system status LED set red, log alert, SNMP</td>
<td>Check leaf connectivity</td>
<td>“Unit voltage is in range”</td>
</tr>
<tr>
<td>ASIC temperature is too hot</td>
<td>A SwitchX unit temperature is higher than the maximum threshold of 105 Celsius on MLNX-OS systems</td>
<td>Email, system status LED set red, log alert, SNMP</td>
<td>Check the fans system</td>
<td>“SwitchX temperature is back to normal”</td>
</tr>
<tr>
<td>Alert Message</td>
<td>Scenario</td>
<td>Notification Indicator</td>
<td>Recovery Action</td>
<td>Recovery Message</td>
</tr>
<tr>
<td>---------------</td>
<td>----------</td>
<td>------------------------</td>
<td>-----------------</td>
<td>------------------</td>
</tr>
<tr>
<td>“BBU&lt;num&gt; active alarms: Under-temperature during discharge (UTD)”</td>
<td>Under-temperature during discharge</td>
<td>Email, system status LED set red, log alert, SNMP</td>
<td>Check ambient temperature. Replace BBU if the problem persist.</td>
<td>“Module BBU&lt;num&gt; has been restored to its normal state”</td>
</tr>
<tr>
<td>“BBU&lt;num&gt; active alarms: Under-temperature during charge (UTC)”</td>
<td>Under-temperature during charge</td>
<td>Email, system status LED set red, log alert, SNMP</td>
<td>Check ambient temperature. Replace BBU if the problem persist.</td>
<td>“Module BBU&lt;num&gt; has been restored to its normal state”</td>
</tr>
<tr>
<td>“BBU&lt;num&gt; active alarms: Over pre-charge current (PCHGC)”</td>
<td>Over pre-charge current</td>
<td>Email, system status LED set red, log alert, SNMP</td>
<td>Replace BBU if the problem persists.</td>
<td>“Module BBU&lt;num&gt; has been restored to its normal state”</td>
</tr>
<tr>
<td>“BBU&lt;num&gt; active alarms: Overcharging voltage (CHGV)”</td>
<td>Overcharging voltage</td>
<td>Email, system status LED set red, log alert, SNMP</td>
<td>Replace BBU if the problem persists.</td>
<td>“Module BBU&lt;num&gt; has been restored to its normal state”</td>
</tr>
<tr>
<td>“BBU&lt;num&gt; active alarms: Overcharging current (CHGC)”</td>
<td>Overcharging current</td>
<td>Email, system status LED set red, log alert, SNMP</td>
<td>Replace BBU if the problem persists.</td>
<td>“Module BBU&lt;num&gt; has been restored to its normal state”</td>
</tr>
<tr>
<td>“BBU&lt;num&gt; active alarms: Overcharge (OC)”</td>
<td>Overcharged BBU</td>
<td>Email, system status LED set red, log alert, SNMP</td>
<td>Replace BBU if the problem persists.</td>
<td>“Module BBU&lt;num&gt; has been restored to its normal state”</td>
</tr>
<tr>
<td>“BBU&lt;num&gt; active alarms: Charge timeout suspend (CTOS)”</td>
<td>Charge timeout suspend</td>
<td>Email, system status LED set red, log alert, SNMP</td>
<td>N/A</td>
<td>“Module BBU&lt;num&gt; has been restored to its normal state”</td>
</tr>
</tbody>
</table>
### Table 28 - System Health Monitor Alerts Scenarios (Sheet 4 of 7)

<table>
<thead>
<tr>
<th>Alert Message</th>
<th>Scenario</th>
<th>Notification Indicator</th>
<th>Recovery Action</th>
<th>Recovery Message</th>
</tr>
</thead>
<tbody>
<tr>
<td>“BBU&lt;num&gt; active alarms: Charge timeout (CTO)”</td>
<td>Charge timeout</td>
<td>Email, system status LED set red, log alert, SNMP</td>
<td>N/A</td>
<td>“Module BBU&lt;num&gt; has been restored to its normal state”</td>
</tr>
<tr>
<td>“BBU&lt;num&gt; active alarms: Pre-charge timeout suspend (PTOS)”</td>
<td>Pre-charge timeout suspend</td>
<td>Email, system status LED set red, log alert, SNMP</td>
<td>N/A</td>
<td>“Module BBU&lt;num&gt; has been restored to its normal state”</td>
</tr>
<tr>
<td>“BBU&lt;num&gt; active alarms: Pre-charge timeout (PTO)”</td>
<td>Pre-charge timeout</td>
<td>Email, system status LED set red, log alert, SNMP</td>
<td>N/A</td>
<td>“Module BBU&lt;num&gt; has been restored to its normal state”</td>
</tr>
<tr>
<td>“BBU&lt;num&gt; active alarms: Over-temperature FET (OTF)”</td>
<td>Over-temperature FET</td>
<td>Email, system status LED set red, log alert, SNMP</td>
<td>N/A</td>
<td>“Module BBU&lt;num&gt; has been restored to its normal state”</td>
</tr>
<tr>
<td>“BBU&lt;num&gt; active alarms: Cell under-voltage compensated (CUVC)”</td>
<td>Cell under-voltage compensated</td>
<td>Email, system status LED set red, log alert, SNMP</td>
<td>Replace BBU if the problem persists.</td>
<td>“Module BBU&lt;num&gt; has been restored to its normal state”</td>
</tr>
<tr>
<td>“BBU&lt;num&gt; active alarms: Over-temperature during discharge (OTD)”</td>
<td>Over-temperature during discharge</td>
<td>Email, system status LED set red, log alert, SNMP</td>
<td>Replace BBU if the problem persists.</td>
<td>“Module BBU&lt;num&gt; has been restored to its normal state”</td>
</tr>
<tr>
<td>“BBU&lt;num&gt; active alarms: Over-temperature during charge (OTC)”</td>
<td>Over-temperature during charge</td>
<td>Email, system status LED set red, log alert, SNMP</td>
<td>Check ambient temperature. Replace BBU if the problem persists.</td>
<td>“Module BBU&lt;num&gt; has been restored to its normal state”</td>
</tr>
</tbody>
</table>
Table 28 - System Health Monitor Alerts Scenarios (Sheet 5 of 7)

<table>
<thead>
<tr>
<th>Alert Message</th>
<th>Scenario</th>
<th>Notification Indicator</th>
<th>Recovery Action</th>
<th>Recovery Message</th>
</tr>
</thead>
<tbody>
<tr>
<td>“BBU&lt;num&gt; active alarms: Short-circuit during discharge latch (ASCDL)”</td>
<td>Short-circuit during discharge latch</td>
<td>Email, system status LED set red, log alert, SNMP</td>
<td>Replace BBU</td>
<td>N/A</td>
</tr>
<tr>
<td>“BBU&lt;num&gt; active alarms: Short-circuit during discharge (ASCL)”</td>
<td>Short-circuit during discharge</td>
<td>Email, system status LED set red, log alert, SNMP</td>
<td>Replace BBU if the problem persists.</td>
<td>“Module BBU&lt;num&gt; has been restored to its normal state”</td>
</tr>
<tr>
<td>“BBU&lt;num&gt; active alarms: Short-circuit during charge latch (ASCCL)”</td>
<td>Short-circuit during charge latch</td>
<td>Email, system status LED set red, log alert, SNMP</td>
<td>Replace BBU</td>
<td>N/A</td>
</tr>
<tr>
<td>“BBU&lt;num&gt; active alarms: Short-circuit during charge (ASCC)”</td>
<td>Short-circuit during charge</td>
<td>Email, system status LED set red, log alert, SNMP</td>
<td>Replace BBU if the problem persists.</td>
<td>“Module BBU&lt;num&gt; has been restored to its normal state”</td>
</tr>
<tr>
<td>“BBU&lt;num&gt; active alarms: Overload during discharge latch (AOLDL)”</td>
<td>Overload during discharge latch</td>
<td>Email, system status LED set red, log alert, SNMP</td>
<td>Replace BBU</td>
<td>N/A</td>
</tr>
<tr>
<td>“BBU&lt;num&gt; active alarms: Overload during discharge (AOLD)”</td>
<td>Overload during discharge</td>
<td>Email, system status LED set red, log alert, SNMP</td>
<td>Replace BBU if the problem persists.</td>
<td>“Module BBU&lt;num&gt; has been restored to its normal state”</td>
</tr>
<tr>
<td>“BBU&lt;num&gt; active alarms: Over-current during discharge 1 (OCD1)”</td>
<td>Over-current during discharge</td>
<td>Email, system status LED set red, log alert, SNMP</td>
<td>Replace BBU if the problem persists.</td>
<td>“Module BBU&lt;num&gt; has been restored to its normal state”</td>
</tr>
<tr>
<td>Alert Message</td>
<td>Scenario</td>
<td>Notification Indicator</td>
<td>Recovery Action</td>
<td>Recovery Message</td>
</tr>
<tr>
<td>------------------------------------------------------------------------------</td>
<td>-------------------------------</td>
<td>----------------------------------------------</td>
<td>----------------------------------------</td>
<td>----------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>“BBU&lt;num&gt; active alarms: Over-current during discharge 2 (OCD2)”</td>
<td>Over-current during discharge</td>
<td>Email, system status LED set red, log alert, SNMP</td>
<td>Replace BBU if the problem persists.</td>
<td>“Module BBU&lt;num&gt; has been restored to its normal state”</td>
</tr>
<tr>
<td>“BBU&lt;num&gt; active alarms: Over-current during charge 1 (OCC1)”</td>
<td>Over-current during charge</td>
<td>Email, system status LED set red, log alert, SNMP</td>
<td>Replace BBU if the problem persists.</td>
<td>“Module BBU&lt;num&gt; has been restored to its normal state”</td>
</tr>
<tr>
<td>“BBU&lt;num&gt; active alarms: Over-current during charge 2 (OCC2)”</td>
<td>Over-current during charge</td>
<td>Email, system status LED set red, log alert, SNMP</td>
<td>Replace BBU if the problem persists.</td>
<td>“Module BBU&lt;num&gt; has been restored to its normal state”</td>
</tr>
<tr>
<td>“BBU&lt;num&gt; active alarms: Cell over-voltage (COV)”</td>
<td>Cell over-voltage</td>
<td>Email, system status LED set red, log alert, SNMP</td>
<td>Replace BBU if the problem persists.</td>
<td>“Module BBU&lt;num&gt; has been restored to its normal state”</td>
</tr>
<tr>
<td>“BBU&lt;num&gt; active alarms: Cell under-voltage (CUV)”</td>
<td>Cell under-voltage</td>
<td>Email, system status LED set red, log alert, SNMP</td>
<td>Replace BBU if the problem persists.</td>
<td>“Module BBU&lt;num&gt; has been restored to its normal state”</td>
</tr>
<tr>
<td>“Module BBU&lt;num&gt; voltage is out of range”</td>
<td>Cell over-voltage</td>
<td>Email, system status LED set red, log alert, SNMP</td>
<td>Replace BBU if the problem persists.</td>
<td>“Module BBU&lt;num&gt; voltage is back in range”</td>
</tr>
<tr>
<td>“Module BBU&lt;num&gt; current is too high”</td>
<td>Over-current during charge</td>
<td>Email, system status LED set red, log alert, SNMP</td>
<td>Replace BBU if the problem persists.</td>
<td>“BBU&lt;num&gt; has been restored to its normal state”</td>
</tr>
</tbody>
</table>
4.13.2 Power Management

4.13.2.1 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.

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

When “show interfaces” is used, a port’s speed appears unchanged even when only one lane is active.
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 463.

Table 29 - LWR Configuration Behavior

<table>
<thead>
<tr>
<th>Switch-A Configuration</th>
<th>Switch-B Configuration</th>
<th>Behavior</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disable</td>
<td>Disable</td>
<td>LWR is disabled.</td>
</tr>
<tr>
<td>Disable</td>
<td>Force</td>
<td>Transmission from Switch-B to Switch-A operates at 1X. On the opposite direction, LWR is disabled.</td>
</tr>
<tr>
<td>Disable</td>
<td>Auto</td>
<td>Depending on traffic flow, transmission from Switch-B to Switch-A may operate at 1X. On the opposite direction, LWR is disabled.</td>
</tr>
<tr>
<td>Auto</td>
<td>Force</td>
<td>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.</td>
</tr>
<tr>
<td>Auto</td>
<td>Auto</td>
<td>Width of the connection depends on the traffic flow</td>
</tr>
<tr>
<td>Force</td>
<td>Force</td>
<td>Connection between the switches operates at 1X</td>
</tr>
</tbody>
</table>
4.13.3 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:

```plaintext
switch (config) # show voltage
```

<table>
<thead>
<tr>
<th>Module</th>
<th>Power Meter</th>
<th>Reg</th>
<th>Expected</th>
<th>Actual</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>PS2</td>
<td>PS_MONITOR</td>
<td>V1</td>
<td>48.00</td>
<td>46.88</td>
<td>OK</td>
</tr>
<tr>
<td>PS3</td>
<td>PS_MONITOR</td>
<td>V1</td>
<td>48.00</td>
<td>48.29</td>
<td>OK</td>
</tr>
<tr>
<td>PS4</td>
<td>PS_MONITOR</td>
<td>V1</td>
<td>48.00</td>
<td>48.29</td>
<td>OK</td>
</tr>
<tr>
<td>MGMT</td>
<td>CPU_BOARD_MONITOR</td>
<td>V1</td>
<td>12.00</td>
<td>11.92</td>
<td>OK</td>
</tr>
<tr>
<td>MGMT</td>
<td>CPU_BOARD_MONITOR</td>
<td>V2</td>
<td>2.50</td>
<td>2.48</td>
<td>OK</td>
</tr>
<tr>
<td>MGMT</td>
<td>CPU_BOARD_MONITOR</td>
<td>V3</td>
<td>3.30</td>
<td>3.31</td>
<td>OK</td>
</tr>
<tr>
<td>MGMT</td>
<td>CPU_BOARD_MONITOR</td>
<td>V4</td>
<td>3.30</td>
<td>3.30</td>
<td>OK</td>
</tr>
<tr>
<td>MGMT</td>
<td>CPU_BOARD_MONITOR</td>
<td>V5</td>
<td>1.80</td>
<td>1.81</td>
<td>OK</td>
</tr>
<tr>
<td>MGMT</td>
<td>CPU_BOARD_MONITOR</td>
<td>V6</td>
<td>1.20</td>
<td>1.26</td>
<td>OK</td>
</tr>
<tr>
<td>S01</td>
<td>BOARD_MONITOR</td>
<td>V1</td>
<td>3.30</td>
<td>3.33</td>
<td>OK</td>
</tr>
<tr>
<td>S01</td>
<td>BOARD_MONITOR</td>
<td>V2</td>
<td>2.27</td>
<td>2.15</td>
<td>OK</td>
</tr>
<tr>
<td>S01</td>
<td>BOARD_MONITOR</td>
<td>V3</td>
<td>1.80</td>
<td>1.76</td>
<td>OK</td>
</tr>
<tr>
<td>S01</td>
<td>BOARD_MONITOR</td>
<td>V4</td>
<td>3.30</td>
<td>3.30</td>
<td>OK</td>
</tr>
<tr>
<td>S01</td>
<td>BOARD_MONITOR</td>
<td>V5</td>
<td>0.90</td>
<td>0.93</td>
<td>OK</td>
</tr>
<tr>
<td>S01</td>
<td>BOARD_MONITOR</td>
<td>V6</td>
<td>1.20</td>
<td>1.19</td>
<td>OK</td>
</tr>
<tr>
<td>S02</td>
<td>BOARD_MONITOR</td>
<td>V1</td>
<td>3.30</td>
<td>3.26</td>
<td>OK</td>
</tr>
<tr>
<td>S02</td>
<td>BOARD_MONITOR</td>
<td>V2</td>
<td>2.27</td>
<td>2.16</td>
<td>OK</td>
</tr>
<tr>
<td>S02</td>
<td>BOARD_MONITOR</td>
<td>V3</td>
<td>1.80</td>
<td>1.79</td>
<td>OK</td>
</tr>
<tr>
<td>S02</td>
<td>BOARD_MONITOR</td>
<td>V4</td>
<td>3.30</td>
<td>3.31</td>
<td>OK</td>
</tr>
<tr>
<td>S02</td>
<td>BOARD_MONITOR</td>
<td>V5</td>
<td>0.90</td>
<td>0.95</td>
<td>OK</td>
</tr>
<tr>
<td>S02</td>
<td>BOARD_MONITOR</td>
<td>V6</td>
<td>1.20</td>
<td>1.20</td>
<td>OK</td>
</tr>
<tr>
<td>L01</td>
<td>BOARD_MONITOR</td>
<td>V1</td>
<td>3.30</td>
<td>3.33</td>
<td>OK</td>
</tr>
<tr>
<td>L01</td>
<td>BOARD_MONITOR</td>
<td>V2</td>
<td>2.27</td>
<td>2.16</td>
<td>OK</td>
</tr>
<tr>
<td>L01</td>
<td>BOARD_MONITOR</td>
<td>V3</td>
<td>1.80</td>
<td>1.76</td>
<td>OK</td>
</tr>
<tr>
<td>L01</td>
<td>BOARD_MONITOR</td>
<td>V4</td>
<td>3.30</td>
<td>3.30</td>
<td>OK</td>
</tr>
<tr>
<td>L01</td>
<td>BOARD_MONITOR</td>
<td>V5</td>
<td>0.90</td>
<td>0.93</td>
<td>OK</td>
</tr>
<tr>
<td>L01</td>
<td>BOARD_MONITOR</td>
<td>V6</td>
<td>1.20</td>
<td>1.19</td>
<td>OK</td>
</tr>
<tr>
<td>L02</td>
<td>BOARD_MONITOR</td>
<td>V1</td>
<td>3.30</td>
<td>3.26</td>
<td>OK</td>
</tr>
<tr>
<td>L02</td>
<td>BOARD_MONITOR</td>
<td>V2</td>
<td>2.27</td>
<td>2.17</td>
<td>OK</td>
</tr>
<tr>
<td>L02</td>
<td>BOARD_MONITOR</td>
<td>V3</td>
<td>1.80</td>
<td>1.79</td>
<td>OK</td>
</tr>
<tr>
<td>L02</td>
<td>BOARD_MONITOR</td>
<td>V4</td>
<td>3.30</td>
<td>3.30</td>
<td>OK</td>
</tr>
<tr>
<td>L02</td>
<td>BOARD_MONITOR</td>
<td>V5</td>
<td>0.90</td>
<td>0.89</td>
<td>OK</td>
</tr>
<tr>
<td>L02</td>
<td>BOARD_MONITOR</td>
<td>V6</td>
<td>1.20</td>
<td>1.19</td>
<td>OK</td>
</tr>
</tbody>
</table>

switch (config) #
Step 3. Display the fan speed and status. Run:

```plaintext
switch (config) # show fan
```

<table>
<thead>
<tr>
<th>Module</th>
<th>Device</th>
<th>Fan Speed</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>FAN1</td>
<td>FAN</td>
<td>6994.00</td>
<td>OK</td>
</tr>
<tr>
<td>FAN2</td>
<td>FAN</td>
<td>6792.00</td>
<td>OK</td>
</tr>
<tr>
<td>FAN3</td>
<td>FAN</td>
<td>6870.00</td>
<td>OK</td>
</tr>
<tr>
<td>FAN4</td>
<td>FAN</td>
<td>6818.00</td>
<td>OK</td>
</tr>
<tr>
<td>S01</td>
<td>FAN</td>
<td>7800.00</td>
<td>OK</td>
</tr>
<tr>
<td>S01</td>
<td>FAN</td>
<td>8130.00</td>
<td>OK</td>
</tr>
<tr>
<td>S02</td>
<td>FAN</td>
<td>8130.00</td>
<td>OK</td>
</tr>
<tr>
<td>S02</td>
<td>FAN</td>
<td>8490.00</td>
<td>OK</td>
</tr>
<tr>
<td>S03</td>
<td>FAN</td>
<td>-</td>
<td>NOT PRESENT</td>
</tr>
<tr>
<td>S04</td>
<td>FAN</td>
<td>-</td>
<td>NOT PRESENT</td>
</tr>
<tr>
<td>S05</td>
<td>FAN</td>
<td>-</td>
<td>NOT PRESENT</td>
</tr>
<tr>
<td>S06</td>
<td>FAN</td>
<td>-</td>
<td>NOT PRESENT</td>
</tr>
</tbody>
</table>

```plaintext
switch (config) #
```

Step 4. Display the voltage current and status of each module in the system. Run:

```plaintext
switch (config) # show power consumers
```

<table>
<thead>
<tr>
<th>Module</th>
<th>Power (Watts)</th>
<th>Voltage (Amp)</th>
<th>Current (Amp)</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>FAN1</td>
<td>15.55</td>
<td>48.00</td>
<td>0.32</td>
<td>OK</td>
</tr>
<tr>
<td>FAN2</td>
<td>16.26</td>
<td>48.00</td>
<td>0.34</td>
<td>OK</td>
</tr>
<tr>
<td>FAN3</td>
<td>15.30</td>
<td>48.00</td>
<td>0.32</td>
<td>OK</td>
</tr>
<tr>
<td>FAN4</td>
<td>14.98</td>
<td>48.00</td>
<td>0.31</td>
<td>OK</td>
</tr>
<tr>
<td>L01</td>
<td>32.45</td>
<td>48.00</td>
<td>0.68</td>
<td>OK</td>
</tr>
<tr>
<td>L02</td>
<td>28.75</td>
<td>48.00</td>
<td>0.60</td>
<td>OK</td>
</tr>
<tr>
<td>MGMT</td>
<td>16.08</td>
<td>48.00</td>
<td>0.34</td>
<td>OK</td>
</tr>
<tr>
<td>S01</td>
<td>37.34</td>
<td>48.00</td>
<td>0.78</td>
<td>OK</td>
</tr>
<tr>
<td>S02</td>
<td>35.09</td>
<td>48.00</td>
<td>0.73</td>
<td>OK</td>
</tr>
</tbody>
</table>

Total power used : 211.79 W
Max power : 686.00 W

```plaintext
switch (config) #
```

4.13.4 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:

```plaintext
scp://username:password@hostname/var/mnt/usb1/<file name>
```

While username and password are the admin username and password and hostname is the IP of the switch.
Examples:

- To fetch an image from a USB device, run the command:
  
  ```
  switch (config) # "image fetch scp://admin:admin@127.0.0.1/var/mnt/usb1/image.img
  ```

- To save log file ‘my-logfile’ to a USB device under the name test_logfile using the logging files command, run (in Enable or Config mode):
  
  ```
  switch (config) # logging files upload my-logfile scp://username:password@hostname/var/mnt/usb1/test_logfile
  ```

- To safely remove the USB and to flush the cache, after writing (log files, for example) to a USB, use the usb eject command (in Enable or Config mode).
  
  ```
  switch (config) # usb eject
  ```

4.13.5 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
  --- MGMT UID Blue
  ```

- To deactivate the UID LED on a switch system, run:

  ```
  switch (config) # led MGMT uid off
  ```

4.13.6 System Reboot

4.13.6.1 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
  ```
4.13.7 Commands

4.13.7.1 Chassis Management

clear counters

clear counters [all | interface <type> <number>]

Clears switch counters.

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>all</td>
<td>Clears all switch counters.</td>
</tr>
<tr>
<td>type</td>
<td>A specific interface type</td>
</tr>
<tr>
<td>number</td>
<td>The interface number.</td>
</tr>
</tbody>
</table>

**Default**

N/A

**Configuration Mode**

Config Interface Port Channel

**History**

3.2.3000

**Role**

admin

**Example**

switch (config) # clear counters

**Related Commands**

**Notes**
health

```plaintext
health {max-report-len <length> | re-notif-cntr <counter> | report-clear}
```

Configures health daemon settings.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>max-report-len &lt;length&gt;</code></td>
<td>Sets the length of the health report - number of line entries. Range: 10-2048.</td>
</tr>
<tr>
<td><code>re-notif-cntr &lt;counter&gt;</code></td>
<td>Health control changes notification counter, in seconds. Range: 120-7200 seconds.</td>
</tr>
<tr>
<td><code>report-clear</code></td>
<td>Clears the health report.</td>
</tr>
</tbody>
</table>

**Default**
- `max-report-len: 50`
- `re-notif-cntr:`

**Configuration Mode**
- Config

**History**
- 3.1.0000

**Role**
- admin

**Example**

```plaintext
switch (config) # health re-notif-cntr 125
switch (config) #
```

**Related Commands**
- `show health-report`

**Notes**
**led uid**

`led <module> uid <on | off>`

Configures the UID LED.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>module</td>
<td>Specifies the module whose UID LED to configure</td>
</tr>
<tr>
<td>on</td>
<td>Turns on UID LED</td>
</tr>
<tr>
<td>off</td>
<td>Turns off UID LED</td>
</tr>
</tbody>
</table>

**Default**

N/A

**Configuration Mode**

Config

**History**

3.6.1002

**Role**

admin

**Example**

```
switch (config) # led MGMT uid on
switch (config) #
```

**Related Commands**

N/A

**Notes**

•
power-management width

```
power-management width {auto | force}
no power-management width
```

Sets the width of the interface to be automatically adjusted. The no form of the command disables power-saving.

### Syntax Description

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>auto</th>
<th>force</th>
</tr>
</thead>
<tbody>
<tr>
<td>auto</td>
<td>Allows the system to automatically decide whether to work in power-saving mode or not.</td>
<td></td>
</tr>
<tr>
<td>force</td>
<td>Forces power-saving mode on the port.</td>
<td></td>
</tr>
</tbody>
</table>

### Default

Disabled

### Configuration Mode

Config Interface Ethernet

### History

3.3.4000

### Role

admin

### Example

```
switch (config interface ib 1/1) # power-management width auto
switch (config) #
```

### Related Commands

show interface

### Notes
### usb eject

**Description**: Gracefully turns off the USB interface.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>N/A</td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Config</td>
</tr>
<tr>
<td>History</td>
<td>3.1.0000</td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
</tr>
</tbody>
</table>
| Example             | switch (config) # usb eject
|                     | switch (config) # |
| Related Commands    | N/A        |
| Notes               | Applicable only for systems with USB interface. |
show asic-version

show asic-version

Displays firmware ASIC version.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>N/A</td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Any Command Mode</td>
</tr>
<tr>
<td>History</td>
<td>3.1.0000</td>
</tr>
<tr>
<td></td>
<td>3.4.2008</td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
</tr>
<tr>
<td>Example</td>
<td>switch (config) # show asic-version</td>
</tr>
<tr>
<td></td>
<td>Module</td>
</tr>
<tr>
<td></td>
<td>MGMT</td>
</tr>
</tbody>
</table>

Related Commands: N/A

Notes
**show bios**

**show bios**

Displays the bios version information.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>N/A</td>
</tr>
<tr>
<td><strong>Configuration Mode</strong></td>
<td>Any Command Mode</td>
</tr>
<tr>
<td><strong>History</strong></td>
<td>3.3.4150</td>
</tr>
<tr>
<td><strong>Role</strong></td>
<td>admin</td>
</tr>
</tbody>
</table>
| **Example** | switch (config) # show bios  
BIOS version : 4.6.5  
BIOS subversion : Official AMI Release  
BIOS release date : 07/02/2013  
switch (config) # |

**Related Commands**

**Notes** The command is available only on x86 systems
### show cpld

**Syntax Description**: Displays status of all CPLDs in the system.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>N/A</td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Any Command Mode</td>
</tr>
<tr>
<td>History</td>
<td>3.1.0000</td>
</tr>
<tr>
<td></td>
<td>3.3.4302</td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
</tr>
</tbody>
</table>

#### Example

```
switch (config) # show cpld

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cpld1</td>
<td>CPLD_TOR</td>
<td>4</td>
</tr>
<tr>
<td>Cpld2</td>
<td>CPLD_PORT1</td>
<td>2</td>
</tr>
<tr>
<td>Cpld3</td>
<td>CPLD_PORT2</td>
<td>2</td>
</tr>
<tr>
<td>Cpld4</td>
<td>CPLD_MEZZ</td>
<td>3</td>
</tr>
</tbody>
</table>

switch (config) #
```

### Related Commands

<table>
<thead>
<tr>
<th>N/A</th>
</tr>
</thead>
</table>

### Notes

<table>
<thead>
<tr>
<th>N/A</th>
</tr>
</thead>
</table>
## show fan

**Description**

Displays fans status.

### Syntax Description

| Syntax Description | N/A |

### Default

| Default | N/A |

### Configuration Mode

| Configuration Mode | Any Command Mode |

### History

| History | 3.1.0000 |

### Role

| Role | admin |

### Example

```
switch (config) # show fan
switch (config) # show fan
```

<table>
<thead>
<tr>
<th>Module</th>
<th>Device</th>
<th>Fan</th>
<th>Speed (RPM)</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>FAN</td>
<td>FAN</td>
<td>F1</td>
<td>5340.00</td>
<td>OK</td>
</tr>
<tr>
<td>FAN</td>
<td>FAN</td>
<td>F2</td>
<td>5340.00</td>
<td>OK</td>
</tr>
<tr>
<td>FAN</td>
<td>FAN</td>
<td>F3</td>
<td>5640.00</td>
<td>OK</td>
</tr>
<tr>
<td>FAN</td>
<td>FAN</td>
<td>F4</td>
<td>5640.00</td>
<td>OK</td>
</tr>
<tr>
<td>PS1</td>
<td>FAN</td>
<td>F1</td>
<td>5730.00</td>
<td>OK</td>
</tr>
<tr>
<td>PS2</td>
<td>FAN</td>
<td></td>
<td></td>
<td>NOT PRESENT</td>
</tr>
</tbody>
</table>

```
switch (config) #
```

### Related Commands

| Related Commands | N/A |

### Notes

| Notes |

---
# show health-report

**show health-report**

Displays health report.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>N/A</td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Any Command Mode</td>
</tr>
<tr>
<td>History</td>
<td>3.1.0000 First version</td>
</tr>
<tr>
<td></td>
<td>3.3.0000 Output update</td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
</tr>
</tbody>
</table>
| Example            | switch (config) # show health-report  
|                    | | ALERTS CONFIGURATION |  
|                    | | Re-notification counter (sec): [3600] |
|                    | | Report max counter: | [50] |
|                    | | | HEALTH REPORT |
|                    | No Health issues file |
|                    | switch (config) # |
| Related Commands   | N/A |
| Notes              | Problems with the power supply cannot be monitored on SX1016 switch systems. |
**show inventory**

Displays system inventory.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>N/A</td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Any Command Mode</td>
</tr>
</tbody>
</table>
| History            | 3.1.0000
|                    | 3.4.1604 | Removed CPU module output from Example |
|                    | 3.5.1000 | Removed Type column from Example |
|                    | 3.6.1002 | Updated output |
| Role               | admin |

**Example**

```
switch (config) # show inventory

<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>
```

switch (config) #

**Related Commands**

N/A

**Notes**
show leds

show leds [<module>]

Displays the LED status of the switch system.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>module</th>
<th>Specifies the module whose LED status to display</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>N/A</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Configuration Mode</th>
<th>Config</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>History</th>
<th>3.6.1002</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>3.6.2002</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Role</th>
<th>admin</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Example</th>
<th>switch (config) # show leds</th>
</tr>
</thead>
<tbody>
<tr>
<td>Module</td>
<td>LED</td>
</tr>
<tr>
<td>---------------------</td>
<td>------------------------------</td>
</tr>
<tr>
<td>MGMT</td>
<td>STATUS</td>
</tr>
<tr>
<td>MGMT</td>
<td>FAN1</td>
</tr>
<tr>
<td>MGMT</td>
<td>FAN2</td>
</tr>
<tr>
<td>MGMT</td>
<td>FAN3</td>
</tr>
<tr>
<td>MGMT</td>
<td>FAN4</td>
</tr>
<tr>
<td>MGMT</td>
<td>PS_STATUS</td>
</tr>
<tr>
<td>MGMT</td>
<td>PS1</td>
</tr>
<tr>
<td>MGMT</td>
<td>PS2</td>
</tr>
<tr>
<td>MGMT</td>
<td>UID</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Related Commands</th>
<th>N/A</th>
</tr>
</thead>
</table>

| Notes                |      |
show memory

show memory
Displays memory status.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>N/A</td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Any Command Mode</td>
</tr>
<tr>
<td>History</td>
<td>3.1.0000</td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
</tr>
</tbody>
</table>

Example

```
switch (config) # show memory
Total     Used     Free     Used+B/C    Free-B/C
Physical  2027 MB  761 MB   1266 MB     1214 MB     813 MB
Swap      0 MB      0 MB     0 MB

Physical Memory Borrowed for System Buffers and Cache:
Buffers:                  0 MB
Cache:                    452 MB
Total Buffers/Cache:      452 MB
```

Related Commands
N/A

Notes
### show module

**show module**

Displays modules status.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>N/A</td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Any Command Mode</td>
</tr>
</tbody>
</table>
| History             | 3.1.0000 First version  
3.3.0000 Added “Is Fatal” column  
3.4.2008 Updated command output  
3.4.3000 Updated command output and added note |
| Role                | admin |
| Example             | switch (config) # show module  
-----------------------  
Module | Status  
-----------------------  
MGMT | ready  
FAN1 | ready  
FAN2 | ready  
PS1 | ready  
PS2 | not-present  
switch (config) # |
| Related Commands    | N/A |
| Notes               | The Status column may have one of the following values: error, fatal, not-present, powered-off, powered-on, ready. |
### show power

**show power**

Displays power supplies and power usage.

<table>
<thead>
<tr>
<th><strong>Syntax Description</strong></th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Default</strong></td>
<td>N/A</td>
</tr>
<tr>
<td><strong>Configuration Mode</strong></td>
<td>Any Command Mode</td>
</tr>
<tr>
<td><strong>History</strong></td>
<td>3.1.0000</td>
</tr>
<tr>
<td></td>
<td>3.5.1000</td>
</tr>
<tr>
<td><strong>Role</strong></td>
<td>admin</td>
</tr>
</tbody>
</table>
| **Example**            | switch (config) # show power

<table>
<thead>
<tr>
<th>Module</th>
<th>Device</th>
<th>Sensor Power</th>
<th>Voltage</th>
<th>Current</th>
<th>Capacity</th>
<th>Feed</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>PS1</td>
<td>power-mon</td>
<td>input</td>
<td>32.25</td>
<td>12.11</td>
<td>1.26</td>
<td>800.00</td>
<td>DC</td>
</tr>
<tr>
<td>PS2</td>
<td>power-mon</td>
<td>input</td>
<td>46.56</td>
<td>12.13</td>
<td>2.33</td>
<td>800.00</td>
<td>DC</td>
</tr>
</tbody>
</table>

**Related Commands**

N/A

**Notes**

N/A
**show power consumers**

Displays power consumption information.

<table>
<thead>
<tr>
<th><strong>Syntax Description</strong></th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Default</strong></td>
<td>N/A</td>
</tr>
<tr>
<td><strong>Configuration Mode</strong></td>
<td>Any Command Mode</td>
</tr>
<tr>
<td><strong>History</strong></td>
<td>3.1.0000</td>
</tr>
<tr>
<td></td>
<td>3.5.1000</td>
</tr>
</tbody>
</table>

**Role**

admin

**Example**

```
switch (config) # show power consumers

+-----------------+--------+--------+--------+-------+
| Module          | Device | Sensor | Power  | Voltage| Current| Status |
|                 |        |        | [Watts]| [Volts]| [Amp]   |        |
| MGMT            | CURR_MONITOR | 12V   | 52.96  | 11.71  | 4.52    | OK     |
```

Total power used : 52.96 Watts

```
switch (config) #
```
### show protocols

**show protocols**

Displays all protocols enabled in the system.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>N/A</td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Any Command Mode</td>
</tr>
<tr>
<td>History</td>
<td>3.2.3000</td>
</tr>
<tr>
<td></td>
<td>3.3.4550 Updated Example</td>
</tr>
<tr>
<td></td>
<td>3.6.1002 Updated Example</td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
</tr>
<tr>
<td>Example</td>
<td>switch (config) # show protocols</td>
</tr>
</tbody>
</table>

**Example**

```
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
```

**Related Commands**

| N/A |

**Notes**

N/A
show resources

Displays system resources.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>N/A</td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Any Command Mode</td>
</tr>
<tr>
<td>History</td>
<td>3.1.0000</td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
</tr>
</tbody>
</table>

**Example**

```plaintext
switch (config) # show resources
Total    Used    Free
Physical  2027 MB  761 MB  1266 MB
Swap      0 MB     0 MB     0 MB

Number of CPUs: 1
CPU load averages: 0.11 / 0.23 / 0.23

CPU 1
  Utilization: 5%
  Peak Utilization Last Hour: 19% at 2012/02/15 13:26:19
  Avg. Utilization Last Hour: 7%

switch (config) #
```

**Related Commands**

N/A

**Notes**

N/A
**show system capabilities**

`show system capabilities`

Displays system capabilities.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>N/A</td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Any Command Mode</td>
</tr>
<tr>
<td>History</td>
<td>3.1.0000 First version</td>
</tr>
<tr>
<td></td>
<td>3.3.0000 Added gateway support</td>
</tr>
<tr>
<td></td>
<td>3.6.1002 Updated output</td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
</tr>
<tr>
<td>Example</td>
<td><code>switch (config) # show system capabilities</code></td>
</tr>
<tr>
<td></td>
<td>Ethernet: Supported, L2, L3</td>
</tr>
<tr>
<td></td>
<td>Ethernet Max licensed speed: 56Gb</td>
</tr>
</tbody>
</table>

**Related Commands**

- `show system profile`

**Notes**
**show system mac**

**show system mac**

Displays system MAC address.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>N/A</td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Any Command Mode</td>
</tr>
<tr>
<td>History</td>
<td>3.1.0000</td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
</tr>
</tbody>
</table>

**Example**

```
switch (config) # show system mac
00:02:C9:5E:AF:18
switch (config) #
```

<table>
<thead>
<tr>
<th>Related Commands</th>
<th>N/A</th>
</tr>
</thead>
</table>

**Notes**
show system profile

show system profile

Displays system profile.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>N/A</td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Any Command Mode</td>
</tr>
<tr>
<td>History</td>
<td>3.2.0000</td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
</tr>
</tbody>
</table>
| Example            | switch (config) # show system profile
|                    | eth-single-switch
|                    | switch (config) # |
| Related Commands   | system profile |
| Notes              |     |
show system type

show system type

Displays system type.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>N/A</td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Any Command Mode</td>
</tr>
<tr>
<td>History</td>
<td>3.5.1000</td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
</tr>
</tbody>
</table>
| Example            | `switch (config) # show system type
SX1036
switch (config) #` |

<table>
<thead>
<tr>
<th>Related Commands</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Notes</th>
</tr>
</thead>
</table>
**show temperature**

**show temperature**

Displays system temperature sensors status.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>N/A</td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Any Command Mode</td>
</tr>
<tr>
<td>History</td>
<td>3.1.0000</td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
</tr>
</tbody>
</table>

**Example**

```
switch (config) # show temperature

<table>
<thead>
<tr>
<th>Module</th>
<th>Component</th>
<th>Reg</th>
<th>CurTemp</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>MGMT</td>
<td>BOARD_MONITOR</td>
<td>T1</td>
<td>25.00</td>
<td>OK</td>
</tr>
<tr>
<td>MGMT</td>
<td>CPU_BOARD_MONITOR</td>
<td>T1</td>
<td>26.00</td>
<td>OK</td>
</tr>
<tr>
<td>MGMT</td>
<td>CPU_BOARD_MONITOR</td>
<td>T2</td>
<td>41.00</td>
<td>OK</td>
</tr>
<tr>
<td>MGMT</td>
<td>QSFP_TEMP1</td>
<td>T1</td>
<td>23.00</td>
<td>OK</td>
</tr>
<tr>
<td>MGMT</td>
<td>QSFP_TEMP2</td>
<td>T1</td>
<td>22.50</td>
<td>OK</td>
</tr>
<tr>
<td>MGMT</td>
<td>QSFP_TEMP3</td>
<td>T1</td>
<td>23.00</td>
<td>OK</td>
</tr>
<tr>
<td>MGMT</td>
<td>SX</td>
<td>T1</td>
<td>37.00</td>
<td>OK</td>
</tr>
</tbody>
</table>
```

**Related Commands**

N/A

**Notes**
### show uboot

**show uboot**

Displays u-boot version.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>N/A</td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Any Command Mode</td>
</tr>
<tr>
<td>History</td>
<td>3.3.5006</td>
</tr>
<tr>
<td></td>
<td>3.4.1110</td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
</tr>
</tbody>
</table>
| Example            | 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) # |
| Related Commands   | N/A |
| Notes              | This command is available only on PPC based systems |
### show version

**show version**

Displays version information for the currently running system image.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>N/A</td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Any Command Mode</td>
</tr>
<tr>
<td>History</td>
<td>3.1.0000</td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
</tr>
</tbody>
</table>

**Example**

```
switch (config) # show version
Product name:      MLNX-OS
Product release:   3.1.0000
Build ID:          #1-dev
Build date:        2012-02-26 08:47:51
Target arch:       ppc
Target hw:         m460ex
Built by:          root@r-fit16
Uptime:            1d 3h 32m 24.656s
Product model:     ppc
Host ID:           0002c911a15e
System memory:     110 MB used / 1917 MB free / 2027 MB total
Swap:              0 MB used / 0 MB free / 0 MB total
Number of CPUs:    1
CPU load averages: 0.18 / 0.19 / 0.16
switch (config) #
```
### show version concise

**show version concise**

Displays concise version information for the currently running system image.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>N/A</td>
</tr>
<tr>
<td><strong>Configuration Mode</strong></td>
<td>Any Command Mode</td>
</tr>
<tr>
<td>History</td>
<td>3.1.0000</td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
</tr>
</tbody>
</table>
| **Example**           | switch (config) # show version concise  
                        | PPC_M460EX 3.4.2000 2015-05-06 20:26:41 ppc  
                        | switch (config) #   |
| Related Commands     | N/A                  |
| Notes                |                      |
show voltage

Displays voltage level measurements on different sensors.

**Syntax Description**
N/A

**Default**
N/A

**Configuration Mode**
Any Command Mode

**History**
3.1.0000

3.3.5006 Updated Example

**Role**
admin

**Example**
switch (config) # show voltage

<table>
<thead>
<tr>
<th>Module</th>
<th>Power Meter</th>
<th>Reg</th>
<th>Expected Voltage</th>
<th>Actual Voltage</th>
<th>Status</th>
<th>High Range</th>
<th>Low Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>MGMT</td>
<td>BOARD_MONITOR</td>
<td>USB 5V sensor</td>
<td>5.00</td>
<td>5.15</td>
<td>OK</td>
<td>5.55</td>
<td>4.45</td>
</tr>
<tr>
<td>MGMT</td>
<td>BOARD_MONITOR</td>
<td>Asic I/O sensor</td>
<td>2.27</td>
<td>2.11</td>
<td>OK</td>
<td>2.55</td>
<td>1.99</td>
</tr>
<tr>
<td>MGMT</td>
<td>BOARD_MONITOR</td>
<td>1.8V sensor</td>
<td>1.80</td>
<td>1.79</td>
<td>OK</td>
<td>2.03</td>
<td>1.57</td>
</tr>
<tr>
<td>MGMT</td>
<td>BOARD_MONITOR</td>
<td>SYS 3.3V sensor</td>
<td>3.30</td>
<td>3.28</td>
<td>OK</td>
<td>3.68</td>
<td>2.92</td>
</tr>
<tr>
<td>MGMT</td>
<td>BOARD_MONITOR</td>
<td>CPU 0.9V sensor</td>
<td>0.90</td>
<td>0.93</td>
<td>OK</td>
<td>1.04</td>
<td>0.76</td>
</tr>
<tr>
<td>MGMT</td>
<td>BOARD_MONITOR</td>
<td>1.2V sensor</td>
<td>1.20</td>
<td>1.19</td>
<td>OK</td>
<td>1.37</td>
<td>1.03</td>
</tr>
<tr>
<td>MGMT</td>
<td>CPU_BOARD_MONITOR</td>
<td>12V sensor</td>
<td>12.00</td>
<td>11.67</td>
<td>OK</td>
<td>13.25</td>
<td>10.75</td>
</tr>
<tr>
<td>MGMT</td>
<td>CPU_BOARD_MONITOR</td>
<td>12V sensor</td>
<td>2.50</td>
<td>2.46</td>
<td>OK</td>
<td>2.80</td>
<td>2.20</td>
</tr>
<tr>
<td>MGMT</td>
<td>CPU_BOARD_MONITOR</td>
<td>2.5V sensor</td>
<td>3.30</td>
<td>3.26</td>
<td>OK</td>
<td>3.68</td>
<td>2.92</td>
</tr>
<tr>
<td>MGMT</td>
<td>CPU_BOARD_MONITOR</td>
<td>SYS 3.3V sensor</td>
<td>3.30</td>
<td>3.24</td>
<td>OK</td>
<td>3.68</td>
<td>2.92</td>
</tr>
<tr>
<td>MGMT</td>
<td>CPU_BOARD_MONITOR</td>
<td>SYS 3.3V sensor</td>
<td>1.80</td>
<td>1.79</td>
<td>OK</td>
<td>2.03</td>
<td>1.57</td>
</tr>
<tr>
<td>MGMT</td>
<td>CPU_BOARD_MONITOR</td>
<td>1.8V sensor</td>
<td>1.20</td>
<td>1.24</td>
<td>OK</td>
<td>1.57</td>
<td>1.03</td>
</tr>
</tbody>
</table>

switch (config) #

**Related Commands**
N/A

**Notes**
N/A
show chassis ha

show chassis ha

Displays Chassis HA parameters and status.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>N/A</td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Config</td>
</tr>
<tr>
<td>History</td>
<td>3.1.0000</td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
</tr>
</tbody>
</table>

**Example**

switch (config) # show chassis ha
2-node HA state:
   Box management IP: 172.30.1.200/16
      interface: mgmt0
         local role: master
         local slot: 1
         other state: ready
         reset count: 0
switch (config) #

**Related Commands**

chassis ha

**Notes**

This command is applicable only for director switch systems.
4.14 Network Management Interfaces

4.14.1 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

4.14.1.1 Standard MIBs

Table 30 - Standard MIBs – Textual Conventions and Conformance MIBs

<table>
<thead>
<tr>
<th>MIB</th>
<th>Standard</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>INET-ADDRESS-MIB</td>
<td>RFC-4001</td>
<td></td>
</tr>
<tr>
<td>SNMPV2-CONF</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SNMPV2-TC</td>
<td>RFC 2579</td>
<td></td>
</tr>
<tr>
<td>SNMPV2-TM</td>
<td>RFC 3417</td>
<td></td>
</tr>
<tr>
<td>SNMP-USM-AES-MIB</td>
<td>RFC 3826</td>
<td></td>
</tr>
<tr>
<td>IANA-LANGUAGE-MIB</td>
<td>RFC 2591</td>
<td></td>
</tr>
<tr>
<td>IANA-RTPROTO-MIB</td>
<td>RFC 2932</td>
<td></td>
</tr>
<tr>
<td>IANAifType-MIB</td>
<td></td>
<td></td>
</tr>
<tr>
<td>IANA-ADDRESS-FAMILY-NUMBERS-MIB</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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 31 - Standard MIBs – Chassis and Switch

<table>
<thead>
<tr>
<th>MIB</th>
<th>Standard</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>RFC1213-MIB</td>
<td>RFC 1213</td>
<td></td>
</tr>
<tr>
<td>IF-MIB</td>
<td>RFC 2863</td>
<td>ifXTable only supported.</td>
</tr>
<tr>
<td>ENTITY-MIB</td>
<td>RFC 4133</td>
<td></td>
</tr>
<tr>
<td>ENTITY-SENSOR-MIB</td>
<td>RFC 3433</td>
<td>Fan and temperature sensors</td>
</tr>
</tbody>
</table>
### Table 31 - Standard MIBs – Chassis and Switch

<table>
<thead>
<tr>
<th>MIB</th>
<th>Standard</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>ENTITY-STATE-MIB</td>
<td>RFC 4268</td>
<td>Fan and temperature states</td>
</tr>
<tr>
<td>Bridge MIB</td>
<td>RFC 4188</td>
<td>dot1dTpFdbGroup and dot1dStaticGroup are not supported in this MIB, it is supported as a part of Q-Bridge-MIB.</td>
</tr>
<tr>
<td>Q-Bridge MIB</td>
<td>RFC 4363</td>
<td>The following SNMP groups are not supported:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• qBridgeVlanStatisticsGroup,</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• qBridgeVlanStatisticsOverflowGroup,</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• qBridgeVlanHCStatisticsGroup,</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• qBridgeLearningConstraintsGroup.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The following SNMP tables are not supported:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• dot1qTpGroupTable (dynamic MAC addresses)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• dot1qForwardAllTable (GMRP)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• dot1qForwardUnregisteredTable (GMRP)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>dot1qVlanCurrentTable (GVRP)</td>
</tr>
<tr>
<td>RSTP-MIB</td>
<td>RFC 4318</td>
<td></td>
</tr>
<tr>
<td>LLDP-MIB</td>
<td>802.1AB-2005</td>
<td></td>
</tr>
<tr>
<td>ENTITY-SENSOR-MIB</td>
<td>RFC 3433</td>
<td>• Port module transmit/receiver power sensors</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Fan, temperature sensors</td>
</tr>
<tr>
<td>BGP4-MIB</td>
<td>RFC 4273</td>
<td>Only supports the following tables:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• bgpLocalAs</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• bgpPeerLocalAddr</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• bgpPeerState</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• bgpIdentifier</td>
</tr>
<tr>
<td>OSPF-MIB</td>
<td>RFC 4750</td>
<td></td>
</tr>
</tbody>
</table>
4.14.1.2 Private MIB

Table 32 - Private MIBs Supported

<table>
<thead>
<tr>
<th>MIB</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MELLANOX-SMI-MIB</td>
<td>Mellanox Private MIB main structure (no objects)</td>
</tr>
<tr>
<td>MELLANOX-PRODUCTS-MIB</td>
<td>List of OID – per managed system (sysObjID)</td>
</tr>
<tr>
<td>MELLANOX-IF-VPI-MIB</td>
<td>IfTable extensions</td>
</tr>
<tr>
<td>MELLANOX-EFM-MIB</td>
<td>Partially deprecated MIB (based on Mellanox-MIB)</td>
</tr>
<tr>
<td>MELLANOX-ENTITY-MIB</td>
<td>Enhances the standard ENTITY-MIB (contains GUID and ASIC revision)</td>
</tr>
<tr>
<td>MELLANOX-POWER-CYCLE</td>
<td>Allows rebooting the switch system</td>
</tr>
<tr>
<td>MELLANOX-SW-UPDATE-MIB</td>
<td>Allows viewing what SW images are installed, uploading and installing new SW images</td>
</tr>
<tr>
<td>MELLANOX-CONFIG-DB</td>
<td>Allows loading, uploading, or deleting configuration files</td>
</tr>
<tr>
<td>MELLANOX-ENTITY-STATE-MIB</td>
<td>Extension to support state change traps</td>
</tr>
<tr>
<td></td>
<td>Note: Currently supported for power supply insertion and extraction only</td>
</tr>
<tr>
<td>MELLANOX-XSTP-MIB</td>
<td>Extension to support STP information</td>
</tr>
<tr>
<td>MELLANOX-DCB-TRAPS</td>
<td>Extension traps for ETC and PFC</td>
</tr>
</tbody>
</table>

Mellanox private MIBs can be downloaded from the Mellanox Support webpage.

4.14.1.3 Mellanox Private Traps

The following private traps are supported by MLNX-OS®.

Table 33 - SNMP Traps

<table>
<thead>
<tr>
<th>Trap</th>
<th>Action Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>asicChipDown</td>
<td>Reboot the system.</td>
</tr>
<tr>
<td>asicOverTempReset</td>
<td>Check fans and environmental temperature.</td>
</tr>
<tr>
<td>asicOverTemp</td>
<td>Check fans and environmental temperature.</td>
</tr>
<tr>
<td>lowPower</td>
<td>Add/connect power supplies.</td>
</tr>
<tr>
<td>internalBusError</td>
<td>N/A</td>
</tr>
<tr>
<td>procCrash</td>
<td>Generate SysDump and contact Mellanox support.</td>
</tr>
<tr>
<td>cpuUtilHigh</td>
<td>N/A</td>
</tr>
<tr>
<td>procUnexpectedExit</td>
<td>Generate SysDump and contact Mellanox support.</td>
</tr>
<tr>
<td>diskSpaceLow</td>
<td>Clean images and sysDump files using the commands “image delete” and “file debug-dump delete”.</td>
</tr>
<tr>
<td>systemHealthStatus</td>
<td>Refer to Health Status table.</td>
</tr>
</tbody>
</table>
4.14.1.4 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:

```
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
```

Community strings are case sensitive.

Director switches require SNMP timeout configuration on the agent of 60 seconds.

For event-to-MIB mapping, please refer to Table 25, “Supported Event Notifications and MIB Mapping,” on page 307.

---

Table 33 - SNMP Traps

<table>
<thead>
<tr>
<th>Trap</th>
<th>Action Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>lowPowerRecover</td>
<td>N/A</td>
</tr>
<tr>
<td>insufficientFans</td>
<td>Check Fans and environmental conditions.</td>
</tr>
<tr>
<td>insufficientFansRecover</td>
<td>N/A</td>
</tr>
<tr>
<td>insufficientPower</td>
<td>Add/connect power supplies, or change power mode using the command “power redundancy mode”.</td>
</tr>
<tr>
<td>insufficientPowerRecover</td>
<td>N/A</td>
</tr>
</tbody>
</table>

For additional information refer to MELLANOX-EFM-MIB.
4.14.1.5 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```

4.14.1.6 Configuring an SNMP Notification

➢ To set up the SNMP Notification (traps or informs):

   Step 1. Make sure SNMP and SNMP notification are enable. Run:

   ```
   switch (config) # snmp-server enable
   switch (config) # snmp-server enable notify
   switch (config) #
   ```

   Step 2. Configure SNMP host with the desired arguments (IP Address, SNMP version, authentication methods). More than one host can be configured. Each host may have different attributes. Run:

   ```
   switch (config) # snmp-server host 10.134.47.3 traps version 3 user my-username auth sha my-password
   switch (config) #
   ```
Step 3. Verify the SNMP host configuration. Run:

```
switch (config) # show snmp host
Notifications enabled: yes
Default notification community: public
Default notification port: 162

Notification sinks:

    10.134.47.3
    Enabled: yes
    Port: 162 (default)
    Notification type: SNMP v3 trap
    Username: my-username
    Authentication type: sha
    Privacy type: aes-128
    Authentication password: (set)
    Privacy password: (set)
```

Step 4. Configure the desired event to be sent via SNMP. Run:

```
switch (config) # snmp-server notify event interface-up
switch (config) #
```

This particular event is used as an example only.
Step 5. Verify the list of traps and informs being sent to out of the system. Run:

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

Events for which traps will be sent:
-asic-chip-down: ASIC (Chip) Down
-cpu-util-high: CPU utilization has risen too high
-disk-space-low: Filesystem free space has fallen too low
-health-module-status: Health module Status
-insufficient-fans: Insufficient amount of fans in system
-insufficient-fans-recover: Insufficient amount of fans in system recovered
-insufficient-power: Insufficient power supply
-interface-down: An interface's link state has changed to down
-interface-up: An interface's link state has changed to up
-internal-bus-error: Internal bus (I2C) Error
-liveness-failure: A process in the system was detected as hung
-low-power: Low power supply
-low-power-recover: Low power supply Recover
-new_root: local bridge became a root bridge
-paging-high: Paging activity has risen too high
-power-redundancy-mismatch: Power redundancy mismatch
-process-crash: A process in the system has crashed
-process-exit: A process in the system unexpectedly exited
-snmp-authtrap: An SNMP v3 request has failed authentication
-topology_change: local bridge triggered a topology change
-unexpected-shutdown: Unexpected system shutdown

```
switch (config) #
```

To print event notifications to the terminal (SSH or CONSOLE) refer to Section 4.5.1, “Monitor,” on page 262.

### 4.14.1.7 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.

#### 4.14.1.7.1 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 (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
```

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 <password2>
```

It is possible to use other configuration options not specified in the example above. Please refer to the command “snmp-server user” on page 520 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 34 which are expanded upon in the following subsections.

**Table 34 - Supported SET OIDs**

<table>
<thead>
<tr>
<th>MIB Name</th>
<th>OID Name</th>
<th>OID</th>
</tr>
</thead>
<tbody>
<tr>
<td>MELLANOX-EFM-MIB</td>
<td>sendTestTrapSet</td>
<td>1.3.6.1.4.1.33049.2.1.1.1.6.0</td>
</tr>
<tr>
<td>SNMPv2-MIB</td>
<td>sysName</td>
<td>1.3.6.1.2.1.1.5.0</td>
</tr>
</tbody>
</table>
4.14.1.7.2 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:
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 1.3.6.1.4.1.33049.12.1.1.2.1.0.

Step 2. Make sure the test trap is received by the aforementioned trap receiver (OID: 1.3.6.1.4.1.33049.12.1.1.2.13).

4.14.1.7.3 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 159 for more information.
4.14.1.7.4 Power Cycle with SNMP

Mellanox supports power cycling its systems using an SNMP SET request as described in MELLANOX-POWER-CYCLE MIB.

Power cycle command is issued via the OID mellanoxPowerCycleCmdExecute. The following options are available:

- Reload – saves any unsaved configuration and reloads the switch
- Reload discard – reboots the system and discards of any unsaved changes
- Reload force – forces an expedited reload on the system even if it is busy without saving unsaved configuration (equals the CLI command `reload force`)
- Reload slave – reloads the slave management on dual management systems (must be executed from the master management module)

On dual management systems it is advised to connect via the BIP to make sure commands are executed from the master management.

4.14.1.7.5 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 are supported:

- Command URI – URI to fetch the configuration file from or upload the file to (for supported URI format please refer to the CLI command “configuration fetch” for more details)
- Config file name – filename to save the configuration file to or to upload to remote location

The following commands are supported:
BinarySwitchTo – replaces the configuration file with a new binary configuration file. This option fetches the configuration file from the URI provided in the `mellanoxConfigDBCmdUri` and switches to that configuration file. This command should be preceded by a reload command in order for the new configuration to apply.

TextApply – fetches a configuration file in human-readable format and applies its configuration upon the current configuration.

BinaryUpload – uploads a binary format configuration file of the current running configuration or an existing configuration file on the switch to the URI in the `mellanoxConfigDBCmdUri` command. The filename parameter indicates what configuration file on the switch to upload.

TextUpload – uploads a human-readable configuration file of the current running configuration of an existing configuration file on the switch to the URI in the `mellanoxConfigDBCmdUri` command. The filename parameter indicates what configuration file on the switch to upload (same as the CLI command `configuration text generate file <filename> upload`).

ConfigWrite – saves active configuration to a filename on the switch as given in the filename parameter. In case filename is “active”, active configuration is saved to the current saved configuration (same as the CLI command `configuration write`).

BinaryDelete – deletes a binary based configuration file

TextDelete – deletes a text based configuration file

4.14.1.7.6 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 220.

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%
- 101 – success
- 200 – failure

4.14.1.8 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 ifTable, 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).

4.14.2 JSON API

JavaScript Object Notation (JSON) is a machine-to-machine data-interchange format which is supported in MLNX-OS® CLI.

The JSON API allows executing CLI commands and receiving outputs in JSON format which can be easily parsed by the calling software.

4.14.2.1 JSON Request Over HTTP/HTTPS

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.
4.14.2.1.1 Authentication

The HTTP client must first be authenticated by sending a POST request to the following URL:
The POST request content should contain the following variables:
• f_user_id
• f_password

4.14.2.1.2 Sending the Request

After authenticating the HTTP client, the user needs to construct a POST request containing the
CLI command they wish to execute as the payload of the request (see Section 4.14.2.1.3, “JSON
Request Format,” on page 500 for the CLI request format). Using the HTTP client, the POST
request 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 reply with an indication of
the request execution result. If there is data resulting from the request, it is returned as part of the
reply.


JSON POST requests may also be sent using the WebUI. For more information, please refer to

4.14.2.1.3 JSON Request Format

The request format is a JSON object consisting of a single name-value pair where the name is the
string “cmd” and the value is the CLI command the user executed as a string also.

```
{
    "cmd": "<CLI command to execute>"
}
```

Only one query/request command is supported at a time.


4.14.2.1.4 JSON Response Format

The HTTP POST response format structure is a JSON object consisting of 3 name-value pairs as
follows:

```
{
    "status" = "<OK|ERROR>",
    "data" = {The information requested}
    "status_message" = "<Information on the status received>",
}
```

• Status – the result of the request execution
  • “OK” if the execution is successful
• “ERROR” in case of a problem with the execution
  The value type of this key is “string”.

• Data – a JSON object containing the information requested
  Returns an empty string if there is no data.

• Status message – additional information on the received status
  May be empty. The value type of this key is “string”.

4.14.2.1.5 Supported 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.

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 C, “Show Commands Supported by JSON API,” on page 1342.

4.14.2.1.6 JSON Examples

The following examples use cURL (common tool in Linux systems) to send HTTP POST requests to the system.

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"

Query Request Example
This example sends a request to query the XML gateway setting on the switch system.

Step 1. Prepare your request.

The request payload must look like this:

```json
{"cmd": "show xml-gw"}
```

Send the POST request using cURL with the request payload as follows:

```bash
echo '{"cmd":" show xml-gw"}' | curl -b /tmp/cookie -X POST -d @-
"http://10.10.10.10/admin/launch?script=json"
```
Step 2. Get the reply.

After sending the request, when the system finishes processing, a reply similar to the following is received:

```
{
  "status": "OK",
  "data": {
    "XML Gateway enabled": "yes"
  },
  "status_message": ""
}
```

You may also prepare a file containing the JSON request as follows:

Step 1. Prepare the JSON request.

The file used in this example is “req_example.json”:

```
{
  "cmd": "show xml-gw"
}
```

Step 2. Use it as the POST request payload like this. Run:

```
curl -b /tmp/cookie -X POST -d @req_example.json http://10.10.10.10/admin/launch?script=json
```

Set Request Example

This example sends a request to enable SNMP server.

Step 1. Prepare your request

The request payload should look like this:

```
{"cmd": "snmp-server enable"}
```

Send the POST request using cURL with the request payload as follows:

```
echo "{"cmd":"snmp-server enable"}" | curl -b /tmp/cookie -X POST -d @-"http://10.10.10.10/admin/launch?script=json"
```

Step 2. Get the reply.

After sending the request, when the system finishes processing, a reply similar to the following is received:

```
{
  "status": "OK",
  "data": "",
  "status_message": ""
}
```

Set commands normally do not return any data or output. In instances where a set command returns an output, it is displayed in the "status_message" field.
Error Response Example

If the request fails, the status value returned is “ERROR” and, if applicable, the “status_msg” value will contain a description of the problem.

For example, sending a request without authentication results in the following ERROR:

```
error_response = 
{'status': 'ERROR',
 'data': '',
 'status_message': 'Request not authenticated'}
```

4.14.2.2 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”.

In the “cmd” field type the CLI command to execute then press “Submit”. The JSON response is then shown in the “JSON Response” box below.
4.14.3 XML API

MLNX-OS XML API is documented in the *MLNX-OS® XML API Reference Guide.*
4.14.4 Commands

4.14.4.1 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.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>Enables SNMPD refresh mechanism.</td>
</tr>
<tr>
<td>interval</td>
<td>Sets SNMPD refresh interval.</td>
</tr>
<tr>
<td>time</td>
<td>In seconds. Range: 20-500.</td>
</tr>
</tbody>
</table>

Default: Enabled. Interval: 60 secs

Configuration Mode: Config

History:

- 3.2.3000
- 3.4.1100 Added time parameter and updated notes

Role: admin

Example:

```
switch (config) # snmp-server auto-refresh interval 120
```

Related Commands:

- show snmp

Notes:

- When configuring an interval lower than 60 seconds, the following warning message appears asking for confirmation: “Warning: this configuration may increase CPU utilization, Type 'YES' to confirm: YES”.
- When disabling SNMP auto-refresh, information is retrieved no more than once every 60 seconds just like SNMP tables that do not have an auto-refresh mechanism.
**snmp-server community**

```
        snmp-server community <community> [ ro | rw]
        no snmp-server community <community>
```

Sets a community name for either read-only or read-write SNMP requests. The no form of the command sets the community string to default.

**Syntax Description**

<table>
<thead>
<tr>
<th>Community</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<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>
</tbody>
</table>

**Default**

- Read-only community: “public”
- Read-write community: “”

**Configuration Mode**

Config

**History**

3.1.0000

**Role**

admin

**Example**

```
switch(config) # snmp-server community private rw
switch (config) # show snmp
SNMP enabled: yes
SNMP port: 161
System contact:
System location:
Read-only community: public
Read-write community: private

Interface listen enabled: yes
No Listen Interfaces.

Traps enabled: yes
Default trap community: public
Default trap port: 162

No trap sinks configured.
switch(config) #
```

**Related Commands**

show snmp

**Notes**

- If neither the “ro” or the “rw” parameters are specified, the read-only community is set as the default community
- If the read-only community is specified, only queries can be performed
- If the read-write community is specified, both queries and sets can be performed
**snmp-server contact**

`snmp-server contact <contact name>`
`no snmp-server contact`

Sets a value for the sysContact variable in MIB-II.
The no form of the command resets the parameter to its default value.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>contact name</td>
<td>Contact name.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Default</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>“”</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Configuration Mode</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Config</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>History</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>3.1.0000</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Role</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>admin</td>
<td></td>
</tr>
</tbody>
</table>

**Example**

```
switch (config) # snmp-server contact my-name
switch (config) # show snmp
SNMP enabled: yes
SNMP port: 161
System contact: my-name
System location:
Read-only community: public
Read-write community: private

Interface listen enabled: yes
No Listen Interfaces.

Traps enabled: yes
Default trap community: public
Default trap port: 162

No trap sinks configured.
switch (config) #
```

**Related Commands**

`show snmp`

**Notes**
snmp-server enable

**snmp-server enable**
**no snmp-server enable**

Enables SNMP-related functionality (SNMP engine, and traps)
The no form of the command disables the SNMP server.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>SNMP is enabled by default</td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Config</td>
</tr>
<tr>
<td>History</td>
<td>3.1.0000</td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
</tr>
<tr>
<td>Example</td>
<td>switch (config) # snmp-server enable</td>
</tr>
<tr>
<td>Related Commands</td>
<td>show snmp</td>
</tr>
<tr>
<td>Notes</td>
<td></td>
</tr>
</tbody>
</table>
### 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.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>SNMP server communities are enabled by default</td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Config</td>
</tr>
<tr>
<td>History</td>
<td>N/A</td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
</tr>
<tr>
<td>Example</td>
<td>switch (config) # snmp-server enable communities</td>
</tr>
<tr>
<td>Related Commands</td>
<td>show snmp</td>
</tr>
<tr>
<td>Notes</td>
<td></td>
</tr>
</tbody>
</table>
**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.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>SNMP server multi-communities are disabled by default</td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Config</td>
</tr>
<tr>
<td>History</td>
<td>N/A</td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
</tr>
<tr>
<td>Example</td>
<td>switch (config) # snmp-server enable mult-communities</td>
</tr>
<tr>
<td>Related Commands</td>
<td>show snmp</td>
</tr>
<tr>
<td>Notes</td>
<td></td>
</tr>
</tbody>
</table>
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.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>SNMP notifies are enabled by default</td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Config</td>
</tr>
<tr>
<td>History</td>
<td>N/A</td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
</tr>
<tr>
<td>Example</td>
<td>switch (config) # snmp-server enable notify</td>
</tr>
<tr>
<td>Related Commands</td>
<td>show snmp</td>
</tr>
<tr>
<td>Notes</td>
<td>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.</td>
</tr>
</tbody>
</table>
**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.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>SNMP MIBs are all given permission for SET requests by default</td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Config</td>
</tr>
<tr>
<td>History</td>
<td>3.6.3004</td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
</tr>
<tr>
<td>Example</td>
<td><code>switch (config) # snmp-server enable set-permission MELLANOX-SW-UPDATE</code></td>
</tr>
<tr>
<td>Related Commands</td>
<td>show snmp set-permission</td>
</tr>
<tr>
<td>Notes</td>
<td></td>
</tr>
</tbody>
</table>
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.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>IP address</th>
<th>IPv4 or IPv6 address.</th>
</tr>
</thead>
<tbody>
<tr>
<td>disable</td>
<td>Temporarily disables sending of traps to this host.</td>
<td></td>
</tr>
<tr>
<td>community</td>
<td>Specifies trap community string.</td>
<td></td>
</tr>
<tr>
<td>port</td>
<td>Overrides default UDP port for this trap sink.</td>
<td></td>
</tr>
<tr>
<td>snmp version</td>
<td>Specifies the SNMP version of traps to send to this host.</td>
<td></td>
</tr>
</tbody>
</table>

**Default**

No hosts are configured
Default community is “public”
Default UDP port is 162
Default SNMP version is 2c

**Configuration Mode**

Config

**History**

3.1.0000 First version
3.2.1050 Add inform option

**Role**

admin
Example

```
switch (config) # snmp-server host 10.10.10.10 traps version 1
switch (config) # show snmp
SNMP enabled: yes
SNMP port: 161
System contact: 
System location: 

Read-only communities:
    public

Read-write communities:
  (none)

Interface listen enabled: yes
No Listen Interfaces.

Traps enabled: yes
Default trap community: public
Default trap port: 162

Trap sinks:
  10.10.10.10
    Enabled: yes
    Type: traps version 1
    Port: 162 (default)
    Community: public (default)
```

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.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>enable</th>
<th>Enables SNMP interface restrictions on access to this system.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>ifName</td>
<td>Adds an interface to the “listen” list for SNMP server. For example: “mgmt0”, “mgmt1”.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Default</th>
<th>N/A</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Configuration Mode</th>
<th>Config</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>History</th>
<th>3.1.0000</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Role</th>
<th>admin</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Example</th>
</tr>
</thead>
</table>
| 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) # |

<table>
<thead>
<tr>
<th>Related Commands</th>
<th>show snmp</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>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.</td>
</tr>
</tbody>
</table>
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.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>System Location</th>
<th>String</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td></td>
<td>&quot;&quot;</td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Config</td>
<td></td>
</tr>
<tr>
<td>History</td>
<td>3.1.0000</td>
<td></td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
<td></td>
</tr>
</tbody>
</table>
| Example            | switch (config) # snmp-server location lab
switch (config) # show snmp
SNMP enabled: yes
SNMP port: 161
System contact: my-name
System location: lab
Read-only community: public
Read-write community: private
Interface listen enabled: yes
No Listen Interfaces.
Traps enabled: yes
Default trap community: public
Default trap port: 162
No trap sinks configured.
switch (config) # |
| Related Commands  | show snmp               |          |
| Notes              |                         |          |
### snmp-server notify

```
snmp-server notify {community <community> | event <event name> | port <port> | send-test}
no snmp-server notify {community | event <event name> | port}
```

Configures SNMP notifications (traps and informs). The no form of the commands negate the SNMP notifications.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>community</th>
<th>Sets the default community for traps sent to hosts which do not have a custom community string set.</th>
</tr>
</thead>
<tbody>
<tr>
<td>event</td>
<td>event</td>
<td>Specifies which events will be sent as traps.</td>
</tr>
<tr>
<td>port</td>
<td>port</td>
<td>Sets the default port to which traps are sent.</td>
</tr>
<tr>
<td>send-test</td>
<td>send-test</td>
<td>Sends a test trap.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Default</th>
<th>Community: public</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>All informs and traps are enabled</td>
</tr>
<tr>
<td></td>
<td>Port: 162</td>
</tr>
</tbody>
</table>

**Configuration Mode**  
Config

**History**  
3.1.0000  
First version

3.2.1050  
Changed traps to notify

**Role**  
admin

**Example**
```
switch (config) # snmp-server community public
switch (config) # show snmp
SNMP enabled: yes
SNMP port: 1000
System contact: my-name
System location: lab
Read-only community: public
Read-write community: private

Interface listen enabled: yes
No Listen Interfaces.

Traps enabled: yes
Default trap community: public
Default trap port: 162

No trap sinks configured.
switch (config) #
```
### Related Commands
- show snmp
- show snmp events

### Notes
- This setting is only meaningful if traps are enabled, though the list of hosts may still be edited if traps are disabled
- Refer to Mellanox MIB file for the list of supported traps
### snmp-server port

**snmp-server port <port>**
**no snmp-server port**

Sets the UDP listening port for the SNMP agent.
The no form of the command resets the parameter to its default value.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>port</td>
<td>UDP port.</td>
</tr>
</tbody>
</table>

**Default** 161

**Configuration Mode** Config

**History** 3.1.0000

**Role** admin

**Example**

```
switch (config) # snmp-server port 1000
switch (config) # show snmp
SNMP enabled:    yes
SNMP port:       1000
System contact:  my-name
System location: lab
Read-only community:  public
Read-write community: private

Interface listen enabled: yes
No Listen Interfaces.

Traps enabled:    yes
Default trap community: public
Default trap port: 162

No trap sinks configured.
switch (config) #
```

**Related Commands**

show snmp

**Notes**
snmp-server user

```
snmp-server user {admin | <username>} v3 {[encrypted] auth <hash-type> <password> [priv <privacy-type> |<password>]} | capability <cap> | enable <sets> | prompt auth <hash-type> [priv <privacy-type>] | require-privacy
no snmp-server user {admin | <username>} v3 {[encrypted] auth <hash-type> <password> [priv <privacy-type> |<password>]} | capability <cap> | enable <sets> | prompt auth <hash-type> [priv <privacy-type>]}
```

Specifies an existing username, or a new one to be added. The no form of the command disables access via SNMP v3 for the specified user.

### Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>v3</td>
<td>Configures SNMP v3 users</td>
</tr>
<tr>
<td>auth</td>
<td>Configures SNMP v3 security parameters, specifying passwords in plaintext on the command line (note: passwords are always stored encrypted)</td>
</tr>
<tr>
<td>capability</td>
<td>Sets capability level for SET requests</td>
</tr>
<tr>
<td>enable</td>
<td>Enables SNMP v3 access for this user</td>
</tr>
<tr>
<td>encrypted</td>
<td>Configures SNMP v3 security parameters, specifying passwords in encrypted form</td>
</tr>
<tr>
<td>prompt</td>
<td>Configures SNMP v3 security parameters, specifying passwords securely in follow-up prompts, rather than on the command line</td>
</tr>
<tr>
<td>require-privacy</td>
<td>Requires privacy (encryption) for requests from this user</td>
</tr>
</tbody>
</table>

### Default

No SNMP v3 users defined

### Configuration Mode

Config

### History

3.1.0000

### Role

admin

### Example

```
switch (config) # snmp-server user admin v3 enable
switch (config) # show snmp user
User name: admin
  Enabled overall: yes
  Authentication type: sha
  Privacy type: aes-128
Authentication password: (NOT SET; user disabled)
Privacy password: (NOT SET; user disabled)
SET access:
  Enabled: yes
  Capability level: admin
switch (config) #
```
Related Commands

show snmp user

Notes

- The username chosen here may be anything that is valid as a local UNIX username (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.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>auto-refresh</td>
<td>SNMP refreshed mechanism status.</td>
</tr>
<tr>
<td>engineID</td>
<td>SNMP Engine ID.</td>
</tr>
<tr>
<td>events</td>
<td>SNMP events.</td>
</tr>
<tr>
<td>host</td>
<td>List of notification sinks.</td>
</tr>
<tr>
<td>user</td>
<td>SNMP users.</td>
</tr>
</tbody>
</table>

| Default   | N/A                             |
| Configuration Mode | Config                      |
| History   | 3.1.0000                        |
| Role      | admin                           |

<table>
<thead>
<tr>
<th>Example</th>
</tr>
</thead>
</table>
| 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) # |

<table>
<thead>
<tr>
<th>Related Commands</th>
<th>show snmp</th>
</tr>
</thead>
</table>

| Notes |
|-------|----------|

show snmp auto-refresh

show snmp auto-refresh

Displays SNMPD refresh mechanism status.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>N/A</td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Config</td>
</tr>
<tr>
<td>History</td>
<td>3.1.0000</td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
</tr>
</tbody>
</table>

**Example**

```
switch (config) # show snmp auto-refresh
------------------
SNMP auto refresh
------------------
Auto-refresh enabled:       yes
Refresh interval (sec):    60
------------------
Auto-Refreshed tables
------------------
entPhysicalTable
ifTable
ifXTable
```

**Related Commands**

snmp-server auto-refresh

**Notes**
### show snmp set-permission

**show snmp set-permission**

Displays SNMP SET permission settings.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>N/A</td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Config</td>
</tr>
<tr>
<td>History</td>
<td>3.6.3004</td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
</tr>
</tbody>
</table>

#### Example

```
switch (config) # show snmp set-permission
```

<table>
<thead>
<tr>
<th>MIB Name</th>
<th>Set Enable</th>
</tr>
</thead>
<tbody>
<tr>
<td>MELLANOX-CONFIG-DB-MIB</td>
<td>yes</td>
</tr>
<tr>
<td>MELLANOX-EFM-MIB</td>
<td>yes</td>
</tr>
<tr>
<td>MELLANOX-POWER-CYCLE</td>
<td>yes</td>
</tr>
<tr>
<td>MELLANOX-SW-UPDATE</td>
<td>no</td>
</tr>
<tr>
<td>RFC1213-MIB</td>
<td>no</td>
</tr>
</tbody>
</table>

#### Related Commands

snmp-server enable set-permission

#### Notes
4.14.4.2 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.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Default</strong></td>
<td>XML Gateway is enabled</td>
</tr>
<tr>
<td><strong>Configuration Mode</strong></td>
<td>Config</td>
</tr>
<tr>
<td><strong>History</strong></td>
<td>3.1.0000</td>
</tr>
<tr>
<td><strong>Role</strong></td>
<td>admin</td>
</tr>
</tbody>
</table>

**Example**

```
switch (config) # xml-gw enable
switch (config) # show xml-gw
XML Gateway enabled: yes
switch (config) #
```

**Related Commands**

- `show xml-gw`

**Notes**
### show xml-gw

**show xml-gw**

Displays the XML gateway setting.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>N/A</td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Any Command Mode</td>
</tr>
<tr>
<td>History</td>
<td>3.1.0000</td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
</tr>
</tbody>
</table>

**Example**

```bash
switch (config) # show xml-gw
XML Gateway enabled: yes
switch (config) #
```

**Related Commands**

xml-gw enable

**Notes**
### json-gw enable

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>JSON API is enabled</td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Config</td>
</tr>
<tr>
<td>History</td>
<td>3.6.3004</td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
</tr>
</tbody>
</table>

**Example**

```
switch (config) # json-gw enable
```

**Related Commands**

- `show json-gw`

**Notes**

This command is available on x86 switch systems only.
show json-gw

Syntax Description
N/A

Default
N/A

Configuration Mode
Any Command Mode

History
3.6.3004

Role
admin

Example
switch (config) # show json-gw
JSON Gateway enabled: yes

Related Commands
json-gw enable

Notes
This command is available on x86 switch systems only.
4.15 Puppet Agent

Puppet is a software that allows network administrators to automate repetitive tasks. MLNX-OS includes a built-in agent for the open-source “Puppet” configuration change management system. The Puppet agent enables configuring Mellanox switches in accordance with the standard “puppet-netdev-stdlib” type library and with the “Mellanox-netdev-stdlib-mlnxos” and “Mellanox-netdev-ospf-stdlib” type libraries provided by Mellanox Technologies to the Puppet community.

For more information, please refer to the CLI commands, to the NetDev documentation at https://github.com/puppetlabs/puppet-netdev-stdlib and to Mellanox’s Puppet modules GitHub page at https://github.com/Mellanox.

4.15.1 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) #
```

4.15.2 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:**

```
switch (config) # puppet-agent master-hostname <please_type_your_hostname_DNS_here>
switch (config) #
switch (config) # puppet-agent enable
switch (config) #
switch (config) # show puppet-agent log continuous
switch (config) #
```
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 13: Accepting an Agent Request through the Console

4.15.3 Installing Modules on the Puppet Server

Mellanox uses netdev-stdlib types and provides a package of Mellanox providers for those types which have to be installed at the Puppet server prior to the first Puppet configuration run (before configuring resources on the Mellanox switch).

To install those modules, run the following commands in the Puppet server:

```bash
# 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.

4.15.4 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:

```puppet
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”).

```puppet
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”)

```perl
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”)

```perl
class lag_example{
    $tags = {
        '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, $tags )
}
```

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).
4.15.5 Supported Configuration Capabilities

4.15.5.1 Ethernet and Port-Channel Interface Capabilities

**Table 35 - Ethernet and Port-Channel Interface Capabilities**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Values</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>ensure</td>
<td>Sets the given values or restores the interface to default</td>
<td>absent, present</td>
<td>ensure =&gt; present</td>
</tr>
<tr>
<td>speed</td>
<td>Sets the speed of the interface.</td>
<td>auto*</td>
<td>10m</td>
</tr>
<tr>
<td>admin</td>
<td>Disables/enables interface admin state.</td>
<td>up, down</td>
<td>admin =&gt; up</td>
</tr>
<tr>
<td>mtu</td>
<td>Configures the maximum transmission unit frame size for the interface.</td>
<td>Ethernet: 1518-9216</td>
<td>mtu =&gt; 1520</td>
</tr>
<tr>
<td>description</td>
<td>Sets the Ethernet and LAG description.</td>
<td>Text</td>
<td>description =&gt; “changed_by_puppet”</td>
</tr>
</tbody>
</table>

4.15.5.2 VLAN Capabilities

**Table 36 - VLAN Capabilities**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Values</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>ensure</td>
<td>Creates or destroys the VLAN given as a resource ID</td>
<td>absent, present</td>
<td>ensure =&gt; present</td>
</tr>
<tr>
<td>vlan_id</td>
<td>The VLAN ID</td>
<td>1-4094 (integer)</td>
<td>vlan_id =&gt; 245</td>
</tr>
</tbody>
</table>

4.15.5.3 Layer 2 Ethernet Interface Capabilities

**Table 37 - L2 Ethernet and Port-Channel Interface Capabilities**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Values</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>ensure</td>
<td>Sets the given values or restores the Layer 2 interface to default.</td>
<td>absent, present</td>
<td>ensure =&gt; present</td>
</tr>
<tr>
<td>vlan_tagging</td>
<td>VLAN tagging mode</td>
<td>enable,disable</td>
<td>vlan_tagging =&gt; enable</td>
</tr>
<tr>
<td>tagged_vlans</td>
<td>List of tagged (trunked) VLANs</td>
<td>2-4994 (range)</td>
<td>tagged_vlans =&gt; [Vlan348,Vlan347]</td>
</tr>
<tr>
<td>untagged_vlan</td>
<td>Untag (access) VLAN</td>
<td>&lt;VLAN name&gt;</td>
<td>untagged_vlan =&gt; Vlan349</td>
</tr>
</tbody>
</table>
### 4.15.5.4 LAG (Port-Channel) Capabilities

**Table 38 - LAG Capabilities**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Values</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>ensure</td>
<td>creates or destroys the port-channel given as a resource ID</td>
<td>absent, present</td>
<td>ensure =&gt; present</td>
</tr>
<tr>
<td>lacp</td>
<td>The LACP mode of the LAG</td>
<td>passive</td>
<td>on</td>
</tr>
<tr>
<td>links</td>
<td>List of ports assigned to the LAG</td>
<td>List of link names</td>
<td>links =&gt; ['ethernet 1/6','ethernet 1/5']</td>
</tr>
</tbody>
</table>

### 4.15.5.5 Layer 3 Interface Capabilities

**Table 39 - L3 Interface Capabilities**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Values</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>ensure</td>
<td>Creates or destroys the interface VLAN specified in the resource ID.</td>
<td>present, absent</td>
<td>ensure =&gt; present</td>
</tr>
<tr>
<td>ipaddress</td>
<td>Sets IP address on the Layer 3 interface (requires netmask).</td>
<td>A valid IP address</td>
<td>ipaddress =&gt; ‘192.168.4.2’</td>
</tr>
<tr>
<td>netmask</td>
<td>Sets netmask for the IP address.</td>
<td>A valid netmask (of the form X.1X2.X3.X4), which creates a valid combination with the given IP address</td>
<td>netmask =&gt; ‘255.255.255.0’</td>
</tr>
<tr>
<td>method</td>
<td>Configures the method of the L3 interface (currently supports only static method).</td>
<td>static</td>
<td>method =&gt; static</td>
</tr>
</tbody>
</table>

### 4.15.5.6 OSPF Interface Capabilities

**Table 40 - OSPF Interface Capabilities**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Values</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>ensure</td>
<td>Creates or destroys the OSPF interface of the associated interface of the VLAN specified in the resource ID</td>
<td>present, absent</td>
<td>ensure =&gt; present</td>
</tr>
<tr>
<td>area_id</td>
<td>The associated area ID</td>
<td>Integer representing an IP</td>
<td>area_id =&gt; ‘7200’</td>
</tr>
</tbody>
</table>
### Table 40 - OSPF Interface Capabilities

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Values</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>The network type</td>
<td>broadcast, point_to_point</td>
<td>type =&gt; ‘point_to_point’</td>
</tr>
</tbody>
</table>
4.15.5.7 OSPF Area Capabilities

Table 41 - OSPF Area Capabilities

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Values</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>ensure</td>
<td>Creates or destroys the OSPF area specified in the resource ID</td>
<td>present, absent</td>
<td>ensure =&gt; present</td>
</tr>
<tr>
<td>router_id</td>
<td>The OSPF area associated router ID (currently supports only default router)</td>
<td>default</td>
<td>router_id =&gt; 'default'</td>
</tr>
<tr>
<td>ospf_area_mode</td>
<td>The OSPF area mode (normal, stub, nssa)</td>
<td>normal, stub, nssa</td>
<td>ospf_area_mode =&gt; 'stub'</td>
</tr>
<tr>
<td>subnets</td>
<td>A list of associated subnets</td>
<td>List of subnets</td>
<td>[&quot;192.168.4.0/24&quot;, &quot;192.168.5.0/24&quot;]</td>
</tr>
</tbody>
</table>

4.15.5.8 Router OSPF Capabilities

Table 42 - Router OSPF Capabilities

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Values</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>ensure</td>
<td>Enables/disables the router ID specified in the resource ID</td>
<td>present, absent</td>
<td>ensure =&gt; present</td>
</tr>
</tbody>
</table>

4.15.5.9 Protocol LLDP, SNMP, IP Routing and Spanning Tree Capabilities

Table 43 - Protocol Enable/Disable Capabilities

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Values</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>ensure</td>
<td>Enables/disables the protocol specified in the resource ID</td>
<td>present, absent</td>
<td>ensure =&gt; present</td>
</tr>
</tbody>
</table>

4.15.5.10 Fetched Image Capabilities

Table 44 - Fetched Image Capabilities

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Values</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>ensure</td>
<td>Enables/disables the protocol specified in the resource ID</td>
<td>present, absent</td>
<td>ensure =&gt; present</td>
</tr>
<tr>
<td>protocol</td>
<td>Specifies the protocol for fetch method</td>
<td>http, https, ftp, tftp, scp, sftp</td>
<td>protocol =&gt; scp</td>
</tr>
<tr>
<td>host</td>
<td>The host where the file-name located</td>
<td>DNS/IP</td>
<td>host =&gt; my_DNS</td>
</tr>
</tbody>
</table>
Table 44 - Fetched Image Capabilities

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Values</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>user</td>
<td>The username for fetching the image</td>
<td>Username</td>
<td>user =&gt; my_username</td>
</tr>
<tr>
<td>password</td>
<td>The password for fetching the image</td>
<td>Password</td>
<td>password =&gt; my_pass</td>
</tr>
<tr>
<td>location</td>
<td>The location of the file name in the host file system</td>
<td>Directory full path</td>
<td>location =&gt; '/tmp'</td>
</tr>
<tr>
<td>force_delete</td>
<td>Remove all the images or only the ones which are not installed on any partition, before fetching</td>
<td>yes, no</td>
<td>force_delete =&gt; no</td>
</tr>
</tbody>
</table>

4.15.5.11 Installed Image Capabilities

Table 45 - Installed Image Capabilities

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Values</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>ensure</td>
<td>Specifies if the image version given in as resource ID is ensured to be installed or not</td>
<td>present, absent</td>
<td>ensure =&gt; present</td>
</tr>
<tr>
<td>is_next_boot</td>
<td>Ensures that the installed image is the next boot partition</td>
<td>yes, no</td>
<td>is_next_boot =&gt; yes</td>
</tr>
<tr>
<td>configuration_write</td>
<td>Writes configurations to database.</td>
<td>yes, no</td>
<td>configuration_write =&gt; yes</td>
</tr>
<tr>
<td>force_reload</td>
<td>Reload if image is in other partition.</td>
<td>yes, no</td>
<td>force_reload =&gt; no</td>
</tr>
</tbody>
</table>

4.15.6 Supported Resources for Each Type

Table 46 - Fetched Image Capabilities

<table>
<thead>
<tr>
<th>Resource Type</th>
<th>Puppet Type Name</th>
<th>Supported Resource IDS</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network device</td>
<td>netdev_device</td>
<td>$hostname</td>
<td>netdev_device { $hostname: }</td>
</tr>
<tr>
<td>Layer 1 interface</td>
<td>netdev_interface</td>
<td>'ethernet &lt;#ID&gt;', 'port-channel &lt;#id&gt;', 'ib &lt;#ID&gt;'</td>
<td>netdev_interface{'ethernet 1/3': ensure =&gt; absent}</td>
</tr>
</tbody>
</table>
### Table 46 - Fetched Image Capabilities

<table>
<thead>
<tr>
<th>Resource Type</th>
<th>Puppet Type Name</th>
<th>Supported Resource IDs</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Layer 2 interface</td>
<td>netdev_l2_interface</td>
<td>'ethernet &lt;#ID&gt;', 'port-channel &lt;#id&gt;'</td>
<td>netdev_l2_interface{'ethernet 1/3': ensure =&gt; absent}</td>
</tr>
<tr>
<td>VLAN</td>
<td>netdev_vlan</td>
<td>VLAN name string</td>
<td>netdev_vlan {'Vlan244': vlan_id =&gt; 244, ensure =&gt; present }</td>
</tr>
<tr>
<td>LAG</td>
<td>netdev_lag</td>
<td>'port-channel &lt;#id&gt;'</td>
<td>netdev_lag {'port-channel 101': ensure =&gt; present}</td>
</tr>
<tr>
<td>Layer 3 interface</td>
<td>netdev_l3_interface</td>
<td>'vlan &lt;#ID&gt;'</td>
<td>netdev_l3_interface{ 'vlan 4': ipaddress =&gt; '192.168.4.2', netmask =&gt; '255.255.255.0' }</td>
</tr>
<tr>
<td>OSPF interface</td>
<td>netdev_ospf_interface</td>
<td>'vlan &lt;#ID&gt;'</td>
<td>netdev_ospf_interface{ 'vlan 4': ensure =&gt; present, ospf_area_mode=&gt;'stub'}</td>
</tr>
<tr>
<td>OSPF area</td>
<td>netdev_ospf_area</td>
<td>Valid area ID (representing an IP)</td>
<td>netdev_ospf_area{ '10': ensure =&gt; present, ospf_area_mode=&gt;'stub'}</td>
</tr>
<tr>
<td>OSPF router</td>
<td>netdev_router_ospf</td>
<td>Currently only supports 'default'</td>
<td>netdev_router_ospf{ 'default': ensure =&gt; present }</td>
</tr>
<tr>
<td>Protocol</td>
<td>mlnx_protocol</td>
<td>ip_routing, lldp, snmp, spanning_tree</td>
<td>mlnx_protocol{ 'ip_routing': ensure =&gt; present}</td>
</tr>
<tr>
<td>Fetched image</td>
<td>mlnx_fetched_img</td>
<td>The image file name</td>
<td>mlnx_fetched_image{ 'image-PPC_M460EX-3.3.4300.img': ensure =&gt; present}</td>
</tr>
<tr>
<td>Installed image</td>
<td>mlnx_installed_img</td>
<td>The image version name</td>
<td>mlnx_installed_img{ '3.3.4300': ensure =&gt; present}</td>
</tr>
</tbody>
</table>
4.15.7 Troubleshooting

This section presents common issues that may prevent the switch from connecting to the puppet server.

4.15.7.1 Switch and Server Clocks are not Synchronized

This can be fixed by using NTP to synchronize the clocks at the switch (using the CLI command `ntp`) and at the server (e.g. using `ntpd`).

4.15.7.2 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).

4.15.7.3 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`).
### puppet-agent

#### 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.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>hostname</th>
<th>Puppet server hostname. Free string may be entered.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>puppet</td>
<td></td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Config Puppet</td>
<td></td>
</tr>
<tr>
<td>History</td>
<td>3.3.4200</td>
<td></td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
<td></td>
</tr>
</tbody>
</table>
| Example            | switch (config puppet-agent) # master-hostname my-puppet-server-host-name
switch (config puppet-agent) # |

Related Commands

Notes
enable

```
failover enable
no failover enable
```

Enables the puppet server on the switch.
The no form of the command disables the puppet server.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>Disabled</td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Config Puppet</td>
</tr>
<tr>
<td>History</td>
<td>3.3.4200</td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
</tr>
</tbody>
</table>
| 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.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>time</th>
<th>Can be in seconds (&quot;30&quot; or &quot;30s&quot;), minutes (&quot;30m&quot;), hours (&quot;6h&quot;), days (&quot;2d&quot;), or years (&quot;5y&quot;).</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>30m</td>
<td></td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Config Puppet</td>
<td></td>
</tr>
<tr>
<td>History</td>
<td>3.3.4302</td>
<td></td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
<td></td>
</tr>
<tr>
<td>Example</td>
<td>switch (config puppet-agent) # run-interval 40m</td>
<td></td>
</tr>
<tr>
<td></td>
<td>switch (config puppet-agent) #</td>
<td></td>
</tr>
<tr>
<td>Related Commands</td>
<td>show puppet-agent</td>
<td></td>
</tr>
<tr>
<td>Notes</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>


**restart**

**puppet-agent restart**

Restarts the puppet agent.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>N/A</td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Config Puppet</td>
</tr>
<tr>
<td>History</td>
<td>3.3.4200</td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
</tr>
</tbody>
</table>

**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.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>N/A</td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Any Command Mode</td>
</tr>
<tr>
<td>History</td>
<td>3.3.4200</td>
</tr>
<tr>
<td></td>
<td>3.3.4302</td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
</tr>
</tbody>
</table>

```
switch (config puppet-agent) # show puppet-agent
Puppet agent is disabled
Puppet master hostname: puppet
Run interval: 40m
```

## 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.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>continuous</td>
<td>Puppet agent log messages as they arrive.</td>
</tr>
<tr>
<td>files</td>
<td>Displays archived Puppet agent log files.</td>
</tr>
<tr>
<td>matching</td>
<td>Displays Puppet agent log that match a given string.</td>
</tr>
<tr>
<td>not</td>
<td>Displays Puppet agent log that do not meet a certain string.</td>
</tr>
<tr>
<td>string</td>
<td>Free string.</td>
</tr>
</tbody>
</table>

Default N/A

Configuration Mode Any Command Mode

History 3.3.4200

Role admin

Example

```
switch (config puppet-agent) # show puppet-agent log
Mon Nov 04 11:52:42 +0000 2013 Puppet (notice): Starting Puppet client version 3.2.3
Mon Nov 04 11:52:44 +0000 2013 Puppet (warning): Unable to fetch my node definition, but the agent run will continue:
Mon Nov 04 11:52:44 +0000 2013 Puppet (warning): Could not intern from pson: source '#<Puppet::Node:0x7f' not in PSON!
Mon Nov 04 11:53:21 +0000 2013 /Netdev_vlan[Vlan104]/ensure (notice): created
Mon Nov 04 11:53:22 +0000 2013 /Netdev_vlan[Vlan101]/ensure (notice): created
Mon Nov 04 11:53:23 +0000 2013 /Netdev_vlan[Vlan102]/ensure (notice): created
Mon Nov 04 11:53:24 +0000 2013 /Netdev_vlan[Vlan103]/ensure (notice): created
Mon Nov 04 11:53:40 +0000 2013 /Netdev_l2_interface[ethernet 1/6]/untagged_vlan (notice): untagged_vlan changed 'default' to 'Vlan103'
Mon Nov 04 11:53:43 +0000 2013 /Netdev_l2_interface[ethernet 1/7]/untagged_vlan (notice): untagged_vlan changed 'default' to 'Vlan103'
Mon Nov 04 11:53:48 +0000 2013 /Netdev_vlan[Vlan100]/ensure (notice): created
Mon Nov 04 11:53:48 +0000 2013 /Netdev_l2_interface[ethernet 1/5]/vlan_tagging (notice): vlan_tagging changed "enable" to "disable"
Mon Nov 04 11:53:48 +0000 2013 /Netdev_l2_interface[ethernet 1/5]/tagged_vlans (notice): tagged_vlans changed "[]" to 
'"[Vlan100,Vlan101,Vlan102]"
Mon Nov 04 11:53:51 +0000 2013 /Netdev_l2_interface[ethernet 1/2]/untagged_vlan (notice): untagged_vlan changed "default" to "Vlan100"
Mon Nov 04 11:53:56 +0000 2013 /Netdev_l2_interface[ethernet 1/3]/untagged_vlan (notice): untagged_vlan changed "default" to "Vlan100"
Mon Nov 04 11:53:56 +0000 2013 /Netdev_l2_interface[ethernet 1/3]/tagged_vlans (notice): tagged_vlans changed "[]" to '"Vlan100,Vlan101,Vlan102"
Mon Nov 04 11:53:56 +0000 2013 /Netdev_l2_interface[ethernet 1/2]/tagged_vlans (notice): tagged_vlans changed "[]" to '"Vlan100,Vlan101,Vlan102"
Mon Nov 04 11:53:56 +0000 2013 /Netdev_l2_interface[ethernet 1/1]/tagged_vlans (notice): tagged_vlans changed "[]" to '"Vlan100,Vlan101,Vlan102"
Mon Nov 04 11:53:56 +0000 2013 /Netdev_l2_interface[ethernet 1/1]/untagged_vlan (notice): untagged_vlan changed "default" to "Vlan100"
Mon Nov 04 11:53:56 +0000 2013 /Netdev_l2_interface[ethernet 1/4]/vlan_tagging (notice): vlan_tagging changed "enable" to "disable"
Mon Nov 04 11:53:56 +0000 2013 /Netdev_l2_interface[ethernet 1/4]/tagged_vlans (notice): tagged_vlans changed "[]" to '"Vlan100,Vlan101,Vlan102"
Mon Nov 04 11:53:56 +0000 2013 /Netdev_l2_interface[ethernet 1/4]/untagged_vlan (notice): untagged_vlan changed "default" to "Vlan100"
Mon Nov 04 11:53:58 +0000 2013 Puppet (notice): Finished catalog run in 47.90 seconds
switch (config puppet-agent) 
```

Related Commands

Notes
4.16 Virtual Machine

A virtual machine (VM) on a switch is added to allow additional OS to run on top of the switch. The VM OS can connect through mgmt0 interface to the switch system’s management interface. In addition, the VM is also connected to the out-of-band network. This allows it to communicate through the network and to control the switch management software.

The number of VMs that may run on a system is user-configurable and also relies on resource availability.

Each VM consumes the following resources:

- Memory
- Processing power which is not policed (the user may determine the core to be used)
- MACs which are required for each vNIC (user configurable)

4.16.1 Virtual Machine Configuration

➢ To configure a VM:

The example below installs Ubuntu 14 and defines 3GB storage with 512MB memory (default) using the first core of the switch system (default) through mgmt0 interface (default) with an auto-generated MAC (default).

Step 1. Enable the VM feature. Run:

```
switch (config) # virtual-machine enable
```

Step 2. Create a VM. Run:

```
switch (config) # virtual-machine host my-vm
switch (config virtual-machine host my-vm) #
```

Step 3. Define storage for the VM. Run:

```
switch (config virtual-machine host my-vm) # storage create disk size-max 3000
100.0% [###################################################]  
Created empty virtual disk volume 'vdisk001.img' in pool 'default' 
Device attached to drive number 1.  
switch (config virtual-machine host my-vm) #
```
Step 4. Display the VM parameters (notice boldface). Run:

```
switch (config virtual-machine host my-vm) # show virtual-machine host my-vm
VM 'my-vm'
  Status:       shut off       Architecture:     x86_64
  VCPU used:    0 sec          Number of VCPUs:  1
  Boot order:   hd, cdrom      Memory size:      512 MB
  Consoles:     text, graphics
  Storage:
    IDE bus, drive 1: default/vdisk001.img (3000 MB capacity)
  Interfaces:
    1: on bridge 'mgmt0'        address unknown (MAC 52:54:00:2F:89:69)
switch (config virtual-machine host my-vm) # exit
```

Step 5. Import the VM image. Run:

```
switch (config) # virtual-machine volume fetch url scp://root@<ip>/.../ubuntu-14.04-server-amd64.iso
Password (if required): *************
100.0% [#################################################################]
switch (config virtual-machine host my-vm) # install cdrom file ubuntu-14.04-server-amd64.iso
```

Step 6. Install the imported image. Run:

```
switch (config) # virtual-machine host my-vm
switch (config virtual-machine host my-vm) # install cdrom file ubuntu-14.04-server-amd64.iso
```

Step 7. Switch to a different terminal, and run the following command to connect VNC viewer to the VM:

```
$ vncviewer -via admin@<switch IP> 127.0.0.1:0
...
Mellanox MLNX-OS Switch Management
Password: *************
```

Continue VM installation from the VNC prompt.

The switch prompt is unresponsive pending a successful VM installation. Successful VM installation is indicated by the reboot of the VM.

VM IP is determined by DHCP configuration according to the MAC address in Step 4.
To verify VM configuration, run:

```
switch {config virtual-machine host my-vm} # show virtual-machine host my-vm
VM 'my-vm'
  Status: running  Architecture: x86_64
  VCPU used: 12 min 27.440 sec  Number of VCPUs: 1
  Boot order: cdrom, hd  Memory size: 512 MB
  Consoles: text, graphics
  Storage:
    IDE bus, drive 1: default/vdisk001.img (3000 MB capacity)
    IDE bus, drive 2: default/ubuntu-14.04-server-amd64.iso (564 MB capacity) READ-ONLY
  Interfaces:
    1: on bridge 'mgmt0'  address unknown  (MAC 52:54:00:2F:89:69)
```

To perform a VM installation from a USB stick:

USB stick with supported VM image should be supplied to the user by Mellanox.

Step 1. Insert the USB stick (supplied by Mellanox) to the USB port of your switch system.

Step 2. Decide on a name for the VM (e.g. “my_vm”).

Step 3. Decide on the network configuration of the VM.
   - Use DHCP or alternately use static IP definitions
   - Assign a MAC address or alternately use the default MAC address

Step 4. Launch the full installation of the VM with the network definitions of your choice.

For a configuration example, please refer to Section B.1, “Deploying Mellanox NEO™ on a MLNX-OS® Switch,” on page 1331.
4.16.2 Commands

4.16.2.1 Config

**virtual-machine enable**

```
virtual-machine enable
no virtual-machine enable
```

Enables VM feature on the switch.
The no form of the command disables VM feature on the switch.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>no virtual-machine enable</td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Config</td>
</tr>
<tr>
<td>History</td>
<td>3.4.0000</td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
</tr>
<tr>
<td>Example</td>
<td>switch (config) # virtual-machine enable</td>
</tr>
</tbody>
</table>

**Related Commands**

**Notes**
virtual-machine host

virtual-machine host <vm-name>
no virtual-machine host <vm-name>

Creates a VM, or enters its configuration context if it already exists. The no form of the command removes the VM with the specified name.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vm-name</td>
<td>Configures a name for the VM</td>
</tr>
</tbody>
</table>

| Default | N/A |

<table>
<thead>
<tr>
<th>Configuration Mode</th>
<th>Config</th>
</tr>
</thead>
</table>

| History | 3.4.0000 |

| Role | admin |

| Example | switch (config)# virtual-machine host my-vm  
          | switch (config virtual-machine host my-vm)# |

| Related Commands | |

| Notes | |
## arch

**arch {i386 | x86_64}**

Configures VM CPU architecture.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>i386</th>
<th>32-bit x86 CPU architecture</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>x86_64</td>
<td>64-bit x86 CPU architecture</td>
</tr>
</tbody>
</table>

**Default**

x86_64

**Configuration Mode**

Config Virtual Machine Host

**History**

3.4.0000

**Role**

admin

**Example**

```
switch (config virtual-machine host my-vm)# arch i386
```

**Related Commands**

virtual-machine

**Notes**
**comment**

```
comment <string>
no comment
```

Configures a comment describing the VM.
The no form of the command deletes the configured comment.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Syntax Description</td>
<td>string</td>
<td>Free string</td>
</tr>
<tr>
<td>Default</td>
<td>N/A</td>
<td></td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Config Virtual Machine Host</td>
<td></td>
</tr>
<tr>
<td>History</td>
<td>3.4.0000</td>
<td></td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
<td></td>
</tr>
<tr>
<td>Example</td>
<td>switch (config virtual-machine host my-vm)# comment “example VM”</td>
<td></td>
</tr>
<tr>
<td>Related Commands</td>
<td>virtual-machine</td>
<td></td>
</tr>
<tr>
<td>Notes</td>
<td>To configure a multi-word string, the string must be placed within quotation marks.</td>
<td></td>
</tr>
</tbody>
</table>
console

console {connect [graphics | text [force]] | graphics vnc | text tty}
no console {graphics vnc | text tty}

Configures or connects to a text or graphical console. The no form of the command clears console settings.

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>connect</td>
<td>Connects to the text console unless specified otherwise:</td>
</tr>
<tr>
<td></td>
<td>• graphics – connects to the X11 graphical (VNC) console</td>
</tr>
<tr>
<td></td>
<td>• text – connects to the text console</td>
</tr>
<tr>
<td>graphics vnc</td>
<td>Enables graphical (VNC) console access</td>
</tr>
<tr>
<td>text tty</td>
<td>Enables TTY text console access</td>
</tr>
</tbody>
</table>

**Default**

Graphical and textual consoles are enabled

**Configuration Mode**

Config Virtual Machine Host

**History**

3.4.0000

**Role**

admin

**Example**

switch (config virtual-machine host my-vm)# console connect text

**Related Commands**

virtual-machine

ssh server x11-forwarding enable

**Notes**

- To exit the text console press Ctrl-6 (or Ctrl-Shift-6)
- If the guest OS is not configured to receive input from a serial console (ttyS0), the VM console becomes unresponsive when connected to.
- To view the graphical console, X display must be enabled. There are two options to activate it, the command `vncviewer -via admin@<switch-chIP> 127.0.0.1:<VNC display num>` (which is run from an external Linux host) and the command `ssh server x11-forwarding enable` (which is run from within the switch and requires that you log out and log back in again using `ssh -X`). The latter command weakens the switch security, therefore, it is recommended to opt for the second option. The VNC display num parameter may be procured by running the command `show virtual-machine <vm-name> detail`. 
install

install {cancel | cdrom [pool <pool-name>] | file <volume-name> | connect-console <console-type> | disk-overwrite | timeout {<minutes> | none}}

Installs an operating system onto this VM (temporarily attach a CD and boot from it).

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>cancel</td>
<td>Cancels an install already in progress</td>
</tr>
<tr>
<td>cdrom</td>
<td>Installs an operating system from a CD-ROM (ISO) image</td>
</tr>
<tr>
<td>pool &lt;pool-name&gt;</td>
<td>Configures storage pool in which to find image to install: • default • usb</td>
</tr>
<tr>
<td>file &lt;volume-name&gt;</td>
<td>Specifies CD-ROM (ISO) image from which to install</td>
</tr>
<tr>
<td>connect-console &lt;console-type&gt;</td>
<td>Connects to the console during installation. The types may be: • text – text console • graphics – graphical console</td>
</tr>
<tr>
<td>disk-overwrite</td>
<td>Installs even if primary target volume is not empty</td>
</tr>
<tr>
<td>timeout {&lt;minutes&gt;</td>
<td>Configures a timeout for installation in minutes (default is no timeout).</td>
</tr>
<tr>
<td>none}</td>
<td></td>
</tr>
</tbody>
</table>

Default N/A

Configuration Mode Config Virtual Machine Host

History 3.4.0000

Role admin

Example switch (config virtual-machine host my-vm)# install cdrom pool usb file <image>

Related Commands virtual-machine

Notes The default pool from which the system installs the ISO image is the /var/partition in the switch.
install-from-usb

install-from-usb [ip-address <ip-address> <mask> default-gateway <gw-ip> [mac <mac-address>]]

Installs a VM including resource allocation and network configurations from a VM image file located on a USB stick.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip-address</td>
<td>The IP address to configure for the installed VM</td>
</tr>
<tr>
<td>mask</td>
<td>The IP mask to configure to the installed VM</td>
</tr>
<tr>
<td></td>
<td>Format example: /24 or 255.255.255.0</td>
</tr>
<tr>
<td></td>
<td>Note that a space is required between the IP</td>
</tr>
<tr>
<td></td>
<td>address and the netmask length</td>
</tr>
<tr>
<td>default-gateway</td>
<td>The IP address of the default gateway to configure</td>
</tr>
<tr>
<td></td>
<td>for the installed VM</td>
</tr>
<tr>
<td>mac</td>
<td>The MAC address to configure for the installed VM</td>
</tr>
<tr>
<td></td>
<td>(e.g. ff:ee:dd:cc:bb:aa)</td>
</tr>
</tbody>
</table>

Default: N/A

Configuration Mode: Config Virtual Machine Host

History: 3.6.2002

Role: admin

Example:

```
switch (config virtual-machine host my-vm)# install-from-usb
100.0% [##############################################################]
VM host my-vm MAC is: aa:bb:cc:dd:ee:ff
switch (config virtual-machine host my-vm)#
```

Related Commands: virtual-machine

Notes: USB stick supplied by Mellanox must be inserted into the USB port of the switch system prior to running this command.
interface

interface <id> {bridge <bridge> | macaddr <mac> | model <model> | name <name>}

Configures virtual interfaces.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;id&gt;</td>
<td>Interface ID number (1-8 permitted)</td>
</tr>
<tr>
<td>bridge &lt;bridge&gt;</td>
<td>Configures bridge for this interface (i.e. mgmt0 or mgmt1)</td>
</tr>
<tr>
<td>macaddr &lt;mac&gt;</td>
<td>Configures MAC address (e.g. ff:ee:dd:cc:bb:aa)</td>
</tr>
<tr>
<td>model &lt;model&gt;</td>
<td>Configures virtual interface model: • realtek-8139 – Realtek 8139 (default) • virtio – Virtual IO</td>
</tr>
<tr>
<td>name &lt;name&gt;</td>
<td>Configures virtual interface name. The name must begin with “vif”.</td>
</tr>
</tbody>
</table>

Default N/A

Configuration Mode Config Virtual Machine Host

History 3.4.0000

Role admin

Example switch (config virtual-machine host my-vm)# interface 1 model virtio

Related Commands virtual-machine

Notes
memory

memory <MB>

Configures memory allowance.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>MB</th>
<th>Size in megabytes.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>512MB</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Configuration Mode</th>
<th>Config Virtual Machine Host</th>
</tr>
</thead>
<tbody>
<tr>
<td>History</td>
<td>3.4.0000</td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
</tr>
<tr>
<td>Example</td>
<td>switch (config virtual-machine host my-vm)# memory 1024</td>
</tr>
<tr>
<td>Related Commands</td>
<td>virtual-machine</td>
</tr>
<tr>
<td>Notes</td>
<td>It is recommended not to allocate more than 1GB of memory per VM.</td>
</tr>
</tbody>
</table>
# power

```
power {cycle [force | connect-console [graphics | text]] | off [force] | on [connect-console [graphics | text]]}
```

Turns the VM on or off, or other related options.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>cycle</td>
<td>Powers the VM down and then on again immediately</td>
</tr>
<tr>
<td>force</td>
<td>Forces an action on the system.</td>
</tr>
</tbody>
</table>
| connect-console <console-type> | Connects to the console after power-on. The types may be:  
  • text – text console  
  • graphics – graphical console |
| off                | Powers down the VM |
| on                 | Powers on VM: |

<table>
<thead>
<tr>
<th>Default</th>
<th>N/A</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Configuration Mode</th>
<th>Config Virtual Machine Host</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>History</th>
<th>3.4.0000</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Role</th>
<th>admin</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Example</th>
<th>switch (config virtual-machine host my-vm)# power cycle force</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Related Commands</th>
<th>virtual-machine</th>
</tr>
</thead>
</table>

Notes
storage create

storage create disk [drive-number <number> | file <filename> | mode {read-only | read-write} | pool <pool-name> | size-max <MB>]

Creates a new storage device for the VM, with an automatically assigned name.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>create disk</td>
<td>Creates a new virtual disk image for this VM.</td>
</tr>
<tr>
<td>drive-number &lt;number&gt;</td>
<td>Specifies the drive number to be assigned to the volume. Insert “new” to assign a new drive number to the volume.</td>
</tr>
<tr>
<td>file &lt;filename&gt;</td>
<td>Specifies filename for new volume to be created</td>
</tr>
<tr>
<td>mode {read-only</td>
<td>read-write}</td>
</tr>
<tr>
<td>pool &lt;pool-name&gt;</td>
<td>Specifies storage pool in which to create new volume</td>
</tr>
<tr>
<td>size-max &lt;MB&gt;</td>
<td>Specifies maximum disk capacity in megabytes</td>
</tr>
</tbody>
</table>

Default N/A

Configuration Mode Config Virtual Machine Host

History 3.4.0000

Role admin

Example switch (config virtual-machine host my-vm)# storage create disk size-max 2000

Related Commands virtual-machine

Notes
storage device

storage device [bus ide] drive-number <number> [mode {read-only | read-write}] source {{pool <pool-name>} file <filename>}
no storage device [bus ide] drive-number <id>

Modifies existing storage device, or create a new one with a specific name. The no form of the command removes a storage device from the VM.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Device Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>device</td>
<td>Modifies existing storage device, or creates a new one with a specific name</td>
</tr>
<tr>
<td>bus ide</td>
<td>Configures bus type to IDE</td>
</tr>
<tr>
<td>drive-number &lt;number&gt;</td>
<td>Selects device to configure by drive number</td>
</tr>
</tbody>
</table>
| mode {read-only | read-write} | Configures the device mode:  
|                              | • read-only – sets the read-only attribute of the volume  
|                              | • read-write – sets the read-write attribute of the volume                        |
| source                      | Specifies where the data for this volume resides                                 |
| file <filename>             | Specifies the filename for this volume                                            |
| pool <pool-name> file <filename> | Specifies the storage pool for this volume                                       |

<table>
<thead>
<tr>
<th>Default</th>
<th>N/A</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Configuration Mode</th>
<th>Config Virtual Machine Host</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>History</th>
<th>3.4.0000</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Role</th>
<th>admin</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Example</th>
<th>switch (config virtual-machine host my-vm)# storage create disk bus ide</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Related Commands</th>
<th>virtual-machine</th>
</tr>
</thead>
</table>

| Notes | |
**vcpus**

`vcpus {count <count> | vcpu <vcpu> pin <cpu-list> [<cpu-list>]}`  
`no vcpus {pin | vcpu <vcpu> pin}`

Specifies virtual CPUs.  
The no form of the command removes certain CPU configuration.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>count &lt;count&gt;</td>
<td>Specifies the number of virtual CPUs</td>
</tr>
<tr>
<td>vcpu &lt;vcpu&gt;</td>
<td>Specifies options for a particular virtual CPU</td>
</tr>
<tr>
<td>pin &lt;cpu-list&gt;</td>
<td>Specifies physical CPUs to pin to this vCPU</td>
</tr>
</tbody>
</table>

| Default | N/A |

**Configuration Mode**: Config Virtual Machine Host  
**History**: 3.4.0000  
**Role**: admin  
**Example**:  
```
switch (config virtual-machine host my-vm)# vcpus count 1
```

**Related Commands**

**Notes**
virtual-machine volume fetch url

```
virt volume fetch url <download-url> [filename <filename> | pool <pool-name> filename <filename>]
```

Fetches volume image from a remote host.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>download-url</td>
<td>Specifies URL from which to fetch a volume. Format: http, https, ftp, tftp, scp and sftp are supported (e.g. scp://username[:password]@hostname/path/filename)</td>
</tr>
<tr>
<td>filename &lt;filename&gt;</td>
<td>Specifies new filename for fetched volume image</td>
</tr>
<tr>
<td>pool-name &lt;pool-name&gt;</td>
<td>Specifies storage pool for fetched volume image</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Default</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuration Mode</td>
<td>Config Virtual Machine Host</td>
</tr>
<tr>
<td>History</td>
<td>3.4.0000</td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
</tr>
</tbody>
</table>

Example

```
switch (config) # virtual-machine volume fetch scp://admin[:admin-pass]@<hostname/path/filename>
```

Related Commands

Notes
## virt volume file

```bash
virt volume file <name> {create disk size-max <MB> | move {new-name <new-name> | pool <pool-name> new-name <new-name>} | upload <upload-url>}
no virt volume file <volume-name>
```

Specifies name of volume file to manage.
The no form of the command deletes the volume file.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>file &lt;name&gt;</td>
<td>Specifies name of volume file to manage</td>
</tr>
<tr>
<td>create</td>
<td>Creates a new volume file under this name</td>
</tr>
<tr>
<td>disk size-max &lt;MB&gt;</td>
<td>Specifies maximum capacity of virtual disk to cre-</td>
</tr>
<tr>
<td>move</td>
<td>Moves or renames this volume</td>
</tr>
<tr>
<td>new-name &lt;filename&gt;</td>
<td>Specifies a name for the destination file</td>
</tr>
<tr>
<td>pool &lt;pool-name&gt; new-name &lt;filename&gt;</td>
<td>Specifies a storage pool for the copy</td>
</tr>
<tr>
<td>upload &lt;upload-url&gt;</td>
<td>Uploads this volume file to a remote host. Format:ftp, tftp, scp and sftp are supported (e.g. scp://username[:password]@hostname/path/file-name)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Default</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuration Mode</td>
<td>Config Virtual Machine Host</td>
</tr>
<tr>
<td>History</td>
<td>3.4.0000</td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
</tr>
<tr>
<td>Example</td>
<td>switch (config) # virt volume file my-vm_file create cdrom extract cdrom1</td>
</tr>
</tbody>
</table>

### Notes
### show virtual-machine configured

**show virtual-machine configured**

Displays global virtualization configuration.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>N/A</td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Any Command Mode</td>
</tr>
<tr>
<td>History</td>
<td>3.4.0000</td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
</tr>
</tbody>
</table>

**Example**

```
switch (config) # show virtual-machine configured
Virtualization enabled: yes
Virtual machines: 2 configured
Virtual networks: 0 configured
switch (config) #
```

**Related Commands**

**Notes**
show virtual-machine host

show virtual-machine host [<vm-name>]

Displays status for this VM.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vm-name</td>
<td>The name of the VM.</td>
</tr>
</tbody>
</table>

Default: N/A

Configuration Mode: Any Command Mode

History: 3.4.0000

Role: admin

Example:

```
switch (config) # show virtual-machine host my-vm
VM 'my-vm'
  Status:       shut off                   Architecture:     x86_64
  VCPU used:    0 sec                      Number of VCPUs:  1
  Boot order:   hd, cdrom                  Memory size:      512 MB
  Consoles:     text, graphics
  Storage:
    IDE bus, drive 1: default/vdisk001.img (3000 MB capacity)
  Interfaces:
    1: on bridge 'mgmt0'            address unknown   (MAC 52:54:00:2F:89:69)
switch (config) #
```

Related Commands

Notes:
If the command is run in the middle of an installation, the following banner appears:

*** INSTALL IN PROGRESS: begun <time> ago ***
**show virtual-machine host configured**

```
show virtual-machine host <vm-name> configured [detail]
```

Displays configuration for this VM.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vm-name</td>
<td>The name of the VM.</td>
</tr>
<tr>
<td>detail</td>
<td>Displays detailed configuration for this VM.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Default</th>
<th>N/A</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Configuration Mode</th>
<th>Any Command Mode</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>History</th>
<th>3.4.0000</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Role</th>
<th>admin</th>
</tr>
</thead>
</table>

**Example**

```
switch (config) # show virtual-machine host my-vm configured detail
VM "my-vm"
  UUID:                0a177a99-f780-5951-877a-bd660e12e5db
  Text console:        enabled
  Graphics console:    enabled
  Auto-power:          last
  Boot order:          hd, cdrom
  Architecture:        x86_64
  Memory size:         512 MB
  Features:            ACPI, APIC
  Number of VCPUs:     1
    (No VCPUs pinned)

  Storage:
    IDE bus, drive 1

  Source pool:       default
  Source file:       vdisk001.img (3000 MB capacity)
  Mode:              read-write

  Interfaces:
    Interface 1

    Name:         vif1
    MAC address:  52:54:00:2F:89:69
    Model:        realtek-8139
    Bound to:     bridge 'mgmt0'

switch (config) #
```

**Related Commands**

**Notes**
show virtual-machine host detail

show virtual-machine host <vm-name> detail

Displays detailed status for this VM.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Default</th>
<th>Configuration Mode</th>
<th>History</th>
<th>Role</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>vm-name</td>
<td>N/A</td>
<td>Any Command Mode</td>
<td>3.4.0000</td>
<td>admin</td>
<td></td>
</tr>
</tbody>
</table>

Example

```
switch (config) # show virtual-machine host my-vm detail
VM 'my-vm'
Status: shut off
UUID: 0a177a99-f780-5951-877a-bd660e12e5db
Text console: enabled
Device: N/A
Graphics console: enabled
VNC display num: N/A
Boot order: hd, cdrom
Architecture: x86_64
Memory size: 512 MB
Features: ACPI, APIC
Number of VCPUs: 1
(State of individual VCPUs unavailable when VM is powered off)
Storage:
IDE bus, drive 1
Source pool: default
Source file: vdisk001.img (3000 MB capacity)
Mode: read-write
Device type: disk
Read requests: N/A
Read bytes: N/A
Write requests: N/A
Write bytes: N/A
Interfaces:
Interface 1
Name: vif1
MAC address: 52:54:00:2F:89:69
Model: realtek-8139
Bound to: bridge 'mgmt0'
IP address:
RX bytes: 0 TX bytes: 0
RX packets: 0 TX packets: 0
RX errors: 0 TX errors: 0
RX drop: 0 TX drop: 0
```

switch (config) #
<table>
<thead>
<tr>
<th>Related Commands</th>
</tr>
</thead>
<tbody>
<tr>
<td>Notes</td>
</tr>
</tbody>
</table>
show virtual-machine install

show virtual-machine host <vm-name> install

Displays status of installation of guest OS.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>vm-name</th>
<th>The name of the VM.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>N/A</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Configuration Mode</th>
<th>Any Command Mode</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>History</th>
<th>3.4.0000</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Role</th>
<th>admin</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Example</th>
</tr>
</thead>
</table>
| switch (config) # show virtual-machine host my-vm install
  Install status for VM 'my-vm'
  Install in progress, begun 2 minutes 28 seconds ago.
  No previous install information available.
  switch (config) # |

<table>
<thead>
<tr>
<th>Related Commands</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Notes</th>
</tr>
</thead>
</table>
show virtual-machine interface

show virtual-machine host <vm-name> interface [brief | configure]

Displays full status of all interfaces for this VM.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vm-name</td>
<td>The name of the VM.</td>
</tr>
<tr>
<td>brief</td>
<td>Displays brief status of all interfaces for this VM.</td>
</tr>
<tr>
<td>configure</td>
<td>Displays configuration of all interfaces for this VM.</td>
</tr>
</tbody>
</table>

**Default**: N/A

**Configuration Mode**: Any Command Mode

**History**: 3.4.0000

**Role**: admin

**Example**
```
switch (config) # show virtual-machine host my-vm interface
Interface 1
    Name:         vif1
    MAC address:  52:54:00:2F:89:69
    Model:        realtek-8139
    Bound to:     bridge 'mgmt0'
    IP address:
      RX bytes:   0                     TX bytes:   0
      RX packets: 0                     TX packets: 0
      RX errors:  0                     TX errors:  0
      RX drop:    0                     TX drop:    0

switch (config) #
```

**Related Commands**

**Notes**
**show virtual-machine storage**

*show virtual-machine host <vm-name> storage*

Displays statistics for attached storage.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>vm-name</th>
<th>The name of the VM.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>N/A</td>
<td></td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Any Command Mode</td>
<td></td>
</tr>
<tr>
<td>History</td>
<td>3.4.0000</td>
<td></td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
<td></td>
</tr>
</tbody>
</table>

**Example**

```
switch (config) # show virtual-machine host my-vm storage
Storage for VM 'my-vm'
  IDE bus, drive 1
  Source pool:   default
  Source file:   vdisk001.img (3000 MB capacity)
  Mode:          read-write
  Device type:   disk
  Read requests: N/A
  Read bytes:    N/A
  Write requests: N/A
  Write bytes:   N/A

switch (config) #
```

**Related Commands**

**Notes**
4.17 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.

### 4.17.1 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-if 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   : -
```
4.17.2 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
  ```

4.17.3 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.
### 4.17.4 Commands

**ip filter enable**  
**ipv6 filter enable**

```plaintext
{ip | ipv6} filter enable
no {ip | ipv6} filter enable
```

Enables IP filtering.  
The no form of the command disables IP filtering.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>Disabled</td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Config</td>
</tr>
<tr>
<td>History</td>
<td>3.5.1000</td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
</tr>
</tbody>
</table>
| Example            | ```switch (config) # ip filter enable
switch (config) #``` |
| Related Commands   | N/A |
| Notes              | It is recommended to run this command only after configuring all of the IP table filter parameters. |
### ip filter chain policy
### ipv6 filter chain policy

```plaintext
{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.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>chain_name</td>
<td>Selects a chain for which to add or modify a filter:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- input – input chain or ingress interfaces</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- output – output chain or egress interfaces</td>
<td></td>
</tr>
<tr>
<td>accept</td>
<td>Accepts all traffic by default for this chain</td>
<td></td>
</tr>
<tr>
<td>drop</td>
<td>Drops all traffic by default for this chain</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Default</th>
<th>Accept for input and output chains</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Configuration Mode</strong></td>
<td>Config</td>
</tr>
<tr>
<td><strong>History</strong></td>
<td>3.5.1000</td>
</tr>
<tr>
<td><strong>Role</strong></td>
<td>admin</td>
</tr>
</tbody>
</table>

**Example**

```plaintext
switch (config) # ipv6 filter chain input policy accept
switch (config) #
```

**Related Commands**

N/A

**Notes**
ip filter chain rule target
ipv6 filter chain rule target

{ip | ipv6} filter chain <chain_name> rule <oper> target <target> [<param>]
no {ip | ipv6} filter chain <chain_name> rule {<number> | all}

Inserts rule before specified rule number.
The no form of the command deletes rule for a specific chain.

| Syntax Description | chain_name | A chain to which to add or modify a filter:
|                    |           | • input – input chain or ingress interfaces
|                    |           | • output – output chain or egress interfaces
| rule               |           | • append tail – appends operation to the bottom
|                    |           | of operation list
|                    |           | • insert <oper_num> – inserts operation at specified
|                    |           | position (existing operation at that position
|                    |           | moves back in the list)
|                    |           | • modify <oper_num> – modifies existing operation
|                    |           | at specified position. Only the parameters
|                    |           | specified in this invocation are altered; every-
|                    |           | thing else is left untouched.
|                    |           | • move <oper_num1> to <oper_num2> – moves
|                    |           | one operation to another place in the operation
|                    |           | list
|                    |           | • set <oper_num> – sets operation at specified
|                    |           | position (overwrites existing)
| target             |           | • accept – allows the packets that match the rule
|                    |           | into the management plane
|                    |           | • drop – drops packets that match the rule
|                    |           | • rate-limit – allows with rate limiting in packets
|                    |           | per sec (PPS)
|                    |           | • reject-with – drops the packet and replies with
|                    |           | an ICMP error message
param

- `comment <text>` – specifies description string for this rule (60 chars max)
- `dest-addr <ip>` – IP matching a specific destination address or address range. A specific IPv4 address can be provided or an entire subnet by giving an address along with netmask in dot notation or as a CIDR notation (e.g. `/24`).
- `not-dest-addr <ip>` – IP not matching a specific destination address range
- `dest-port <port(s)>` – matching a specific destination port or port range
- `not-dest-port <port(s)>` – port not matching a specific destination port or port range
- `dup-delete` – deletes any preexisting duplicates of this rule
- `in-intf` – interface matching a specific inbound interface
- `not-in-intf <if_name>` – interface not matching a specific inbound interface
- `out-intf <if_name>` – matches a specific outbound interface
- `not-out-intf <if_name>` – interface not matching a specific outbound interface
param4 (cont.)

- protocol <if_name> – matches a specific protocol
  - tcp
  - udp
  - icmp
  - all
- not-protocol <protocol> – does not match a specific protocol
  - tcp
  - udp
  - icmp
  - all
- source-addr <ip> – matches a specific source address range
- not-source-addr <ip> – does not match a specific source address range
- source-port <port(s)> – matches a specific source port or port range
- not-source-port <port(s)> – does not match a specific source port or port range
- state – matches packets in a particular state. Possible values:
  - established – packet associated with an established connection which has seen traffic in both directions
  - related – packet that starts a new connection but is related to an existing connection
  - new – packet that starts a new, unrelated connection
  - A combination can be entered separated by commas

Default  
N/A

Configuration Mode  
Config

History  
3.5.1000

Role  
admin

Example

```
switch (config) # ipv6 filter enable chain input rule append tail target drop state related protocol all dup-delete
switch (config) #
```
<table>
<thead>
<tr>
<th>Related Commands</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Notes</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• 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).</td>
</tr>
<tr>
<td></td>
<td>• The port parameter only works in conjunction with TCP and UDP.</td>
</tr>
<tr>
<td></td>
<td>• Setting a “positive” rule removes any corresponding “not-” rules, and vice-versa</td>
</tr>
<tr>
<td></td>
<td>• The “state” parameter is a classification of the packet relative to existing connections</td>
</tr>
<tr>
<td></td>
<td>• 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.</td>
</tr>
</tbody>
</table>
## 4.18 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

### 4.18.1 Ethernet Resources

#### 4.18.1.1 Strict Mode

Table 47 presents the number of resources available for each SwitchX® based node in strict mode.

**Table 47 - Number of Resources per Node in Strict Mode**

<table>
<thead>
<tr>
<th>Resource</th>
<th>Max Resources</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of ACL rules</td>
<td>1488</td>
</tr>
<tr>
<td>Number of MAC addresses</td>
<td>48K</td>
</tr>
<tr>
<td>Number of IPv4 neighbors</td>
<td>2048</td>
</tr>
<tr>
<td>Number of IPv4 UC routes</td>
<td>4094</td>
</tr>
<tr>
<td>Number of IPv4 MC routes</td>
<td>671</td>
</tr>
<tr>
<td>Number of IPv4 (ECMP) UC routes</td>
<td>2K</td>
</tr>
</tbody>
</table>
4.18.1.2 Loose Mode – SwitchX®

Table 48 presents the number of resources available for each SwitchX® based node in loose mode.

Table 48 - Number of Resources per Node in Strict Mode for SwitchX Based Systems

<table>
<thead>
<tr>
<th>Resource</th>
<th>Max Resources</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of ACL rules</td>
<td>5120</td>
</tr>
<tr>
<td>Number of MAC addresses</td>
<td>48K</td>
</tr>
<tr>
<td>Number of IPv4 neighbors</td>
<td>8000</td>
</tr>
<tr>
<td>Number of IPv4 UC routes</td>
<td>10936</td>
</tr>
<tr>
<td>Number of IPv4 MC routes</td>
<td>2047</td>
</tr>
<tr>
<td>Number of IPv4 (ECMP) UC routes</td>
<td>5312</td>
</tr>
</tbody>
</table>

4.18.1.3 Loose Mode – Spectrum™

Table 49 presents the number of resources available for each Spectrum™ based node in strict mode.

Table 49 - Number of Resources per Node in Strict Mode for Spectrum Based Systems

<table>
<thead>
<tr>
<th>Resource</th>
<th>Max Resources</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of ACL rules</td>
<td>5120</td>
</tr>
<tr>
<td>Number of MAC addresses</td>
<td>88K</td>
</tr>
<tr>
<td>Number of IPv4 neighbors</td>
<td>8000</td>
</tr>
<tr>
<td>Number of IPv4 UC routes</td>
<td>10936</td>
</tr>
<tr>
<td>Number of IPv4 MC routes</td>
<td>2047</td>
</tr>
<tr>
<td>Number of IPv4 (ECMP) UC routes</td>
<td>5312</td>
</tr>
</tbody>
</table>
4.18.2 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.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>loose</th>
<th>Sets system resource table mode as loose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>strict</td>
<td>Sets system resource table mode as strict</td>
</tr>
</tbody>
</table>

**Default**

- SwitchX®-2 PPC: Strict
- SwitchX®-2 x86: Loose
- Spectrum™: Loose

**Configuration Mode**

Config

**History**

- 3.5.1000
- 3.6.3004 Added support for Proxy-ARP

**Role**

admin

**Example**

`switch (config) # system resource table strict`

**Related Commands**

N/A

**Notes**

- x86 based systems support strict and loose modes
- Spectrum based systems only support loose mode
- Loose mode is supported on PPC systems only in Proxy-ARP mode
- Transition between modes saves configuration and reloads the system (after user approval)
**show system resource table**

*show system resource table [<table-id>]*

Displays all system resource in-use value.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>table-id</th>
<th>Displays information for a specific in-use resource table</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>N/A</td>
<td></td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Any Command Mode</td>
<td></td>
</tr>
<tr>
<td>History</td>
<td>3.5.1000</td>
<td></td>
</tr>
<tr>
<td></td>
<td>3.6.3004</td>
<td>Added support for Proxy-ARP</td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
<td></td>
</tr>
<tr>
<td>Example</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

```
switch (config) # show system resource table
--------------------------------------
Table-Id    In-Use
--------------------------------------
acl         0         0
ipv4-uc     1         0
ipv4-mc     0         0
ipv4-neigh  0         0
ipv6-uc     0         0
ipv6-mc     0         0
ipv6-neigh  0         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
```

**Related Commands**  N/A

**Notes**
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 40GbE QSFP interfaces as 10GbE (via QSA adapter), the speed must be manually set with the command “speed 10000” 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 14: 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-xxxxR
- 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 manufacture. The parameters include identifier (connector type), cable type, speed and additional inventory attributes.
To display transceiver information of a specific interface, run:

```
switch (config) # show interfaces ethernet 1/60 transceiver
Port 1/60 state
    identifier : QSFP+
    cable/module type : Passive copper, unequalized
    ethernet speed and type: 56GigE
    vendor : Mellanox
    cable length : 1m
    part number : MC2207130-001
    revision : A3
    serial number : MT1238VS04936
switch (config) #
```

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

### 5.1.4 High Power Transceivers

Mellanox switch systems offer high power transceiver (LR4) support in the following ports:

#### Table 50 - LR4/ER4 switch support

<table>
<thead>
<tr>
<th>Transceiver</th>
<th>Speed</th>
<th>Protocol</th>
<th>Power Consumption [W]</th>
<th>Switch OPN</th>
<th>Supported Ports</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>40G</td>
<td>LR4/ER4</td>
<td>3.5</td>
<td>SX1036/SX1700</td>
<td>1, 3, 33, 35</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>SX1024/SX1400</td>
<td>50, 52, 54, 56, 58, 60</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>SX1024/SX1400</td>
<td>50, 52, 54, 56, 58, 60</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>SN2100/SN2410/SN2700</td>
<td>All ports</td>
</tr>
<tr>
<td></td>
<td>100G</td>
<td>LR4</td>
<td>4.5</td>
<td>SN2100</td>
<td>1, 2, 15, 16</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>SN2410</td>
<td>49, 50, 55, 56</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>SN2700</td>
<td>1, 2, 31, 32</td>
</tr>
</tbody>
</table>

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 or 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>[-<slot>/<port>]
```

Enters the Ethernet interface or Ethernet interface range configuration mode.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;slot&gt;/&lt;port&gt;</td>
<td>Ethernet port number.</td>
</tr>
<tr>
<td>subport</td>
<td>Ethernet subport number. to be used in case of split port.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Default</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Config Mode</td>
<td>Config</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>History</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.1.0000</td>
<td>First version</td>
</tr>
<tr>
<td>3.2.1100</td>
<td>Added range support</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Role</th>
<th>admin</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Example</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>switch (config) # interface ethernet 1/1</td>
<td></td>
</tr>
<tr>
<td>switch (config interface ethernet 1/1) # exit</td>
<td></td>
</tr>
<tr>
<td>switch (config) # interface ethernet 1/1-10</td>
<td></td>
</tr>
<tr>
<td>switch (config interface ethernet 1/1-1/10)</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Related Commands</th>
<th>show interfaces ethernet</th>
</tr>
</thead>
</table>

Note
### 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.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>time</th>
<th>Boot delay time in seconds</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Range: 0-600</td>
</tr>
</tbody>
</table>

| Default            | 0 seconds |

**Configuration Mode**
- Config Interface Ethernet
- Config Interface Port Channel
- Config Interface MLAG Port Channel

**History**
3.6.2002

**Role**
admin

**Example**
```
switch (config interface ethernet 1/1) # boot-delay 60
```

**Related Commands**
- show interfaces ethernet

**Note**
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.

**Syntax Description**
- receive | send: receive - ingresses direction, send - egresses direction
- off | on: on - enables IEEE 802.3x link-level flow control for the specified interface on receive or send, off - disables IEEE 802.3x link-level flow control for the specified interface on receive or send
- force: Forces command implementation.

**Default**
receive off, send off

**Configuration Mode**
- Config Interface Ethernet
- Config Interface Port Channel
- Config Interface MLAG Port Channel

**History**
- 3.1.0000
- 3.3.4500: Added MLAG port-channel configuration mode

**Role**
admin

**Example**
```
switch (config interface ethernet 1/1) # flowcontrol receive off
switch (config interface ethernet 1/1) #
```

**Related Commands**
- show interfaces ethernet

**Note**
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.

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>type</td>
<td>qsfp - Port runs at 40000/56000Mbps</td>
</tr>
<tr>
<td></td>
<td>qsfp-split-2 - Port is split and runs at 2X10000Mbps/s</td>
</tr>
<tr>
<td></td>
<td>qsfp-split-4 - Port is split and runs at 4X10000Mbps/s</td>
</tr>
<tr>
<td>force</td>
<td>Force the split operation without asking for user confirmation.</td>
</tr>
</tbody>
</table>

**Default**

QSFP

**Configuration Mode**

Config Interface Ethernet

**History**

3.1.1400

3.5.0000

**Role**

admin

**Example**

```
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) #
```

**Related Commands**

- The affected interfaces should be disabled prior to the operation
- In order to unsplit the interface, use the command with “qsfp”, the speed is set to 40Gb/s “module-type qsfp”
- The following speeds are supported on the different Ethernet interface types:
  - qsfp-split-4 - 1G, 10G, 25G
**mtu**

**mtu <frame-size>**

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

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>frame-size</td>
<td>This value may be 1500-9216 bytes</td>
</tr>
</tbody>
</table>

| Default | 1500 bytes |

<table>
<thead>
<tr>
<th>Configuration Mode</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Config Interface Ethernet</td>
<td></td>
</tr>
<tr>
<td>Config Interface Port Channel</td>
<td></td>
</tr>
<tr>
<td>Config Interface MLAG Port Channel</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>History</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>3.1.0000</td>
<td></td>
</tr>
<tr>
<td>3.3.4500</td>
<td>Added MLAG port-channel configuration mode</td>
</tr>
</tbody>
</table>

| Role | admin |

<table>
<thead>
<tr>
<th>Example</th>
<th>switch (config interface ethernet 1/1) # mtu 9216</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>switch (config interface ethernet 1/1) #</td>
</tr>
</tbody>
</table>

| Related Commands | show interfaces ethernet |

| Note | |

### shutdown

**shutdown**

**no shutdown**

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

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>The interface is enabled.</td>
</tr>
</tbody>
</table>
| Configuration Mode | Config Interface Ethernet  
                        Config Interface Port Channel  
                        Config Interface MLAG Port Channel |
| History            | 3.1.0000  
                        3.3.4500 Added MLAG port-channel configuration mode |
| Role               | admin |
| Example            | switch (config interface ethernet 1/1) # shutdown  
                        switch (config interface ethernet 1/1) # |
| Related Commands   | show interfaces ethernet |
| Note               | |
**description**

```
description <string>
no description
```

Sets an interface description.
The no form of the command returns the interface description to its default value.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>string</th>
<th>40 bytes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>&quot;&quot;</td>
<td></td>
</tr>
</tbody>
</table>

**Configuration Mode**

- Config Interface Ethernet
- Config Interface Port Channel
- Config Interface MLAG Port Channel

**History**

- 3.1.0000
- 3.3.4500 Added MLAG port-channel configuration mode

**Role**

- admin

**Example**

```
switch (config interface ethernet 1/1) # description my-interface
switch (config interface ethernet 1/1)#
```

**Related Commands**

- show interfaces ethernet

**Note**
**Syntax**

```
speed <port speed> [force]
no speed
```

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

**Syntax Description**

<table>
<thead>
<tr>
<th>port speed</th>
<th>The following options are available:</th>
</tr>
</thead>
<tbody>
<tr>
<td>1G or 1000</td>
<td>- 1GbE</td>
</tr>
<tr>
<td>10G or 10000</td>
<td>- 10GbE</td>
</tr>
<tr>
<td>25G or 25000</td>
<td>- 25GbE</td>
</tr>
<tr>
<td>40G or 40000</td>
<td>- 40GbE</td>
</tr>
<tr>
<td>50G or 50000</td>
<td>- 50GbE</td>
</tr>
<tr>
<td>56G or 56000</td>
<td>- 56GbE</td>
</tr>
<tr>
<td>100G or 100000</td>
<td>- 100GbE</td>
</tr>
</tbody>
</table>

| force            | Forces speed change configuration    |

**Default**

Depends on the port module type, see the “Notes” section below.

**Configuration Mode**

- Config Interface Ethernet
- Config Interface Port Channel
- Config Interface MLAG Port Channel

**History**

- 3.1.0000
- 3.3.4500 Added MLAG port-channel configuration mode
- 3.5.0000 Added 25GbE, 50GbE, and 100GbE speeds and updated notes

**Role**

admin

**Example**

```
switch (config interface ethernet 1/1) # speed 40G
switch (config interface ethernet 1/1) #
```

**Related Commands**

- show interfaces ethernet

**Note**

- The default speed depends on the interface capabilities, interface capable of 40GbE will have 40GbE speed by default
- SwitchX systems do not support 25GbE, 50GbE, and 100GbE speeds
- Not all interfaces support all speed options
load-interval

load-interval <time>
no load-interval

Sets the interface counter interval.
The no form of the command resets the interval to its default value.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>time</th>
<th>In seconds.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>300 seconds.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Configuration Mode</th>
<th>Config Interface Ethernet</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Config Interface Port Channel</td>
</tr>
<tr>
<td></td>
<td>Config Interface MLAG Port Channel</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>History</th>
<th>3.3.0000</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>3.3.4500</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Role</th>
<th>admin</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>switch (config interface ethernet 1/1) # load-interval 30</td>
</tr>
<tr>
<td>switch (config interface ethernet 1/1) #</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Related Commands</th>
<th>show interfaces ethernet</th>
</tr>
</thead>
</table>

| Note | This interval is used for the ingress rate and egress rate counters. |
ip address dhcp

Enables DHCP on this Ethernet interface.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>Disabled</td>
</tr>
</tbody>
</table>
| Configuration Mode | Config Interface Ethernet set as router interface  
                       Config Interface Port Channel set as router interface |
| History            | 3.4.2008 |
| Role               | admin |
| Example            | switch (config interface ethernet 1/1) # ip address dhcp  
                       switch (config interface ethernet 1/1) # |
| Related Commands   | interface ethernet  
                       show interfaces ethernet |

Note
**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.

| Syntax Description | fec-configuration | • auto – auto-FEC selection  
|                    |                  | • no-fec – disables FEC  
|                    |                  | • fec-on – enables FEC  
| force              | force            | Forces configuration (does not require toggling interface to take effect)  

| Default            | Auto-FEC selection  
| Configuration Mode | Config Interface Ethernet  
| History            | 3.5.0000  
|                    | 3.6.2002 Added force option  
| Role               | admin  
| Example            | switch (config interface ethernet 1/2) # fec-override fec-on  
| Related Commands   | show interfaces ethernet  
| Notes              | • This command is supported only on Spectrum™ based switch systems  
|                    | • Use this command with caution. There is no limitation in configuring non-standard FEC. It may cause the link to malfunction.
## clear counters

**clear counters**

Clears the interface counters.

<table>
<thead>
<tr>
<th><strong>Syntax Description</strong></th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Default</strong></td>
<td>N/A</td>
</tr>
</tbody>
</table>
| **Configuration Mode** | Config Interface Ethernet  
                         | Config Interface Port Channel |
| **History**            | 3.1.0000  
                         | 3.3.4500 Added MLAG port-channel configuration mode |
| **Role**               | admin |
| **Example**            | `switch (config interface ethernet 1/1) # clear counters` |
| **Related Commands**   | `show interfaces ethernet` |
| **Note**               | |


show interfaces ethernet

show interfaces ethernet <inf>

Displays the configuration and status for the interface.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>inf</th>
<th>Interface number: &lt;slot&gt;/&lt;port&gt;.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>N/A</td>
<td></td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Any Command Mode</td>
<td></td>
</tr>
<tr>
<td>History</td>
<td>3.1.0000</td>
<td></td>
</tr>
<tr>
<td></td>
<td>3.6.1002</td>
<td>Added “error packets” counter to Tx, “Last change in operational status”, and “Isolation group” to output</td>
</tr>
<tr>
<td></td>
<td>3.6.2002</td>
<td>Added “boot delay” parameters to output</td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
<td></td>
</tr>
</tbody>
</table>
Example

```
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: 40 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
  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

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
```

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 591.
show interfaces ethernet capabilities

show interfaces ethernet [<inf>] capabilities

Displays the interface capabilities.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>inf</th>
<th>Interface number: &lt;slot&gt;/&lt;port&gt;.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>N/A</td>
<td></td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Any Command Mode</td>
<td></td>
</tr>
<tr>
<td>History</td>
<td>3.1.0000</td>
<td></td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
<td></td>
</tr>
</tbody>
</table>
| Example            | switch (config) # show interfaces ethernet 1/1 capabilities
Eth1/1
Speed : 10000,40000
FlowControl : Send, Receive
switch (config) # |
| Related Commands   |                                              |
| Note               |                                              |
show interfaces ethernet counters

show interfaces ethernet <inf> counters [priority <prio>]

Displays the extended counters for the interface.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>inf</th>
<th>Interface number: &lt;slot&gt;/&lt;port&gt;</th>
</tr>
</thead>
<tbody>
<tr>
<td>priority</td>
<td>Displays interface extended counters per priority. Range: 0-7 or “all”</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Default</th>
<th>N/A</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Configuration Mode</th>
<th>Any Command Mode</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>History</th>
<th>3.1.0000</th>
</tr>
</thead>
</table>

| 3.5.1000 | Added notes |
| 3.6.1002 | Added “error packets” counter to Tx |

<table>
<thead>
<tr>
<th>Role</th>
<th>admin</th>
</tr>
</thead>
</table>
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 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
0 bytes
0 error packets
0 discard packets
0 pause packets
0 TX wait
0 TX wait useconds
0 queue depth TC0
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
```

Related Commands

- Spectrum™ based systems display queue depth for TC0 - TC7
- SwitchX® based systems display queue depth for TC0 - TC3 only

Note
show interfaces ethernet description

show interfaces ethernet [<inf>] description

Displays the admin status and protocol status for the specified interface.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>inf</th>
<th>Interface number: &lt;slot&gt;/&lt;port&gt;.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>N/A</td>
<td></td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Any Command Mode</td>
<td></td>
</tr>
<tr>
<td>History</td>
<td>3.1.0000</td>
<td></td>
</tr>
<tr>
<td></td>
<td>3.4.1100</td>
<td>Updated Example</td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
<td></td>
</tr>
<tr>
<td>Example</td>
<td>switch (config) # show interfaces ethernet description</td>
<td></td>
</tr>
</tbody>
</table>

<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>

switch (config) # show interfaces ethernet 1/60 description

<table>
<thead>
<tr>
<th>Eth1/60</th>
</tr>
</thead>
<tbody>
<tr>
<td>Admin state: Enabled</td>
</tr>
<tr>
<td>Operational state: Down (Suspend)</td>
</tr>
</tbody>
</table>

Related Commands

Note
show interfaces ethernet rates

show interfaces ethernet [<inf>] rates [<transfer-rate-unit>]

Displays the current transfer rate of the interface.

**Syntax Description**

- **transfer-rate-unit**
  - KB – displays interface transfer rate in KB/s
  - MB – displays interface transfer rate in MB/s
  - GB – displays interface transfer rate in GB/s
  - If no parameter is entered transfer rate is displayed in readable unit (KB/MB/GB/BS) depending on the range

**Default**

N/A

**Configuration Mode**

Any Command Mode

**History**

3.6.2002

**Role**

admin

**Example**

```markdown
switch (config) # show interfaces ethernet rates KB

<table>
<thead>
<tr>
<th>Port</th>
<th>egress avg rate (KB/s)</th>
<th>egress pkts/sec</th>
<th>ingress avg rate (KB/s)</th>
<th>ingress 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>0.032</td>
<td>1</td>
</tr>
<tr>
<td>...</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

switch (config) #
```

**Related Commands**

**Note**
show interfaces ethernet status

show interfaces ethernet [inf] status

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

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>inf</th>
<th>Interface number: &lt;slot&gt;/&lt;port&gt;.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>N/A</td>
<td></td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Any Command Mode</td>
<td></td>
</tr>
<tr>
<td>History</td>
<td>3.1.0000</td>
<td></td>
</tr>
<tr>
<td></td>
<td>3.4.1100</td>
<td>Updated Example</td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
<td></td>
</tr>
<tr>
<td>Example</td>
<td>switch (config) # show interfaces ethernet status</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Port</td>
<td>Operational state</td>
</tr>
<tr>
<td></td>
<td>----</td>
<td>------------------</td>
</tr>
<tr>
<td></td>
<td>Eth1/58</td>
<td>Down</td>
</tr>
<tr>
<td></td>
<td>Eth1/59</td>
<td>Up</td>
</tr>
<tr>
<td></td>
<td>Eth1/60</td>
<td>Down (Suspend)</td>
</tr>
<tr>
<td>switch (config) #</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
**show interfaces ethernet transceiver**

`show interfaces ethernet [<inf>] transceiver`

Displays the transceiver info.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>inf</th>
<th>interface number: &lt;slot&gt;/&lt;port&gt;</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>N/A</td>
<td></td>
</tr>
</tbody>
</table>

**Configuration Mode**

Any Command Mode

**History**

3.1.0000

**Role**

admin

**Example**

```
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
```

**Related Commands**

**Note**

- For a full list of the supported cables and transceivers, please refer to the LinkX™ Cables and Transceivers webpage in Mellanox.com: [http://www.mellanox.com/page/cables?mtag=cable_overview](http://www.mellanox.com/page/cables?mtag=cable_overview).
- If a high power transceiver (e.g. LR4) is used, it will be indicated in the field “cable/module type”.

---

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

If a high power transceiver (e.g. LR4) is used, it will be indicated in the field “cable/module type”.
show interfaces ethernet transceiver counters

show interfaces ethernet [<inf>] transceiver counters

Displays PHY counters.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>inf</th>
<th>interface number: &lt;slot&gt;/&lt;port&gt;</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>N/A</td>
<td></td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Any Command Mode</td>
<td></td>
</tr>
<tr>
<td>History</td>
<td>3.6.1002</td>
<td></td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
<td></td>
</tr>
</tbody>
</table>

Example

switch (config) # show interfaces ethernet 1/1 transceiver counters

Rx
phy received bits 17725862707200
phy symbol errors 0
phy corrected bits 0

Related Commands

Note

- 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
- 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
- The counter “phy corrected bits” provides the number of corrected bits by the active FEC mode (RS/FC)
- This command is only supported on Spectrum™ based switch systems
show interfaces ethernet transceiver counters details

show interfaces ethernet [<inf>] transceiver counters

Displays all PHY counters.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>inf</th>
<th>interface number: &lt;slot&gt;/&lt;port&gt;</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>N/A</td>
<td></td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Any Command Mode</td>
<td></td>
</tr>
<tr>
<td>History</td>
<td>3.6.1002</td>
<td></td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
<td></td>
</tr>
</tbody>
</table>
| Example                             | 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

Related Commands

Note
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.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>inf</th>
<th>Interface number: &lt;slot&gt;/&lt;port&gt;</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>N/A</td>
<td></td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Any Command Mode</td>
<td></td>
</tr>
<tr>
<td>History</td>
<td>3.6.2002</td>
<td></td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
<td></td>
</tr>
</tbody>
</table>
Example

```
switch (config) # show interfaces ethernet 1/1 transceiver diagnostics
Port 1/1 transceiver diagnostic data:

Temperature (-127C to +127C)
  Temperature                   : 33 C
  Hi Temp Alarm Thresh          : 17 C
  Low Temp Alarm Thresh         : 2 C
  Temperature Alarm             : None

Voltage (0 to 6.5535 V)
  Voltage                       : 3.29450 V
  Hi Volt Alarm Thresh          : 3.70000 V
  Low Volt Alarm Thresh         : 2.90000 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 to 6.5535 mW)
  Ch1 Tx Power                  : 1.03080 mW
  Ch2 Tx Power                  : 1.05070 mW
  Ch3 Tx Power                  : 1.07150 mW
  Ch4 Tx Power                  : 1.10180 mW
  Hi Tx Power Alarm Thresh      : 3.46730 mW
  Low Tx Power Alarm Thresh     : 0.07240 mW
  Ch1 Tx Power Alarm            : None
  Ch2 Tx Power Alarm            : None
  Ch3 Tx Power Alarm            : None
  Ch4 Tx Power Alarm            : None

Rx Power (0 to 6.5535 mW)
  Ch1 Rx Power                  : 1.13980 mW
  Ch2 Rx Power                  : 1.11720 mW
  Ch3 Rx Power                  : 1.08800 mW
  Ch4 Rx Power                  : 1.16450 mW
  Hi Rx Power Alarm Thresh      : 0.33000 mW
  Low Rx Power Alarm Thresh     : 1.01830 mW
  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) : 12-05-2016
```

Related Commands

Note
This example is for a QSFP transceiver
show interfaces ethernet transceiver raw

Displays cable info for this interface.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>inf</th>
<th>Interface number: &lt;slot&gt;/&lt;port&gt;</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>N/A</td>
<td></td>
</tr>
</tbody>
</table>

**Configuration Mode**
- Any Command Mode

**History**
- 3.6.1002

**Role**
- admin

**Example**
```
switch (config) # show interfaces ethernet 1/7 transceiver raw
Port 1/7 raw transceiver data:

I2C Address 0x50, Page 0, 0:255:
  0000 0d 02 06 00 00 00 00 00 00 00 00 00 00 00 00 00 ............
  0010 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ............
  0020 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ............
  0030 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ............
  0040 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ............
  0050 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ............
  0060 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ............
  0070 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ............
  0080 0d 00 23 08 00 00 00 00 00 00 00 00 00 00 00 00 ............
  0090 00 00 01 a0 4d 65 6c 6c 61 6e 6f 20 20 20 20 20 20 20  ....Mellanox
  00a0 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20  ....MC220713
  00b0 30 2d 30 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00A   Ff
  00c0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ............
  00d0 32 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 38 36 34  ....MT1227VS0064
  00e0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ............
  00f0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ............

I2C Address 0x50, Pages 1, 128:255:
  0080 0d 02 06 00 00 00 00 00 00 00 00 00 00 00 00 00 ............
  0090 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ............
  00a0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ............
  00b0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ............
  00c0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ............
  00d0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ............
  00e0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ............
  00f0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ............

...
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

➢ 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
```

Figure 15: Interface Isolation Example
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.
<table>
<thead>
<tr>
<th>Default</th>
<th>Disabled</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuration Mode</td>
<td>Config</td>
</tr>
<tr>
<td>History</td>
<td>3.6.1002</td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
</tr>
<tr>
<td>Example</td>
<td>switch (config) # protocol isolation-group</td>
</tr>
<tr>
<td>Related Commands</td>
<td></td>
</tr>
<tr>
<td>Note</td>
<td>• MLAG must be disabled before enabling interface isolation</td>
</tr>
<tr>
<td></td>
<td>• When disabled, all configuration is lost</td>
</tr>
</tbody>
</table>
### isolation-group

**Syntax**

- isolation-group <name>
- no isolation-group <name>

Creates isolation group.
The no form of the command deletes isolation group.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>N/A</td>
</tr>
</tbody>
</table>

**Configuration Mode**

- Config

**History**

- 3.6.1002

**Role**

- admin

**Example**

```
switch (config) # isolation-group mygroup
```

**Related Commands**

- protocol isolation-group

**Note**

- The no form of this command deletes the isolation group, removes its attached ports, and the VLANs from the group
- Up to 64 isolation groups can be created
**shutdown**

```
shutdown
no shutdown
```

Enables isolation group.
The no form of the command disables isolation group.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>Disabled</td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Config Isolation Group</td>
</tr>
<tr>
<td>History</td>
<td>3.6.1002</td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
</tr>
<tr>
<td>Example</td>
<td>switch (config isolation-group mygroup) # no shutdown</td>
</tr>
<tr>
<td>Related Commands</td>
<td>protocol isolation-group</td>
</tr>
<tr>
<td></td>
<td>isolation-group</td>
</tr>
<tr>
<td>Note</td>
<td>Enabling isolation groups fails if there are VLANs with ports both inside and outside the group.</td>
</tr>
</tbody>
</table>
**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.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>N/A</td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Config Isolation Group</td>
</tr>
<tr>
<td>History</td>
<td>3.6.1002</td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
</tr>
<tr>
<td>Example</td>
<td>switch (config isolation-group mygroup) # vlan 10</td>
</tr>
<tr>
<td>Related Commands</td>
<td>protocol isolation-group isolation-group</td>
</tr>
</tbody>
</table>
| Note               | • Enabling isolation groups fails if there are VLANs with ports both inside and outside the group
• The VLAN must be created before running this command
• All interfaces in the VLAN must be attached to only this isolation group
• The VLAN added cannot have a respective VLAN interface |
### isolation-group mode

**Syntax:**

- `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.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<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>
</tbody>
</table>

**Default:** N/A

**Configuration Mode:**

- Config Interface Ethernet
- Config Interface Port Channel

**History:** 3.6.1002

**Role:** admin

**Example:**

```
switch (config interface ethernet 1/2) # isolation-group mygroup mode
privileged
```

**Related Commands**

- Enabling isolation groups fails if there are VLANs with ports both inside and outside the group
- The VLAN must be created before running this command
- All interfaces in the VLAN must be attached to only this isolation group
- The VLAN added cannot have a respective VLAN interface
show isolation-group

show isolation-group <name>

Displays isolation group information.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>N/A</td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Any Command Mode</td>
</tr>
<tr>
<td>History</td>
<td>3.6.1002</td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
</tr>
</tbody>
</table>

Example

```
switch (config) # show isolation-group mygroup
State:          Enabled
VLANs:          3, 4, 3000
Privileged port: Eth1/25
Isolated ports: Eth1/1, Eth1/2, Eth1/3, Eth1/4, Eth1/5, Eth1/17, Eth1/18, Eth1/19, Eth1/20, Eth1/21, Eth1/27, Eth1/28, Eth1/29, Po60, Po777
```

Related Commands

Note
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.

**Syntax Description**

- **1-4096 / 2-4096**: LAG number

**Default**

- N/A

**Configuration Mode**

- Config

**History**

- 3.1.1400: First version
- 3.2.1100: Added range support
- 3.4.0000: Added note

**Role**

- admin

**Example**

```
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) #
```

**Related Commands**

**Note**

If a LAG is also an IPL, attempting to delete it without first deleting the IPL is rejected by the management.
### lacp

**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
IACP system-priority

IACP system-priority <1-65535>
no IACP system-priority

Configures the IACP system priority.
The no form of the command sets the IACP system-priority to default.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>1-65535</th>
<th>LACP system-priority.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>32768</td>
<td></td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Config</td>
<td></td>
</tr>
<tr>
<td>History</td>
<td>3.1.1400</td>
<td></td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
<td></td>
</tr>
</tbody>
</table>

Example

switch (config)# IACP system-priority 1
switch (config)# show IACP 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)#

Related Commands

Note
**lACP (interface)**

```bash
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.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>rate fast</th>
<th>Sets LACP PDUs on the port to be in fast (1 second) or slow rate. (30 seconds).</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>rate - slow (30 seconds)</td>
<td>LACP port-priority.</td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Config</td>
<td></td>
</tr>
<tr>
<td>History</td>
<td>3.1.1400</td>
<td></td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
<td></td>
</tr>
</tbody>
</table>

**Example**

```bash
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,

<table>
<thead>
<tr>
<th>Port</th>
<th>State</th>
<th>Port Admin</th>
<th>Port Oper</th>
<th>Port Key</th>
<th>Port Number</th>
<th>Port State</th>
</tr>
</thead>
<tbody>
<tr>
<td>1/7</td>
<td>Down</td>
<td>128</td>
<td>1</td>
<td>1</td>
<td>0x7</td>
<td>0x0</td>
</tr>
</tbody>
</table>
```

**Related Commands**

**Note**

Configuring LACP rate (fast or slow) will configure the peer port to send (fast or slow), it does not make any affect on the local port LACP rate.
### port-channel load-balance 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.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Possible load balance methods:</th>
</tr>
</thead>
<tbody>
<tr>
<td>method</td>
<td>• destination-ip</td>
</tr>
<tr>
<td></td>
<td>• destination-mac</td>
</tr>
<tr>
<td></td>
<td>• destination-port</td>
</tr>
<tr>
<td></td>
<td>• source-destination-ip</td>
</tr>
<tr>
<td></td>
<td>• source-destination-mac</td>
</tr>
<tr>
<td></td>
<td>• source-destination-port</td>
</tr>
<tr>
<td></td>
<td>• source-ip</td>
</tr>
<tr>
<td></td>
<td>• source-mac</td>
</tr>
<tr>
<td></td>
<td>• source-port</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Default</th>
<th>source-destination-mac</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuration Mode</td>
<td>Config</td>
</tr>
<tr>
<td>History</td>
<td>3.1.1400</td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
</tr>
</tbody>
</table>

**Example**
```
switch (config)# port-channel load-balance ethernet destination-ip
source-port source-mac
switch (config)# show interfaces port-channel load-balance
destination-ip,source-mac,source-port
switch (config)#
```

**Related Commands**

**Note**
Several load balance methods can be configured (refer to the example)
**channel-group**

`channel-group <1-4096> [mode {on | active | passive}]`

`no channel-group`

Assigns and configures a physical interface to a port channel. The no form of the command removes a physical interface from the port-channel.

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>1-4096</th>
<th>The port channel number.</th>
</tr>
</thead>
<tbody>
<tr>
<td>mode on</td>
<td>Static assignment the port to LAG. LACP will not be enabled on this port.</td>
<td></td>
</tr>
<tr>
<td>mode active/passive</td>
<td>Dynamic assignment of the port to LAG. LACP will be enabled in either passive or active mode.</td>
<td></td>
</tr>
</tbody>
</table>

**Default**

N/A

**Configuration Mode**

Config Interface Ethernet

**History**

3.1.1400

3.4.0008 Added a note

**Role**

admin

**Example**

switch (config interface ethernet 1/7)# channel-group 1 mode active

**Related Commands**

show interfaces port-channel summary
show interfaces port-channel compatibility-parameters
show lacp interfaces ethernet

**Note**

- Setting the mode to active/passive is possible only in LACP is enabled.
- The first port in the LAG decide if the LAG will be static (“on”) or LACP (“active”, “passive”).
- All the ports in the LAG must have the same configuration, determined 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’
- A physical port may only be part of one channel-group
**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.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>force</th>
<th>Toggles the interface after enabling LACP-individual.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>N/A</td>
<td></td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Config Interface Port Channel</td>
<td></td>
</tr>
<tr>
<td>History</td>
<td>3.4.1100</td>
<td></td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
<td></td>
</tr>
<tr>
<td>Example</td>
<td>switch (config interface port-channel 10)# lACP-individual enable force</td>
<td></td>
</tr>
<tr>
<td>Related Commands</td>
<td>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.</td>
<td></td>
</tr>
</tbody>
</table>
### ip address dhcp

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>Disabled</td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Config Interface Port Channel set as router interface</td>
</tr>
<tr>
<td>History</td>
<td>3.4.2008</td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
</tr>
</tbody>
</table>
| Example            | switch (config interface port channel 10) # ip address dhcp  
                      switch (config interface port channel 10) # |
| Related Commands   | interface port-channel  
                      show interface port-channel |

**Note**
### show lacp counters

**show lacp counters**

Displays the LACP PDUs counters.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>N/A</td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Any Command Mode</td>
</tr>
<tr>
<td>History</td>
<td>3.1.1400</td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
</tr>
</tbody>
</table>

**Example**

```
switch (config)# show lacp counters

LACPDUs     Marker     Marker Response      LACPDUs
Port      Sent Recv      Sent Recv         Sent Recv Illegal    Unknown
----------------------------------------------------------------------
Port-channel: 1
----------------------------------------------------------------------
  1/7       0   0           0   0             0
0       0       0
```

**Related Commands**

**Note**
show lACP interfaces ethernet

show lACP interface ethernet <inf>

Displays the LACP interface configuration and status.

**Syntax Description**

| inf | Interface number, for example “1/1”. |

**Default**

N/A

**Configuration Mode**

Any Command Mode

**History**

3.1.1400

**Role**

admin

**Example**

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,

<table>
<thead>
<tr>
<th>Port</th>
<th>LACP Port</th>
<th>Admin</th>
<th>Oper</th>
<th>Port</th>
<th>Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>1/4</td>
<td>Down</td>
<td>128</td>
<td>1</td>
<td>1</td>
<td>0x4</td>
</tr>
</tbody>
</table>

switch (config) #

**Related Commands**

**Note**
### show lACP interfaces neighbor

**show lACP interfaces neighbor**

Displays the LACP interface neighbor status.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>N/A</td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Any Command Mode</td>
</tr>
<tr>
<td>History</td>
<td>3.1.1400</td>
</tr>
<tr>
<td></td>
<td>3.4.0000</td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
</tr>
</tbody>
</table>
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.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>N/A</td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Any Command Mode</td>
</tr>
<tr>
<td>History</td>
<td>3.4.0000</td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
</tr>
</tbody>
</table>

**Example**

```
switch (config) # show lacp
Port-channel Module Admin Status is enabled
switch (config) #
```

**Related Commands**

**Note**
**show lACP interfaces system-identifier**

```plaintext
show lACP interfaces {mlag-port-channel | port-channel} <instance> system-identifier
```

Displays the system identifier of LACP.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>instance</th>
<th>LAG or MLAG instance.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>N/A</td>
<td></td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Any Command Mode</td>
<td></td>
</tr>
<tr>
<td>History</td>
<td>3.4.0000</td>
<td></td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
<td></td>
</tr>
</tbody>
</table>
| Example            | switch (config)# show lACP interfaces port-channel 2 system-identifier
Priority: 12345
MAC: 00:02:C9:AC:2A:60
switch (config)# |

**Related Commands**

**Note**
show interfaces port-channel

show interfaces port-channel <port-channel>

Displays port-channel configuration properties.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Default</th>
<th>Configuration Mode</th>
<th>History</th>
<th>Role</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>port-channel</td>
<td>N/A</td>
<td>Any Command Mode</td>
<td>3.3.4000</td>
<td>admin</td>
<td>switch (config) # show interfaces port-channel 2</td>
</tr>
<tr>
<td>LAG interface whose properties to display</td>
<td></td>
<td></td>
<td>3.4.1100 Updated Example</td>
<td></td>
<td>Po2</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>3.6.1002 Added “error packets” counter to Tx</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>3.3.4000</td>
<td></td>
<td>switch (config) # show interfaces port-channel 2</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>3.4.1100 Updated Example</td>
<td></td>
<td>Po2</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>3.6.1002 Added “error packets” counter to Tx</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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
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

<table>
<thead>
<tr>
<th>Rx</th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>24060</td>
<td>packets</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>23447</td>
<td>unicast packets</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>598</td>
<td>multicast packets</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>15</td>
<td>broadcast packets</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1796876</td>
<td>bytes</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>0</td>
<td>error packets</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>0</td>
<td>discard packets</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Tx</th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>23961</td>
<td>packets</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>23454</td>
<td>unicast packets</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>496</td>
<td>multicast packets</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>11</td>
<td>broadcast packets</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1805778</td>
<td>bytes</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>0</td>
<td>error packets</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>discard packets</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

switch (config) #
Related Commands

Note
show interfaces port-channel counters

show interfaces port-channel <port-channel> counters

Displays the extended counters for the interface.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>port-channel</th>
<th>LAG interface whose properties to display</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>N/A</td>
<td></td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Any Command Mode</td>
<td></td>
</tr>
<tr>
<td>History</td>
<td>3.6.1002</td>
<td></td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
<td></td>
</tr>
<tr>
<td>Example</td>
<td>switch (config) # show interfaces port-channel 3 counters</td>
<td></td>
</tr>
</tbody>
</table>

```
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
```

Related Commands

Note
show interfaces port-channel compatibility-parameters

show interfaces port-channel compatibility-parameters

Displays port-channel parameters.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>N/A</td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Any Command Mode</td>
</tr>
<tr>
<td>History</td>
<td>3.3.4000</td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
</tr>
</tbody>
</table>

Example

```
switch (config) # show interfaces port-channel compatibility-parameters
* Port-mode
* Speed
* MTU
* Flow Control
* Access VLAN
* Allowed VLAN list
* Flowcontrol & PFC
* Channel-group mode
* CoS parameters
* MAC learning disable

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) #
```

Related Commands

Note
**show interfaces port-channel load-balance**

Displays the type of load-balancing in use for port-channels.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>N/A</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>N/A</td>
<td></td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Any Command Mode</td>
<td></td>
</tr>
<tr>
<td>History</td>
<td>3.3.4000</td>
<td></td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
<td></td>
</tr>
</tbody>
</table>

**Example**

```
switch (config) # show interfaces port-channel load-balance
source-destination-mac
switch (config) #
```

**Related Commands**

**Note**
show interfaces port-channel summary

show interfaces port-channel summary

Displays a summary for the port-channel interfaces.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>N/A</td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Any Command Mode</td>
</tr>
<tr>
<td>History</td>
<td>3.1.1400</td>
</tr>
<tr>
<td></td>
<td>3.4.1100</td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
</tr>
</tbody>
</table>
| Example            | 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

<table>
<thead>
<tr>
<th>Group Port-Channel</th>
<th>Type</th>
<th>Member Ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 Po2(U)</td>
<td>LACP</td>
<td>Eth1/58(D) Eth1/59(I) Eth1/60(S)</td>
</tr>
<tr>
<td>2 Po5(D)</td>
<td>LACP</td>
<td>Eth1/1(S) Eth1/33(I)</td>
</tr>
<tr>
<td>3 Po10(U)</td>
<td>LACP</td>
<td>Eth1/49(P) Eth1/50(P) Eth1/51(S) Eth1/52(S)</td>
</tr>
</tbody>
</table>

Related Commands

Note
5.4 MLAG

**Figure 16: Basic MLAG Setup**

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).

- All nodes in an MLAG must be of the same CPU type (i.e. PPC or 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).
- 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 17, “Basic MLAG Topology,” on page 650 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 6.6, “VRRP,” on page 1290 or Section 6.7, “MAGP,” on page 1305 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.
5.4.1 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 standalone 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.

5.4.2 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.

5.4.3 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.
5.4.4 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.

5.4.5 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 666) before closing its ports.

For more information on MLAG upgrade, please see Section 4.3.2, “Upgrading MLNX-OS HA Groups,” on page 216.

5.4.6 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:

```bash
switch (config)# ip routing
```

Step 2. (Recommended) Enable LACP in the switch. Run:

```bash
switch (config)# lacp
```

Step 3. Enable QoS on the switch to avoid congestion on the IPL port. Run:

```bash
switch (config)# dcb priority-flow-control enable force
```

Step 4. Enable the MLAG protocol commands. Run:

```bash
switch (config)# protocol mlag
```

Configuring the IPL:

Step 1. Create a VLAN for the inter-peer link (IPL) to run on. Run:

```bash
switch (config)# vlan 4000
```

Step 2. Create a LAG. Run:

```bash
switch (config)# interface port-channel 1
```

Step 3. Map a physical port to the LAG in active mode (LACP). Run:

```bash
switch (config)# interface ethernet 1/1 channel-group 1 mode active
```

Step 4. Set this LAG as an IPL. Run:

```bash
switch (config interface port-channel 1)# ipl 1
```

Step 5. Enable QoS on this specific interface. Run:

```bash
switch (config interface port-channel 1)# dcb priority-flow-control mode on force
```

Step 6. Create a VLAN interface. Run:

```bash
switch (config)# interface vlan 4000
```

Step 7. Set an IP address and netmask for the VLAN interface.

On SwitchA, run:

```bash
switch (config interface vlan 4000)# ip address 10.10.10.1 /30
```

On SwitchB, run:

```bash
switch (config interface vlan 4000)# ip address 10.10.10.2 /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:

```bash
switch (config interface vlan 4000)# ipl 1 peer-address 10.10.10.2
```
On SwitchB, run:

```
switch (config interface vlan 4000)# ip l 1 peer-address 10.10.10.1
```

**Step 9.** Configure a virtual IP (VIP) for the MLAG. Run:

On SwitchA, run:

```
switch (config)# mlag-vip my-vip ip 10.10.10.254 /24 //mask may also be 255.255.255.0
```

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 bpdufilter 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 6.6, “VRRP,” on page 1290 or Section 6.7, “MAGP,” on page 1305 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
```
Step 2.

Examine the MLAG summary table. Run:

```text
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) (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
MLAG 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.

### 5.4.7 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.

<table>
<thead>
<tr>
<th>Syntax Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Default</strong></td>
</tr>
<tr>
<td><strong>Configuration Mode</strong></td>
</tr>
<tr>
<td><strong>History</strong></td>
</tr>
<tr>
<td><strong>Role</strong></td>
</tr>
<tr>
<td><strong>Example</strong></td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>
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

Enters MLAG configuration mode.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>N/A</td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Config</td>
</tr>
<tr>
<td>History</td>
<td>3.3.4500</td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
</tr>
</tbody>
</table>

```
switch (config) # mlag
switch (config mlag) #
```

Note
**shutdown**

shutdown
no shutdown

Disables MLAG.
The no form of the command enables MLAG.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>Disabled</td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Config MLAG</td>
</tr>
<tr>
<td>History</td>
<td>3.3.4500</td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
</tr>
</tbody>
</table>

**Example**

switch (config mlag) # no shutdown
switch (config mlag) #

**Related Commands**

**Note**
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.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>if-number</th>
<th>Integer. Interface number range: 1-1000.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>N/A</td>
<td></td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Config</td>
<td></td>
</tr>
<tr>
<td>History</td>
<td>3.3.4500</td>
<td></td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
<td></td>
</tr>
</tbody>
</table>
| Example            | switch (config) # interface mlag-port-channel 1
switch (config interface mlag-port-channel 1) # |

Related Commands

Note
- The maximum number of interfaces is 64.
- The default Admin state is disabled.
- Range configuration is possible on this interface.
- This interface number must be the same in all the MLAG switches.
**ipl**

`ipl <ipl-id>`

Sets this LAG as an IPL port.
The no form of the command resets this LAG as regular LAG.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ipl-id</td>
<td>IPL ID. Only “1” IPL port is supported.</td>
</tr>
</tbody>
</table>

| Default            | no ipl               |

<table>
<thead>
<tr>
<th>Configuration Mode</th>
<th>Config Interface Port Channel</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>History</th>
<th>3.3.4500</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Role</th>
<th>admin</th>
</tr>
</thead>
</table>

**Example**

switch (config interface port-channel 1)# ipl 1

**Related Commands**

**Note**

- If a LAG is set as IPL, only the commands “[no] shutdown”, “no ipl” and “no interface port-channel” become applicable.
- A LAG interface set as IPL must have default LAG configuration, otherwise the set is rejected. Force option can be used.
### 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.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>ipl-id</td>
<td>IPL ID. Only “1” IPL port is supported.</td>
<td></td>
</tr>
<tr>
<td>IP-Address</td>
<td>IPv4 address.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Default</th>
<th>N/A</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Configuration Mode</th>
<th>Config Interface VLAN</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>History</th>
<th>3.3.4500</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Role</th>
<th>admin</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Example</th>
</tr>
</thead>
</table>
| switch (config interface vlan 1)# ipl 1 peer-address 10.10.10.10
| switch (config interface vlan 1)# |

<table>
<thead>
<tr>
<th>Related Commands</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Note</th>
</tr>
</thead>
<tbody>
<tr>
<td>• The subnet mask is the same subnet mask of the VLAN interface.</td>
</tr>
<tr>
<td>• This VLAN interface should be used for IPL only.</td>
</tr>
</tbody>
</table>
**keep-alive-interval**

```plaintext
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.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>value</th>
<th>Time in seconds. Range: 1-300.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>1 second</td>
<td></td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Config MLAG</td>
<td></td>
</tr>
<tr>
<td>History</td>
<td>3.3.4500</td>
<td></td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
<td></td>
</tr>
</tbody>
</table>
| Example            | switch (config mlag) # keep-alive-interval 1  
|                    | switch (config mlag) #         |                                 |

**Note**
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.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>if-number</th>
<th>Integer. Interface number range: 1-1000.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>on</td>
<td>Binds to static MLAG.</td>
</tr>
<tr>
<td></td>
<td>active</td>
<td>Sets MLAG LAG in LACP active mode.</td>
</tr>
<tr>
<td></td>
<td>passive</td>
<td>Sets MLAG LAG in LACP passive mode.</td>
</tr>
</tbody>
</table>

| Default          | N/A       |
| Configuration Mode | Config Interface Ethernet |
| History          | 3.3.4500  |
| Role             | admin     |

| Example          | switch (config interface ethernet 1/1)# mlag-channel-group 1 mode on |
|                  | switch (config interface ethernet 1/1)# |

| Related Commands |

| Note |

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.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>domain-name</th>
<th>MLAG group name</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>&lt;ip-address&gt;</td>
<td>IP address</td>
</tr>
<tr>
<td></td>
<td>&lt;masklen&gt;</td>
<td>Format example: /24. Note that a space is required between the IP address and the mask.</td>
</tr>
<tr>
<td></td>
<td>&lt;netmask&gt;</td>
<td>Format example: 255.255.255.0. Note that a space is required between the IP address and the mask.</td>
</tr>
<tr>
<td></td>
<td>force</td>
<td>Forces the IP address if another IP is already configured.</td>
</tr>
</tbody>
</table>

Default: N/A

Configuration Mode: Config

History: 3.3.4500

Role: admin

Example:

```
switch (config)# mlag-vip my-mlag-domain ip 10.10.10.254/24
switch (config)#
```

Related Commands

Note
- This IP address must be configured in one of the MLAG switches and must be in the box management subnet.
- Other switches in the MLAG must join the same domain name.
## reload-delay

**reload-delay**

**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.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>value</th>
<th>Time in seconds. Range: 0-300.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>30 seconds</td>
<td></td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Config MLAG</td>
<td></td>
</tr>
<tr>
<td>History</td>
<td>3.3.4500</td>
<td></td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
<td></td>
</tr>
</tbody>
</table>
| Example            | switch (config mlag) # reload-delay 30  
switch (config mlag) # |
| Related Commands   |       |

**Note**

- This interval allows the switch to learn the IPL topology to identify the master and sync the MAC address before opening the MLAG ports.
- This parameter must be similar in all MLAG peers.
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.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>virtual-mac</th>
<th>MAC address</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td></td>
<td>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.</td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Config MLAG</td>
<td></td>
</tr>
<tr>
<td>History</td>
<td>3.4.2008</td>
<td></td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
<td></td>
</tr>
</tbody>
</table>
| Example            | switch (config mlag) # system-mac 00:00:5E:00:01:5D
switch (config mlag) # |             |
| Related Commands   |             |             |
| Note               | 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.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>time</td>
<td></td>
<td>Time in minutes. Range: 0-120 minutes.</td>
</tr>
</tbody>
</table>

| Default |   | 60 |

| Configuration Mode |   | Config MLAG |

| History |   | 3.4.2008 |

| Role |   | admin |

| Example |   | `switch (config mlag) # upgrade-timeout 60`  
|         |   | `switch (config mlag) #` |

**Related Commands**

**Note**

This parameter must be configured the same in all MLAG peers.
show mlag

Displays MLAG configuration and status.

**Syntax Description**
N/A

**Default**
N/A

**Configuration Mode**
Any Command Mode

**History**
3.3.4500
3.3.5006 Updated example
3.4.2008 Updated example with system MAC and upgrade timeout

**Role**
admin

**Example**
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:
<table>
<thead>
<tr>
<th>ID</th>
<th>Group</th>
<th>Vlan</th>
<th>Operational</th>
<th>Local</th>
<th>Peer</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Port-Channel</td>
<td>Interface</td>
<td>State</td>
<td>IP address</td>
<td>IP address</td>
</tr>
<tr>
<td>----</td>
<td>---------------</td>
<td>------------</td>
<td>--------</td>
<td>-------------</td>
<td>-------------</td>
</tr>
<tr>
<td>1</td>
<td>Po1</td>
<td></td>
<td>Up</td>
<td>10.10.10.1</td>
<td>10.10.10.2</td>
</tr>
</tbody>
</table>

MLAG Members Summary:
System-id State Hostname
F4:52:14:2D:9B:88 Up <SX2>
F4:52:14:2D:9B:08 Up SX1
SX2 [mellanox: master] (config)#

**Related Commands**

**Note**
show mlag-vip

**show mlag-vip**

Displays MLAG VIP configuration and status.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>N/A</td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Any Command Mode</td>
</tr>
<tr>
<td>History</td>
<td>3.3.4500</td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
</tr>
</tbody>
</table>

**Example**

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

<table>
<thead>
<tr>
<th>Hostname</th>
<th>VIP-State</th>
<th>IP Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>SwitchA</td>
<td>master</td>
<td>10.10.10.1</td>
</tr>
<tr>
<td>SwitchB</td>
<td>standby</td>
<td>10.10.10.2</td>
</tr>
</tbody>
</table>
```

**Related Commands**

**Note**
show interfaces mlag-port-channel

show interfaces mlag-port-channel <if-number>

Displays the MLAG LAG configuration and status.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>N/A</td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Any Command Mode</td>
</tr>
<tr>
<td>History</td>
<td>3.3.4500</td>
</tr>
<tr>
<td></td>
<td>3.6.1002 Added “error packets” counter to Tx</td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
</tr>
</tbody>
</table>
| Example            | 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
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
switch (config)# |

Related Commands

Note
**show interfaces mlag-port-channel counters**

```
show interfaces mlag-port-channel <if-number> counters
```

Displays the extended counters for the interface.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>N/A</td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Any Command Mode</td>
</tr>
<tr>
<td>History</td>
<td>3.6.1002</td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
</tr>
</tbody>
</table>

**Example**

```
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)#
```
### show interfaces mlag-port-channel summary

**Syntax Description**
N/A

**Default**
N/A

**Configuration Mode**
Any Command Mode

**History**
- 3.3.4500: First version
- 3.4.0000: Added notes and updated example
- 3.4.1100: Updated Example

**Role**
admin

**Example**
```
switch [my-vip: standby] (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

<table>
<thead>
<tr>
<th>Group</th>
<th>Port-Channel</th>
<th>Type</th>
<th>Local Ports</th>
<th>Peer Ports</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td>(D/U/P/S)</td>
<td>(D/P/S/I)</td>
</tr>
<tr>
<td>1</td>
<td>Mpo2(U)</td>
<td>Static</td>
<td>Eth1/2(P)</td>
<td>Eth1/2(P)</td>
</tr>
<tr>
<td>2</td>
<td>Mpo3(U)</td>
<td>Static</td>
<td>Eth1/4(P)</td>
<td>Eth1/8(P)</td>
</tr>
<tr>
<td>3</td>
<td>Mpo4(U)</td>
<td>LACP</td>
<td>Eth1/5(P)</td>
<td>Eth1/5(P)</td>
</tr>
</tbody>
</table>

switch (config)#
```

**Related Commands**

- `switchport_mode mlag` (Mellanox Technologies Confidential)

**Note**
- If a cluster is not available, the column “Peer Ports” shows “N/A”. If the cluster is available but is not configured on the peer, the “Peer Ports” column shows nothing.
- If the system happens to be busy, peer ports may be unavailable and the following prompt may appear in the output: “System busy and partial information is presented – please try again later”.
- The “I” flag indicates an interface which is part of a port-channel and in individual state.
- The “S” flag indicates an interface which is part of a port-channel and in suspended state.
### show mlag statistics

**show mlag statistics**

Displays the MLAG IPL counters.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>N/A</td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Any Command Mode</td>
</tr>
<tr>
<td>History</td>
<td>3.3.4500</td>
</tr>
<tr>
<td></td>
<td>3.4.0000 Updated example</td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
</tr>
</tbody>
</table>
| Example            | 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 |

**Related Commands**

**Note**
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 1/36
switch (config interface ethernet 1/36) #
```

**Step 6.** From within the interface context, configure the interface mode to Access. Run:

```
switch (config interface ethernet 1/36) # switchport mode access
switch (config interface ethernet 1/36) #
```
Step 7. From within the interface context, configure the Access VLAN membership. Run:

```
switch (config interface ethernet 1/36) # switchport access vlan 6
switch (config interface ethernet 1/36) #
```

Step 8. Change back to config mode. Run:

```
switch (config interface ethernet 1/36) # exit
switch (config) #
```

### 5.5.2 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 1/36
switch (config interface ethernet 1/36) #
```

**Step 6.** From within the interface context, configure the interface mode to Access. Run:

```
switch (config interface ethernet 1/36) # switchport mode hybrid
switch (config interface ethernet 1/36) #
```

**Step 7.** From within the interface context, configure the Access VLAN membership. Run:

```
switch (config interface ethernet 1/36) # switchport access vlan 6
switch (config interface ethernet 1/36) #
```

**Step 8.** Change to config mode again. Run:

```
switch (config interface ethernet 1/36) # exit
switch (config) #
```

### 5.5.3 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
```
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

\[ \text{vlan \{<vlan-id> | <vlan-range>\}} \]
\[ \text{no vlan \{<vlan-id> | <vlan-range>\}} \]

Creates a VLAN or range of VLANs, and enters a VLAN context. The no form of the command deletes the VLAN or VLAN range.

**Syntax Description**

<table>
<thead>
<tr>
<th><strong>Syntax</strong></th>
<th><strong>Description</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan-id</td>
<td>1-4094.</td>
</tr>
<tr>
<td>vlan-range</td>
<td>Any range of VLANs.</td>
</tr>
</tbody>
</table>

**Default**

VLAN 1 is enabled by default.

**Configuration Mode**

Config

**History**

3.1.1400

**Role**

admin

**Example**

```
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 ...

```

**Related Commands**

- show vlan
- switchport mode
- switchport [trunk | hybrid] allowed-vlan

**Note**

Interfaces are not added automatically to VLAN unless configured with trunk or hybrid mode with “all” option turned on.
**name**

```
name <vlan-name>
no name
```

Adds VLAN name.
The no form of the command deletes the VLAN name.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan-name</td>
<td>40-character long string.</td>
<td>No name available.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Configuration Mode</th>
<th>Role</th>
<th>Example</th>
</tr>
</thead>
</table>
| Config VLAN        | admin  | switch (config) # vlan 10    
                    |        | switch (config vlan 10) # name my-vlan-name     
                    |        | switch (config vlan 10) # show vlan                                                                 |

```

<table>
<thead>
<tr>
<th>VLAN</th>
<th>Name</th>
<th>Ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>10</td>
<td>my-vlan-name</td>
<td></td>
</tr>
</tbody>
</table>

**Related Commands**

- show vlan
- switchport mode
- switchport [trunk | hybrid] allowed-vlan

**Note**

Name can not be added to a range of VLANs.
show vlan

show vlan [id <vlan-id>]

Displays the VLAN table.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan-id</td>
<td>1-4094</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Default</th>
<th>N/A</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Configuration Mode</th>
<th>Any Command Mode</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>History</th>
<th>3.1.1400</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Role</th>
<th>admin</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Example</th>
<th>switch (config vlan 10) # show vlan</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLAN</td>
<td>Name</td>
</tr>
<tr>
<td>____</td>
<td>-----------</td>
</tr>
<tr>
<td>1</td>
<td>default</td>
</tr>
<tr>
<td>10</td>
<td>my-vlan-name</td>
</tr>
</tbody>
</table>

| Related Commands | show vlan  
switchport mode  
switchport [trunk | hybrid] allowed-vlan  
vlan |
|------------------|-----------------------------------------------|

<table>
<thead>
<tr>
<th>Note</th>
</tr>
</thead>
</table>
### switchport mode

```
switchport mode {access | dot1q-tunnel | trunk | hybrid | access-decb}
no switchport mode
```

Sets the switch port mode. The no form of the command sets the switch port mode to access.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>access</th>
<th>Untagged port. 802.1q tagged traffic are filtered. Egress traffic is untagged.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>dot1q-tunnel</td>
<td>Allows both tagged and untagged ingress Ethernet packets. Egress packets are tagged with a second VLAN (802.1Q) header.</td>
</tr>
<tr>
<td></td>
<td>trunk</td>
<td>802.1q tagged port, untagged traffic is filtered.</td>
</tr>
<tr>
<td></td>
<td>hybrid</td>
<td>Both 802.1q tagged and untagged traffic is allowed on the port.</td>
</tr>
<tr>
<td></td>
<td>access-decb</td>
<td>Untagged port, egress traffic is priority tagged.</td>
</tr>
</tbody>
</table>

**Default**
access

**Configuration Mode**
Config Interface Ethernet  
Config Interface Port Channel  
Config Interface MLAG Port Channel

**History**
3.1.1400
3.3.4500 Added MLAG port-channel configuration mode
3.4.3000 Added dot1q-tunnel parameter

**Role**
admin

#### Example
```
switch (config) # interface ethernet 1/7
switch (config interface ethernet 1/7) # switchport mode access
switch (config interface ethernet 1/7) # show interfaces switchport

<table>
<thead>
<tr>
<th>Interface</th>
<th>Mode</th>
<th>Access vlan</th>
<th>Allowed vlans</th>
</tr>
</thead>
<tbody>
<tr>
<td>Eth1/2</td>
<td>access</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>Eth1/3</td>
<td>access</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>Eth1/4/1</td>
<td>access</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>Eth1/4/2</td>
<td>access</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>Eth1/5</td>
<td>access</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>Eth1/6</td>
<td>access</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>....</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Po34</td>
<td>access</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>Po4096</td>
<td>access</td>
<td>1</td>
<td></td>
</tr>
</tbody>
</table>

switch (config interface ethernet 1/7) #
```
**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.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>pipe</th>
<th>Gives the service provider’s traffic QoS 0</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>uniform</td>
<td>Gives the service provider’s traffic the same QoS as the customer’s traffic</td>
</tr>
</tbody>
</table>

**Default**

pipe

**Configuration Mode**

- Config Interface Ethernet
- Config Interface Port Channel
- Config Interface MLAG Port Channel

**History**

3.4.3000

**Role**

admin

**Example**

```
switch (config interface ethernet 1/1) # switchport dot1q-tunnel qos-mode uniform
switch (config interface ethernet 1/1) #
```

**Related Commands**

- show vlan
- show interfaces switchport
- switchport access vlan
- switchport [trunk | hybrid] allowed-vlan
- vlan

**Note**
**switchport access**

*switchport access vlan <vlan-id>*

*no switchport access vlan*

Sets the port access VLAN.
The no form of the command sets the port access VLAN to 1.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>vlan-id</th>
<th>1-4094.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td></td>
<td>1</td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Config Interface Ethernet</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Config Interface Port Channel</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Config Interface MLAG Port Channel</td>
<td></td>
</tr>
<tr>
<td>History</td>
<td>3.1.1400</td>
<td>First version</td>
</tr>
<tr>
<td></td>
<td>3.2.0500</td>
<td>Format change (removed hybrid and access-deb options). Previous command format was: “switchport {hybrid</td>
</tr>
<tr>
<td></td>
<td>3.3.4500</td>
<td>Added MLAG port-channel configuration mode</td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
<td></td>
</tr>
</tbody>
</table>

**Example**

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

<table>
<thead>
<tr>
<th>Interface</th>
<th>Mode</th>
<th>Access vlan</th>
<th>Allowed vlans</th>
</tr>
</thead>
<tbody>
<tr>
<td>Eth1/2</td>
<td>access</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>Eth1/3</td>
<td>access</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>Eth1/4/1</td>
<td>access</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>Eth1/4/2</td>
<td>access</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>Eth1/5</td>
<td>access</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>Eth1/6</td>
<td>access</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>Eth1/7</td>
<td>access</td>
<td>10</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Po4096</td>
<td>access</td>
<td>1</td>
<td></td>
</tr>
</tbody>
</table>

switch (config interface ethernet 1/7) #

**Related Commands**

show vlan
show interfaces switchport
switchport mode
switchport [trunk | hybrid] allowed-vlan
vlan

**Note**

This command is not applicable for interfaces with port mode trunk.
only one option ("access", "access-deb" 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.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan</td>
<td>VLAN ID (1-4094) or VLAN range.</td>
</tr>
<tr>
<td>add</td>
<td>Adds VLAN or range of VLANs.</td>
</tr>
<tr>
<td>remove</td>
<td>Removes VLANs or range of VLANs.</td>
</tr>
<tr>
<td>all</td>
<td>Adds all VLANs in available in the VLAN table. New VLANs added to the VLAN table are added automatically.</td>
</tr>
<tr>
<td>except</td>
<td>Adds all VLANs expect this VLAN or VLAN range.</td>
</tr>
<tr>
<td>none</td>
<td>Removes all VLANs.</td>
</tr>
</tbody>
</table>

**Default**
N/A

**Configuration Mode**
Config Interface Ethernet  
Config Interface Port Channel  
Config Interface MLAG Port Channel

**History**
3.1.1400

**Role**
admin

**Example**
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

<table>
<thead>
<tr>
<th>Interface</th>
<th>Mode</th>
<th>Access vlan</th>
<th>Allowed vlans</th>
</tr>
</thead>
<tbody>
<tr>
<td>Eth1/2</td>
<td>access</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>Eth1/3</td>
<td>access</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>Eth1/4/1</td>
<td>access</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>Eth1/4/2</td>
<td>access</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>Eth1/5</td>
<td>access</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>Eth1/6</td>
<td>access</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>Eth1/7</td>
<td>hybrid</td>
<td>1</td>
<td>1, 10</td>
</tr>
<tr>
<td>Po34</td>
<td>access</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>Po4096</td>
<td>access</td>
<td>1</td>
<td></td>
</tr>
</tbody>
</table>

switch (config interface ethernet 1/7) #
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**

```bash
switchport voice vlan <vlan-id>
no switchport voice vlan
```

Configures voice VLAN for the interface. The no form of the command disables voice VLAN.

**Syntax Description**

<table>
<thead>
<tr>
<th>vlan-id</th>
<th>1-4094.</th>
</tr>
</thead>
</table>

**Default**

Disabled

**Configuration Mode**

- Config Interface Ethernet
- Config Interface Port Channel
- Config Interface MLAG Port Channel

**History**

3.6.1002

**Role**

admin

**Example**

```bash
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
```

<table>
<thead>
<tr>
<th>Interface</th>
<th>Mode</th>
<th>Access vlan</th>
<th>Allowed vlans</th>
</tr>
</thead>
<tbody>
<tr>
<td>Eth1/2</td>
<td>access</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>Eth1/3</td>
<td>access</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>Eth1/4/1</td>
<td>access</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>Eth1/4/2</td>
<td>access</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>Eth1/5</td>
<td>access</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>Eth1/6</td>
<td>access</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>Eth1/7</td>
<td>access</td>
<td>10</td>
<td></td>
</tr>
<tr>
<td>....</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Po4096</td>
<td>access</td>
<td>1</td>
<td></td>
</tr>
</tbody>
</table>

**Related Commands**

- lldp med-tlv-select
- show vlan
- show interfaces switchport
- switchport mode
- switchport [trunk | hybrid] allowed-vlan
- vlan

**Note**
show interface switchport

Displays all interface switch port configurations.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>N/A</td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Any Command Mode</td>
</tr>
<tr>
<td>History</td>
<td>3.1.1400</td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
</tr>
</tbody>
</table>

**Example**

```
switch (config) #show interfaces switchport

<table>
<thead>
<tr>
<th>Interface</th>
<th>Mode</th>
<th>Access vlan</th>
<th>Allowed vlans</th>
</tr>
</thead>
<tbody>
<tr>
<td>Eth1/2</td>
<td>access</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>Eth1/3</td>
<td>access</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>Eth1/4/1</td>
<td>access</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>Eth1/4/2</td>
<td>access</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>Eth1/5</td>
<td>access</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>Eth1/6</td>
<td>access</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>Eth1/7</td>
<td>hybrid</td>
<td>1</td>
<td>1, 10</td>
</tr>
<tr>
<td>Po34</td>
<td>access</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>Po4096</td>
<td>access</td>
<td>1</td>
<td></td>
</tr>
</tbody>
</table>
```

**Related Commands**

- show vlan
- switchport access vlan
- switchport mode
- vlan

**Note**
5.6 Voice VLAN

This feature 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 18, 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 18: Tagging Voice Packets with a Different VLAN ID](image-url)
5.6.1 Configuring Voice VLAN

➢ To configure LLDP-MED TLV, run:

```bash
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: 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
...```

```
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         : 11
  L2 Priority     : 0
  DSCP Value      : 0
```
To configure voice VLAN:

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

```bash
switch (config) # vlan 200
switch (config vlan 200) # exit
switch (config) #
```

**Step 2.** Set the interface mode to be hybrid. Run:

```bash
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:

```bash
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:

```bash
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:

```bash
switch (config)# show interfaces switchport
```

<table>
<thead>
<tr>
<th>Interface</th>
<th>Mode</th>
<th>Access vlan</th>
<th>Allowed vlans</th>
</tr>
</thead>
<tbody>
<tr>
<td>Eth1/1</td>
<td>access</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>Eth1/2</td>
<td>access</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>Eth1/3</td>
<td>access</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>Eth1/4</td>
<td>hybrid</td>
<td>300</td>
<td>200</td>
</tr>
<tr>
<td>Eth1/5</td>
<td>access</td>
<td>1</td>
<td></td>
</tr>
</tbody>
</table>

```bash
switch (config)# show lldp interfaces ethernet 1/4
```

TLV flags:
- CEE: Converged Enhanced Ethernet DCBX version
- MED-CAP: Media Capabilities
- MED-NWP: MED-Network Policy

```bash
switch (config)# show lldp interfaces ethernet 1/4
```

<table>
<thead>
<tr>
<th>Interface Receive</th>
<th>Transmit</th>
<th>TLVs</th>
</tr>
</thead>
<tbody>
<tr>
<td>Eth1/4</td>
<td>Enabled</td>
<td>Enabled</td>
</tr>
<tr>
<td></td>
<td>PD, SN, SD, SC, MA, PFC, AP, ETS-C, ETS-R, MED-CAP, MED-NWP</td>
<td></td>
</tr>
</tbody>
</table>
To remove voice VLAN and LLDP-MED TLV:

**Step 1.** Remove the voice VLAN from the interface. Run:

```bash
switch (config)# no interface ethernet 1/4 switchport voice vlan
```

**Step 2.** Disable the MED TLV from the interface. Run:

```bash
switch (config)# interface ethernet 1/4 lldp med-tlv-select none
```

### 5.6.2 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.
5.7 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.

5.7.1 QinQ Operation Modes

QinQ can be enabled on a port or according to predefined conditions.

- 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.

5.7.2 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
...            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
```

5.7.3 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.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>pipe</th>
<th>Gives the service provider’s traffic the same QoS as the customer’s traffic</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>uniform</td>
<td>Gives the service provider’s traffic QoS 0</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Default</th>
<th>pipe</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Configuration Mode</th>
<th>Config Interface Ethernet</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Config Interface Port Channel</td>
</tr>
<tr>
<td></td>
<td>Config Interface MLAG Port Channel</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>History</th>
<th>3.4.3000</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Role</th>
<th>admin</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Example</th>
<th>switch (config interface ethernet 1/1) # switchport dot1q-tunnel qos-mode uniform</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>switch (config interface ethernet 1/1) #</td>
</tr>
</tbody>
</table>
Related Commands

- show vlan
- show interfaces switchport
- switchport access vlan
- switchport [trunk | hybrid] allowed-vlan
- vlan

Note
### 5.8 MAC Address Table

#### 5.8.1 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
```

#### 5.8.2 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 19: MAC Learning Disable Example Case*
### 5.8.3 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.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>age</th>
<th>10-1000000 seconds.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>300</td>
<td></td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Config</td>
<td></td>
</tr>
<tr>
<td>History</td>
<td>3.1.0600</td>
<td></td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
<td></td>
</tr>
</tbody>
</table>

**Example**

```
switch (config) # mac-address-table aging-time 50
switch (config) # show mac-address-table aging-time

Mac Address Aging Time: 50

switch (config) #
```

**Related Commands**

- show mac-address-table
- show mac-address-table aging time

**Note**
**mac-address-table static**

- `mac-address-table static <mac address> vlan <vlan> interface <if-type> <if-number>`
- `no mac-address-table static <mac address> vlan <vlan> interface <if-type> <if-number>`

Configures a static MAC address in the forwarding database. The no form of the command deletes a configured static MAC address from the forwarding database.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>mac address</code></td>
<td>Destination MAC address.</td>
</tr>
<tr>
<td><code>vlan</code></td>
<td>VLAN ID or VLAN range.</td>
</tr>
<tr>
<td><code>if-type</code></td>
<td>Ethernet or port-channel interface type.</td>
</tr>
<tr>
<td><code>if-number</code></td>
<td>The interface number (i.e. 1/1, 3).</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Default</th>
<th>No static MAC addresses available in default.</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Configuration Mode</th>
<th>Config</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>History</th>
<th>3.1.0600</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Role</th>
<th>admin</th>
</tr>
</thead>
</table>

**Example**

```bash
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

<table>
<thead>
<tr>
<th>Vlan</th>
<th>Mac Address</th>
<th>Type</th>
<th>Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>aa:aa:aa:aa:aa:aa</td>
<td>static</td>
<td>Eth1/7</td>
</tr>
</tbody>
</table>

Number of unicast: 1
Number of multicast: 0
```

**Related Commands**

- `show mac-address-table`
- `mac-address-table aging time`

**Note**

The no form of the command will not clear a dynamic MAC address. Dynamic MAC addresses are cleared using the “clear mac-address-table dynamic” command.
mac-learning disable

mac-learning disable
no mac-learning disable

Disables MAC-address learning.
The no form of the command enables MAC-address learning.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>Enabled</td>
</tr>
</tbody>
</table>
| Configuration Mode | Config Interface Ethernet  
|                    | Config Interface Port Channel |
| History            | 3.1.0600         |
| Role               | admin            |
| Example            | switch (config interface ethernet 1/1) # mac-learning disable |

Note
- When adding a port to a LAG, the port needs to be aligned with the LAG’s configuration
- When removing a port from a LAG, the port remains in whichever configuration the LAG is in
- Disabling MAC learning is not supported on a local analyzer port.
- Disabling MAC learning is not supported on an IPL LAG.
clear mac-address-table dynamic

Clear the dynamic entries in the MAC address table.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>N/A</td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Config</td>
</tr>
<tr>
<td>History</td>
<td>3.1.0600</td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
</tr>
</tbody>
</table>

**Example**

```
switch (config) # clear mac-address-table dynamic
switch (config) #
```

**Related Commands**

- mac-address-table aging-time
- mac-address-table static
- show mac-address-table

**Note**

This command does not clear the MAC addresses learned on the mgmt0 port. Static entries are deleted using the “no mac-address-table static” command.
show mac-address-table

show mac-address-table [address <mac-address> | interface ethernet <if-number> | vlan [<vlan> | range <range>] | unicast | multicast]

Displays the static and dynamic unicast and multicast MAC addresses for the switch. Various of filter options available.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>mac-address</td>
<td>Filter the table to a specific MAC address.</td>
</tr>
<tr>
<td>if-number</td>
<td>Filter the table to a specific interface.</td>
</tr>
<tr>
<td>vlan</td>
<td>Filter the table to a specific VLAN number (1-4094).</td>
</tr>
<tr>
<td>range</td>
<td>Filter the table to a range of VLANs.</td>
</tr>
<tr>
<td>unicast</td>
<td>Filter the table to a unicast addresses only.</td>
</tr>
<tr>
<td>multicast</td>
<td>Filter the table to a multicast addresses only.</td>
</tr>
</tbody>
</table>

Default: N/A

Configuration Mode: Any Command Mode

History: 3.1.0600

3.3.4500 Updated Example

Role: admin

Example:

```
switch (config) # show mac-address-table

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
```

Related Commands: mac-address-table static

Note:

clear mac-address-table
show mac-address-table aging-time

Displays the MAC address table aging time.

**Syntax Description**
N/A

**Default**
N/A

**Configuration Mode**
Any Command Mode

**History**
3.1.0600

**Role**
admin

**Example**
```
switch (config) # mac-address-table aging-time 300
switch (config) # show mac-address-table aging-time
Mac Address Aging Time: 300
switch (config) #
```

**Related Commands**
mac-address-table aging-time
mac-address-table static
clear mac-address-table

**Note**
MAC addresses learned on the mgmt0 is not shown by this command.
### show mac-address-table summary

**show mac-address-table summary**

Displays total number of unicast/multicast MAC address entries.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>N/A</td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Any Command Mode</td>
</tr>
<tr>
<td>History</td>
<td>3.6.2002</td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
</tr>
</tbody>
</table>
| Example            | switch (config) # show mac-address-table summary  
|                    | Number of unicast: 4  
|                    | Number of multicast: 0 |
| Related Commands   | mac-address-table static  
|                    | clear mac-address-table |

**Note**
5.9  **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.

5.9.1  **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>
```

5.9.2  **Port Type**

Port type has the following configuration options:

- **edge** – is not assumed to be converged by the RSTP learning/forwarding mechanism. It converges to forwarding quickly.

  It is recommended to configure the port type for all ports connected to hosts as edge ports.

- **normal** – is assumed to be connected to a switch, thus it tries to be converged by the RSTP learning/forwarding. However, if it does not receive any BPDUs, it is operationally moved to be edge.

- **network** – is assumed to be connected to a switch. If it does not receive any BPDUs, it is moved to discarding state.

Each of these configuration options is mutually exclusive.
Port type is configured using the command spanning-tree port type. It may be applied globally on
the switch (Config) level, which configures all switch interfaces. Another option is to configure
ports individually by entering the interface’s configuration mode.

- Global configuration:

```
switch (config)# spanning-tree port type {edge , normal , network} default
```

- Interface configuration:

```
switch (config interface ethernet <inf>)# spanning-tree port type {edge , normal, network}
```

### 5.9.3 BPDU Filter

Using BPDU filter prevents the CPU from sending/receiving BPDUs on specific ports.

BPDU filtering is configured per interface. When configured, the port does not send any BPDUs
and drops all BPDUs that it receives. To configure BPDU filter, use the following command:

```
switch (config interface ethernet <inf>)# spanning-tree 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.

### 5.9.4 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 ethernet <inf>)# spanning-tree port type <type> bpduguard
```

### 5.9.5 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 design-
nated bridge cannot disappear unless it sends an inferior BPU or brings the link down on a
point-to-point connection.

The loop guard configuration is only allowed on “network” port type.

If loop guard is enabled and the port does not receive BPDUs, the port is put into an inconsistent
state (blocking) until the port starts to receive BPDUs again. A port in the inconsistent state does
not transmit BPDUs. If BPDUs are received again, loop guard alters its inconsistent state condition. STP converges to a stable topology without the failed link or bridge after loop guard isolates the failure.

Disabling loop guard moves all loop-inconsistent ports to listening state.

To configure loop guard use the following command:

```
switch (config interface ethernet <inf>)# spanning-tree guard loop
```

### 5.9.6 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 ethernet <inf>)# spanning-tree guard root
```

### 5.9.7 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.

### 5.9.8 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 20 exhibits a typical RPVST network configuration to get a better utilization on the inter-switch trunk ports.
5.9.8.1 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. On x86 switch systems the limitation is 128 VLANs, and on PPC systems it ranges from 13-18 VLANs depending on the switch system. The more ports the switch system has the less VLANs it can support.

Table 51 - Supported VLANs by RPVST per Switch System

<table>
<thead>
<tr>
<th>Switch System Model</th>
<th>Number of Supported VLANs</th>
</tr>
</thead>
<tbody>
<tr>
<td>x86 systems</td>
<td>128</td>
</tr>
<tr>
<td>SX1012</td>
<td>17</td>
</tr>
<tr>
<td>SX1016</td>
<td>13</td>
</tr>
<tr>
<td>SX1024</td>
<td>13</td>
</tr>
<tr>
<td>SX1035</td>
<td>13</td>
</tr>
<tr>
<td>SX1036</td>
<td>13</td>
</tr>
</tbody>
</table>

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.
5.9.8.2 RPVST and RSTP Interoperability

**Figure 21: 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.

5.9.9 Commands

**spanning-tree**

```
spanning-tree  
no spanning-tree
```

Globally enables the spanning tree feature. The no form disables the spanning tree feature.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>Spanning tree is enabled.</td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Config</td>
</tr>
<tr>
<td>History</td>
<td>3.1.0000</td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
</tr>
<tr>
<td>------------</td>
<td>-------</td>
</tr>
</tbody>
</table>
| Example    | switch (config) # no spanning-tree  
            | switch (config) # |
| Related Commands | show spanning-tree |
| Note       |       |
### 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.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>mst</th>
<th>Multiple spanning tree.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>rst</td>
<td>Rapid spanning tree.</td>
</tr>
<tr>
<td></td>
<td>rpvst</td>
<td>Rapid per-VLAN spanning tree.</td>
</tr>
</tbody>
</table>

| Default | rst |

**Configuration Mode**
- `Config`

**History**
- 3.3.4150

**Role**
- `admin`

**Example**
```
switch (config)# spanning-tree mode mst
```

**Related Commands**

**Note**
- On x86 switch systems, the number of VLANs supported by RPVST are 128
- On PPC switch systems, the number of VLANs supported by RPVST are between 13-18
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.

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>forward-time</td>
<td>Controls how fast a port changes its spanning tree state from Blocking state to Forwarding state. Parameter range: 4-30 seconds.</td>
</tr>
<tr>
<td>hello-time</td>
<td>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.</td>
</tr>
<tr>
<td>max-age</td>
<td>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.</td>
</tr>
</tbody>
</table>

**Default**

forward-time: 15 seconds  
hello-time: 2 seconds  
max-age: 20 seconds

**Configuration Mode**

Config

**History**

3.1.0000

**Role**

admin

**Example**

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

**Related Commands**

show spanning-tree

**Note**

The following formula applies on the spanning tree timers:

\[2 \times (\text{ForwardTime} - 1) \geq \text{MaxAgeTime} \geq 2 \times (\text{Hello Time} + 1)\]
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.

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>edge</td>
<td>Assumes all ports are connected to hosts/servers.</td>
</tr>
<tr>
<td>bpdufilter</td>
<td>Configures to enable the spanning tree BPDU filter.</td>
</tr>
<tr>
<td>bpduguard</td>
<td>Configures to enable the spanning tree BPDU guard.</td>
</tr>
<tr>
<td>network</td>
<td>Assumes all ports are connected to switches and bridges.</td>
</tr>
<tr>
<td>normal</td>
<td>The port type (edge or network) determines according to the spanning tree operational mode.</td>
</tr>
</tbody>
</table>

**Default**

Normal

**Configuration Mode**

Config

**History**

3.1.0000

3.4.0008 Updated command syntax

**Role**

admin

**Example**

switch (config) # spanning-tree port type edge default
switch (config) #

**Related Commands**

show spanning-tree

**Note**
spanning-tree priority

spanning-tree priority <bridge-priority>
no spanning-tree priority

Sets the spanning tree bridge priority.
The no form of the command sets the bridge priority to default.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>bridge-priority</th>
</tr>
</thead>
<tbody>
<tr>
<td>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.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Default</th>
<th>32786</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuration Mode</td>
<td>Config</td>
</tr>
<tr>
<td>History</td>
<td>3.1.0000</td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
</tr>
</tbody>
</table>
| Example | switch (config) # spanning-tree priority 4096
switch (config) # |
| Related Commands | show spanning-tree |
| Note |
spanning-tree port-priority

    spanning-tree port-priority <priority>
    no spanning-tree port-priority

Configures the spanning-tree interface priority.
The no form of the command returns configuration to its default.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>priority</th>
<th>Spanning tree interface priority. The possible values are: 0, 16, 32,48, 64, 80, 96, 112, 128,144, 160, 176, 192, 208, 224, 240.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>128</td>
<td></td>
</tr>
</tbody>
</table>
| Configuration Mode| Config Interface Ethernet  
                  | Config Interface Port Channel  
                  | Config Interface MLAG Port Channel |
| History           | 3.1.0000 |                                                                                                                                 |
|                   | 3.3.4500 | Added MLAG port-channel configuration mode                                                                                         |
| Role              | admin    |                                                                                                                                 |
| Example           | switch (config) # interface ethernet 1/1  
                  | switch (config interface ethernet 1/1) # spanning-tree port-priority 16  
                  | switch (config interface ethernet 1/1) # |
| Related Commands  | show spanning-tree |
| Note              |                                                                                                                                 |
spanning-tree cost

spanning-tree cost <port cost>
no spanning-tree cost

Configures the interface cost of the spanning tree.
The no form of the command returns configuration to its default.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>port cost</td>
<td>Sets the spanning tree cost of an interface. Value range is 0-200000000.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Default</th>
<th>The default cost is derived from the speed.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>1Gbps 20000</td>
</tr>
<tr>
<td></td>
<td>10Gbps 2000</td>
</tr>
<tr>
<td></td>
<td>40Gbps 500</td>
</tr>
<tr>
<td></td>
<td>56Gbps 357</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Configuration Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>Config Interface Ethernet</td>
</tr>
<tr>
<td>Config Interface Port Channel</td>
</tr>
<tr>
<td>Config Interface MLAG Port Channel</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>History</th>
<th>Added MLAG port-channel configuration mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.1.0000</td>
<td></td>
</tr>
<tr>
<td>3.3.4500</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Role</th>
<th>admin</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>switch (config) # interface ethernet 1/1</td>
</tr>
<tr>
<td>switch (config interface ethernet 1/1) # spanning-tree cost 1000</td>
</tr>
<tr>
<td>switch (config interface ethernet 1/1) #</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Related Commands</th>
<th>show spanning-tree</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Note</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• LAG default cost is calculated by dividing the port speed by the number of active links in UP state. For example: if there were 4 links in the LAG out of which only two are in UP state, assuming the port speed is 10Gbps, the LAG cost will be 2000/2 = 1000.</td>
</tr>
<tr>
<td></td>
<td>• When configuring the cost for a LAG, the cost will be fixed to this configuration, no matter what the number of active links (UP state) in the LAG is.</td>
</tr>
<tr>
<td></td>
<td>• Unstable network may cause the LAG cost to change dynamically assuming the cost parameter is not configured for anything else other than default.</td>
</tr>
</tbody>
</table>
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.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>default</th>
<th>According to global configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>edge</td>
<td>Assumes all ports are connected to hosts/servers.</td>
</tr>
<tr>
<td></td>
<td>normal</td>
<td>The port type (edge or network) determines according to the spanning tree operational mode.</td>
</tr>
<tr>
<td></td>
<td>network</td>
<td>Assumes all ports are connected to switches and bridges.</td>
</tr>
<tr>
<td></td>
<td>bpdufilter</td>
<td>Configures to enable the spanning tree BPDU filter.</td>
</tr>
<tr>
<td></td>
<td>bpduguard</td>
<td>Configures to enable the spanning tree BPDU guard.</td>
</tr>
</tbody>
</table>

| Default | Globally defined by the command “spanning-tree port type <port-type> default” |

<table>
<thead>
<tr>
<th>Configuration Mode</th>
<th>Config Interface Ethernet</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Config Interface Port Channel</td>
</tr>
<tr>
<td></td>
<td>Config Interface MLAG Port Channel</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>History</th>
<th>3.1.0000</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>3.3.4500</td>
</tr>
</tbody>
</table>

| Role | admin |

| Example | switch (config) # interface ethernet 1/1  
|---------|------------------------------------------|
|         | switch (config interface ethernet 1/1) # spanning-tree port type edge  
|         | switch (config interface ethernet 1/1) # |

| Related Commands | show spanning-tree |

| Note | |


spanning-tree guard

spanning-tree guard {loop | root}
no spanning-tree guard {loop | root}

Configures spanning-tree guard.
The no form of the command returns configuration to default.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>loop</td>
<td>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.</td>
</tr>
<tr>
<td>root</td>
<td>Enables root-guard on the interface. If root-guard is enabled on the interface, the interface will never be selected as root port.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Default</th>
<th>loop-guard and loop-guard are disabled.</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Configuration Mode</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Config Interface Ethernet</td>
<td></td>
</tr>
<tr>
<td>Config Interface Port Channel</td>
<td></td>
</tr>
<tr>
<td>Config Interface MLAG Port Channel</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>History</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.1.0000</td>
<td></td>
</tr>
<tr>
<td>3.3.4500</td>
<td>Added MLAG port-channel configuration mode</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Role</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>admin</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Example</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>switch (config) # interface ethernet 1/1</td>
<td></td>
</tr>
<tr>
<td>switch (config interface ethernet 1/1) # spanning-tree guard root</td>
<td></td>
</tr>
<tr>
<td>switch (config interface ethernet 1/1) #</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Related Commands</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>show spanning-tree</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Note</th>
<th>Details</th>
</tr>
</thead>
</table>
### spanning-tree bpdufilter

```plaintext
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.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>disable</td>
<td>Disables the BPDU filter on this port.</td>
</tr>
<tr>
<td>enable</td>
<td>Enables the BPDU filter on this port.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Default</th>
<th>BPDU filter is disabled.</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Configuration Mode</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Config Interface Ethernet</td>
<td></td>
</tr>
<tr>
<td>Config Interface Port Channel</td>
<td></td>
</tr>
<tr>
<td>Config Interface MLAG Port Channel</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>History</th>
<th>3.1.0000</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Role</th>
<th>admin</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Example</th>
</tr>
</thead>
</table>
| switch (config) # interface ethernet 1/1
| switch (config interface ethernet 1/1) # spanning-tree bpdufilter enable |

<table>
<thead>
<tr>
<th>Related Commands</th>
<th>show spanning-tree</th>
</tr>
</thead>
</table>

| Note | This command can be used when the switch is connected to hosts. |
### clear spanning-tree counters

**clear spanning-tree counters**

Clears the spanning-tree counters.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>N/A</td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Config</td>
</tr>
<tr>
<td>History</td>
<td>3.1.0000</td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
</tr>
</tbody>
</table>
| Example             | switch (config) # clear spanning-tree counters  
switch (config) #  
show spanning tree |

**Note**
### spanning-tree mst max-hops

```
spanning-tree mst max-hops <max-hops>
no spanning-tree mst max-hops
```

Specifies the max hop value inserts into BPDUs that sent out as the root bridge.
The no form of the command sets the parameter to its default value.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>max-hops</td>
<td>Max hop value. The range is 6-40.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Default</th>
<th>20</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Configuration Mode</th>
<th>Config</th>
</tr>
</thead>
<tbody>
<tr>
<td>History</td>
<td>3.3.4150</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Role</th>
<th>admin</th>
</tr>
</thead>
</table>

| Example | switch (config)# spanning-tree mst max-hops 20  
|---------| switch (config)# |

<table>
<thead>
<tr>
<th>Related Commands</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Note</th>
</tr>
</thead>
</table>
| - The max hop setting determines the number of bridges in an MST region that a BPDU can traverse before it is discarded  
| - This command is available when global STP mode is set to MST |
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.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>mst-instance</th>
<th>MST instance. Range is 1-64.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>priority</td>
<td>MST instance port priority. Possible values are: 0, 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152, 53248, 57344, 61440</td>
</tr>
</tbody>
</table>

Default 32768

Configuration Mode Config

History 3.3.4150

Role admin

Example
switch (config)# spanning-tree mst 1 priority 32768
switch (config)#

Related Commands

Note
- The bridge priority is the four most significant digits of the bridge ID, which is used by spanning tree algorithms to select the root bridge and choose among redundant links. Bridge ID numbers range from 0-65535 (16 bits); bridges with smaller bridge IDs are elected over other bridges.
- This command is available when global STP mode is set to MST
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.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>mst-instance</th>
<th>MST instance. Range is 1-64.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>vlan &lt;vlan-range&gt;</td>
<td>A single VLAN or a range of VLANs. The format is &lt;vlan&gt; or &lt;from-vlan&gt;-&lt;to-vlan&gt;.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Default</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuration Mode</td>
<td>Config</td>
</tr>
<tr>
<td>History</td>
<td>3.3.4150</td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
</tr>
</tbody>
</table>

**Example**

```
switch (config)# spanning-tree mst 1 vlan 10-20
switch (config)#
```

**Related Commands**

**Note**

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.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>number</td>
<td>The MST revision number. Range is 0-65535.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Default</th>
<th>0</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Configuration Mode</th>
<th>Config</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>History</th>
<th>3.3.4150</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Role</th>
<th>admin</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>switch (config)# spanning-tree mst revision 1</td>
</tr>
<tr>
<td>switch (config)#</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Related Commands</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Note</th>
</tr>
</thead>
<tbody>
<tr>
<td>• 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</td>
</tr>
<tr>
<td>• This command is available when global STP mode is set to MST</td>
</tr>
</tbody>
</table>
**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.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>name</th>
<th>MST name: Up to 32 characters.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>N/A</td>
<td></td>
</tr>
</tbody>
</table>

**Configuration Mode**

Config

**History**

3.3.4150

**Role**

admin

**Example**

```
switch (config)# spanning-tree mst name my-mst
switch (config)#
```

**Related Commands**

**Note**

- The name is one of three parameters, along with the MST revision number and VLAN-to-instance map, that identifies the switch’s MST region
- This command is available when global STP mode is set to MST
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.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>mst-instance</th>
<th>MSTP instance. Possible range is 1-64.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>role</td>
<td>Values: “primary” or “secondary”.</td>
</tr>
</tbody>
</table>

Default:
primary

Configuration Mode:
Config

History:
3.3.4150

Role:
admin

Example:
```
switch (config)# spanning-tree mst name my-mst
switch (config)#
```

Related Commands:

Note:
- The root command is a way to automate a system configuration while ‘playing’ with the priority field. The priority field granularity may be too explicit for some users in case you wish to have 2 levels of priority (primary and secondary). So by default all the switches get the same priority and while using the root option you can get the role of master and backup by setting the priority field to a predefined value.
- This command is available when global STP mode is set to MST.
spanning-tree mst port-priority

description of command

Changes the spanning tree mode.
The no form of the command sets the parameter to its default value.

Syntax Description

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>mst-instance</th>
<th>MST instance. Range is 0-4094.</th>
</tr>
</thead>
<tbody>
<tr>
<td>priority</td>
<td>priority</td>
<td>MST instance port priority. Valid values are: 0, 16, 32, 48, 64, 80, 96, 112, 128, 144, 160, 176, 192, 208, 224 and 240.</td>
</tr>
</tbody>
</table>

Default
rst

Configuration Mode

<table>
<thead>
<tr>
<th>Configuration Mode</th>
<th>Config Interface Ethernet</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Config Interface Port Channel</td>
</tr>
</tbody>
</table>

History
3.3.4150

Role
admin

Example

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

Related Commands

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.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>mst-instance</td>
<td>MST instance. Range is 1-64.</td>
</tr>
<tr>
<td>cost-value</td>
<td>MST instance port cost. Range is 0-200000000.</td>
</tr>
</tbody>
</table>

| Default | 2000 for 10Gb/s, 500 for 40Gb/s, 20000 for 1Gb/s, 357 for 56Gb/s |

<table>
<thead>
<tr>
<th>Configuration Mode</th>
<th>Config Interface Port Channel</th>
</tr>
</thead>
<tbody>
<tr>
<td>History</td>
<td>3.3.4150</td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
</tr>
</tbody>
</table>
| Example            | switch (config interface ethernet 1/1)# spanning-tree mst 1 cost 4000
switch (config interface port-channel 1)# spanning-tree mst 1 cost 4000
switch (config)# |

Related Commands

Note 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.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>secs</th>
<th>Parameter range: 4-30 seconds.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>15 seconds</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Configuration Mode</th>
<th>Config</th>
</tr>
</thead>
<tbody>
<tr>
<td>History</td>
<td>3.4.1100</td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
</tr>
</tbody>
</table>

**Example**

```
switch (config) # spanning-tree vlan 10 forward-time 15
```

**Related Commands**

```
show spanning-tree
```

**Note**

- The following formula applies on the spanning tree timers:
  
  $2 \times (\text{ForwardTime} - 1) \geq \text{MaxAgeTime} \geq 2 \times (\text{Hello Time} + 1)$

- This command is available when global STP mode is set to RPVST
### spanning-tree vlan hello-time

```plaintext
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.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>secs Parameter range: 1-2 seconds.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>2 seconds</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Configuration Mode</th>
<th>Config</th>
</tr>
</thead>
<tbody>
<tr>
<td>History</td>
<td>3.4.1100</td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
</tr>
</tbody>
</table>

#### Example

```plaintext
switch (config) # spanning-tree vlan 10 hello-time 2
```

**Related Commands**

- show spanning-tree

**Note**

- The following formula applies on the spanning tree timers:
  \[2 \times (\text{ForwardTime} - 1) \geq \text{MaxAgeTime} \geq 2 \times (\text{Hello Time} + 1)\]
- This command is available when global STP mode is set to RPVST
**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.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>secs</th>
<th>Parameter range: 6-40 seconds.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>20</td>
<td>seconds</td>
</tr>
</tbody>
</table>

**Configuration Mode**  
`Config`

**History**  
3.4.1100

**Role**  
`admin`

**Example**  
`switch (config) # spanning-tree vlan 10 max-age 20`

**Related Commands**  
`show spanning-tree`

**Note**  
- The following formula applies on the spanning tree timers:  
  \[2 \times (\text{ForwardTime} - 1) \geq \text{MaxAgeTime} \geq 2 \times (\text{Hello Time} + 1)\]
- This command is available when global STP mode is set to RPVST
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.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>priority Possible values are: 0, 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152, 53248, 57344, 61440.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>32768</td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Config</td>
</tr>
<tr>
<td>History</td>
<td>3.4.1100</td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
</tr>
<tr>
<td>Example</td>
<td>switch (config) # spanning-tree vlan 10 priority 32768</td>
</tr>
<tr>
<td>Related Commands</td>
<td>show spanning-tree</td>
</tr>
</tbody>
</table>
| Note               | • The following formula applies on the spanning tree timers:  
                        2*(ForwardTime -1)>=MaxAgeTime >= 2*(Hello Time + 1)  
                        • This command is available when global STP mode is set to RPVST |
show spanning-tree

Displays spanning tree information.

**Syntax Description**

N/A

**Default**

N/A

**Configuration Mode**

Any Command Mode

**History**

3.1.0000

3.4.1100 Updated Example with R and G flags

**Role**

admin

**Example**

```
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

<table>
<thead>
<tr>
<th>Interface</th>
<th>Role</th>
<th>Sts</th>
<th>Cost</th>
<th>Prio</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Eth1/9</td>
<td>Designated</td>
<td>Forwarding</td>
<td>500</td>
<td>128</td>
<td>normal</td>
</tr>
<tr>
<td>Eth1/22</td>
<td>Designated</td>
<td>Discarding(R)</td>
<td>500</td>
<td>128</td>
<td>normal</td>
</tr>
<tr>
<td>Eth1/32</td>
<td>Root</td>
<td>Forwarding</td>
<td>500</td>
<td>128</td>
<td>normal</td>
</tr>
<tr>
<td>Eth1/39</td>
<td>Disabled</td>
<td>Discarding(G)</td>
<td>2000</td>
<td>128</td>
<td>normal</td>
</tr>
</tbody>
</table>

switch (config) #
```

**Related Commands**

- clear spanning-tree counters
- spanning-tree

**Note**
show spanning-tree detail

Syntax Description: Displays detailed spanning-tree configuration and statistics.

Default: N/A

Configuration Mode: Any Command Mode

History: 3.1.0000

Role: admin

Example:
```
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 has priority 32768, address 00:02:c9:96:c6:d0
  Configured hello time 2, max age 20, forward delay 15
  Current root has priority 32768, address 00:02:c9:7a:e9:40
  Root port is Eth1/32( Ethernet1/32),cost of root path is 1000
  Number of topology changes 21,last change occurred 00:00:03 ago
  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) #
```

Related Commands:
- clear spanning-tree counters
- spanning-tree

Note:
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.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>ethernet</th>
<th>Ethernet interface.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>port-channel</td>
<td>LAG instance.</td>
</tr>
<tr>
<td></td>
<td>mlag-port-channel</td>
<td>MLAG instance.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Default</th>
<th>N/A</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Configuration Mode</th>
<th>Any Command Mode</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>History</th>
<th>3.3.4150</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Role</th>
<th>admin</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Example</th>
</tr>
</thead>
</table>
| 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 |

<table>
<thead>
<tr>
<th>Related Commands</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear spanning-tree counters</td>
</tr>
<tr>
<td>spanning-tree</td>
</tr>
</tbody>
</table>

| Note | |
|------|
**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.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Details</th>
<th>Displays detailed multi-spanning-tree configuration and statistics.</th>
</tr>
</thead>
<tbody>
<tr>
<td>ethernet</td>
<td>Ethernet interface.</td>
<td></td>
</tr>
<tr>
<td>port-channel</td>
<td>LAG instance.</td>
<td></td>
</tr>
<tr>
<td>mlag-port-channel</td>
<td>MLAG instance.</td>
<td></td>
</tr>
</tbody>
</table>

**Default**

N/A

**Configuration Mode**

Any Command Mode

**History**

3.3.4150

**Role**

admin

**Example**

```
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) #

**Related Commands**

clear spanning-tree counters
spanning-tree

**Note**
show spanning-tree root

Syntax Description
Displays root multi-spanning-tree information.

Default
N/A

Configuration Mode
Any Command Mode

History
3.3.4150

Role
admin

Example
```
switch (config) # show spanning-tree root

<table>
<thead>
<tr>
<th>Instance</th>
<th>Priority</th>
<th>MAC addr</th>
<th>Root Cost</th>
<th>Hello Time</th>
<th>Max Age</th>
<th>FWD Dly</th>
<th>Root Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>MST0</td>
<td>32768</td>
<td>00:02:c9:71:ed:40</td>
<td>500</td>
<td>2</td>
<td>20</td>
<td>15</td>
<td>Eth1/20</td>
</tr>
<tr>
<td>MST1</td>
<td>32768</td>
<td>00:02:c9:71:f0:c0</td>
<td>0</td>
<td>2</td>
<td>20</td>
<td>15</td>
<td>-</td>
</tr>
<tr>
<td>MST2</td>
<td>0</td>
<td>00:02:c9:71:f0:c0</td>
<td>0</td>
<td>2</td>
<td>20</td>
<td>15</td>
<td>-</td>
</tr>
<tr>
<td>MST3</td>
<td>32768</td>
<td>00:02:c9:71:f0:c0</td>
<td>0</td>
<td>2</td>
<td>20</td>
<td>15</td>
<td>-</td>
</tr>
</tbody>
</table>
```

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.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>vid</th>
<th>VLAN ID. Range is also supported. Format: &lt;vid1&gt;-&lt;vid2&gt;</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>detail</td>
<td>Displays detailed RPVST configuration and statistics.</td>
</tr>
<tr>
<td></td>
<td>ethernet</td>
<td>Ethernet interface.</td>
</tr>
<tr>
<td></td>
<td>port-channel</td>
<td>LAG instance.</td>
</tr>
<tr>
<td></td>
<td>mlag-port-channel</td>
<td>MLAG instance.</td>
</tr>
</tbody>
</table>

Default: N/A

Configuration Mode: Any Command Mode

History: 3.4.1100

Role: admin

Example:

switch (config) # show spanning-tree vlan 10

Switch ethernet-default

Spanning tree protocol is enabled rpvst

Spanning tree force version:2

Vlan 10

Root ID

| Priority 10 |
| Address 00:02:c9:96:c6:d0 |
| This bridge is the root |
| Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec |

Bridge ID

| Priority 10 |
| Address 00:02:c9:96:c6:d0 |
| Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec |

L - Loop Inconsistent

<table>
<thead>
<tr>
<th>Interface</th>
<th>Role</th>
<th>Sts</th>
<th>Cost</th>
<th>Prio</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mpo21</td>
<td>Designated</td>
<td>Forwarding</td>
<td>500</td>
<td>128</td>
<td>normal</td>
</tr>
<tr>
<td>Mpo20</td>
<td>Back Up</td>
<td>Discarding</td>
<td>500</td>
<td>128</td>
<td>normal</td>
</tr>
</tbody>
</table>

switch (config) #
| Related Commands   | clear spanning-tree counters  
|--------------------|-------------------------------  
|                    | spanning-tree                 
| Note               |                               

5.10 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.

5.10.1 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 theflowing 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.

5.10.2 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 22: MLNX-OS and OpenFlow Pipeline

![MLNX-OS and OpenFlow Pipeline Diagram]
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 52 presents a general summary of the capabilities of the OpenFlow 1.3 pipeline, which are described in detail further on in the document.

**Table 52 - OpenFlow 1.3 Pipeline Capabilities Summary Table**

<table>
<thead>
<tr>
<th>Table</th>
<th>Match</th>
<th>Actions</th>
<th>Group</th>
<th>Meters</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACLs [0-249]</td>
<td>• in_port &lt;br&gt; • dl_src &lt;br&gt; • dl_dst &lt;br&gt; • dl_type &lt;br&gt; • vlan_vid &lt;br&gt; • vlan_pcp &lt;br&gt; • ip_src &lt;br&gt; • ip_dst &lt;br&gt; • ipv6_dst &lt;br&gt; • ipv6_src &lt;br&gt; • ip_proto &lt;br&gt; • ip_dscp &lt;br&gt; • ip_ecn &lt;br&gt; • ip_ttl &lt;br&gt; • 14_src_port &lt;br&gt; • 14_dst_port &lt;br&gt; • metadata 0xFFF (Dynamic key) (Arbitrary mask)</td>
<td>• Push/pop VLAN &lt;br&gt; • SET_TTL &lt;br&gt; • DEC_TTL &lt;br&gt; • Set queue &lt;br&gt; • Eth SRC/DST MAC &lt;br&gt; • VLAN ID &lt;br&gt; • PCP &lt;br&gt; • DSCP &lt;br&gt; • ECN &lt;br&gt; • Output &lt;br&gt; • Group &lt;br&gt; • Meters &lt;br&gt; • Normal</td>
<td>• ALL - Output ports &lt;br&gt; • Select - {weights} Output ports (without LAG) &lt;br&gt; • FF - Output ports</td>
<td>• KBPS/PKTS - {Burst} &lt;br&gt; • Drop</td>
</tr>
<tr>
<td>FDB [250]</td>
<td>• vlan_vid &lt;br&gt; • dl_dst (Exact match)</td>
<td>• OUTPUT &lt;br&gt; • DROP &lt;br&gt; • Normal</td>
<td>Select - {Weights} Output ports (without LAG)</td>
<td>N/A</td>
</tr>
<tr>
<td>Router [251]</td>
<td>• ipv4_dst &lt;br&gt; • ipv6_dst (LPM)</td>
<td>• DEC_TTL &lt;br&gt; • SET_DMAC &lt;br&gt; • OUTPUT &lt;br&gt; • DROP (Must have DEC_TTL and SET_DMAC when Output action is implemented)</td>
<td>Select - {Weights} Output ports + set_dmac + dec_ttl</td>
<td>N/A</td>
</tr>
</tbody>
</table>

**5.10.2.1 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
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.

### 5.10.2.1.1 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”.

5.10.2.1.2 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/pktps limit
• OFPIT_WRITE_METADATA – writes meta-data with mask <METADATA>/0xFFF
• OFPIT_EXPERIMENTE – sends the packet for processing by another controller
• OFPIT_APPLY_ACTIONS – applies certain actions specified in the section below

5.10.2.1.3 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

5.10.2.1.4 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

5.10.2.1.5 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

5.10.2.2 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.

5.10.2.2.1 Supported FDB Apply Actions

• OFPAT_OUTPUT – the packet is sent out to a port (may be controller port)
• DROP – drops packet
• Normal
5.10.2.2 Supported FDB Matching Rules

- OXM_OF_VLAN_VID – matches VLAN ID
- OXM_OF_ETH_DST – matches destination MAC address

5.10.2.3 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).

5.10.2.3.1 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.

5.10.2.3.2 Supported Router Set Fields

- OXM_OF_ETH_DST – sets the destination MAC address of the packet

5.10.2.3.3 Supported Router Matching Rules

- OXM_OF_IPV4_DST – matches destination IPv4 address
- OXM_OF_IPV6_DST – matches destination IPv6 address

5.10.3 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:

```bash
switch (config) # interface ethernet 1/1-1/4 openflow mode hybrid
```

Step 3. Configure the OpenFlow controller IP and TCP port. Run:

```bash
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:

```bash
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
```

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).

### 5.10.4 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:

```bash
switch (config) # crypto certificate name my-openflow public-cert pem "-----BEGIN CERTIFICATE-----
> MIIDYzCCAkscCQC9EQEPMu5xNBzANBgkqihkG9w0BAQsFADBeMQswCQYDVQQGEwJJ...
> fEt2u9taB1d19480xDsGUXwUDX4YOa/bQDjp99z+cEUXUe2eYzeEwnTdrCzP2uQo
> -----END CERTIFICATE-----"
Successfully installed certificate with name 'my-openflow'
```

Step 2. Import key of certificate. Run:

```bash
switch (config) # crypto certificate name my-openflow private-key pem "-----BEGIN RSA PRIVATE KEY-----
> MIIEpAIIBA/KCAQEAypJn2kwbhmt71Kf/M06cy7QmWWhHCozz2RwuNGKse+MxSmfC...
> QAw0VgR11SyIEnYU+X0rMhc/9tqUH/8C7mBKwj7dcccMnRNw2djsjg==
> -----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-----
> MIIDjzCCCAenegAwIBAgIJALVou4mcQtx1MA0GCSqGSIb3DQEBCwUAMF4xCzAJBgNV
> BAUEAwEBбиgY29tcGxldGluZzETAQIBAQIXMTExMS4xNjIuMjIuMjExMDAw
> ...>
> +zfQIOCF58gY4BDc73W4ugr38mqIA8UXAMPwqjCbk4NyOh0rJ1P6WT8fYzvunct
> -----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: 14e1d36035c7a5fe9f7f0f423572c9954cb9fac

  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: 0xbd10f6cebb18cd07
  SHA-1 Fingerprint: 1e0e3302182ab56f2cbe3ca21722dec55299d670

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: 9855536f6ee0177356ffbd547f803bc83fb4c6

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:

```bash
switch (config) # controller-ip 10.10.10.10 tls
```

### 5.10.5 Commands

**protocol openflow**

```
protocol openflow
no protocol openflow
```

Unhides the OpenFlow commands. The no form of the command hides the OpenFlow commands.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>no protocol openflow</td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Config</td>
</tr>
<tr>
<td>History</td>
<td>3.3.4200</td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
</tr>
</tbody>
</table>
| Example            | switch (config) # protocol openflow
|                    | switch (config) # |

**Related Commands**

**Note**
openflow description (SwitchX)

openflow description <string>

Sets the OpenFlow description.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>string</th>
<th>Free string.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>N/A</td>
<td></td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Config</td>
<td></td>
</tr>
<tr>
<td>History</td>
<td>3.3.4302</td>
<td>3.6.1002</td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
<td></td>
</tr>
<tr>
<td>Example</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

```
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
```

Related Commands

| Note | 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.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>no openflow mode</td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Config Interface Ethernet</td>
</tr>
<tr>
<td>History</td>
<td>3.3.4200</td>
</tr>
</tbody>
</table>
|                    | 3.6.2100  
|                    | Updated Note section |
| Role               | admin |
| Example            | switch (config interface ethernet 1/1)# openflow mode hybrid
|                    | switch (config interface ethernet 1/1)# |
| Related Commands   | On Spectrum based systems, it is possible to run “interface port-channel <port number> openflow mode hybrid” |
| Note               | |


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.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>ip-address</th>
<th>The IPv4 address of the OpenFlow controller</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>tls</td>
<td>Configures secure connection to OpenFlow controller</td>
</tr>
<tr>
<td></td>
<td>tcp-port</td>
<td>Sets the TCP port number of the OpenFlow controller</td>
</tr>
</tbody>
</table>

**Default**
TCP port 6633

**Configuration Mode**
Config OpenFlow

**History**
3.6.1002
3.6.2002 Added “tls” parameter

**Role**
admin

**Example**
```
switch (config openflow) # controller-ip 10.10.10.10 tls tcp-port 6633
```

**Related Commands**

**Note**
This command is only supported on Spectrum™ based switch systems
controller-ip

openflow controller-ip <ip-address> [tcp-port <tcp-port>]
o 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.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip-address</td>
<td>The IPv4 address of the OpenFlow controller</td>
</tr>
<tr>
<td>tcp-port</td>
<td>Sets the TCP port number of the OpenFlow controller</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>TCP port 6633</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Configuration Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>Config OpenFlow</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>History</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.3.4200</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>admin</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>switch (config openflow) # controller-ip 10.10.10.10 tcp-port 6633</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Related Commands</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Note</th>
</tr>
</thead>
<tbody>
<tr>
<td>This command is only supported on SwitchX based switch systems</td>
</tr>
</tbody>
</table>
**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.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>value</td>
<td>The most significant 16 bits of the agent data-path ID. Range is 0x0000-0xFFFF in hexa.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Default</th>
<th>0x0000</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Configuration Mode</th>
<th>Config OpenFlow</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>History</th>
<th>3.3.4200</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Role</th>
<th>admin</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>switch (config openflow) # datapath-id 0x1234</td>
</tr>
<tr>
<td>switch (config openflow) #</td>
</tr>
</tbody>
</table>

**Related Commands**

**Note**
forward-to-controller

forward-to-controller {[ospf] [lldp] [arp-unicast] [arp-broadcast] all | none}

Forwards the selected traffic types to the controller from all the ports on which OpenFlow enabled.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ospf</td>
<td>Forwards OSPF traffic to the controller</td>
</tr>
<tr>
<td>lldp</td>
<td>Forwards LLDP traffic to the controller</td>
</tr>
<tr>
<td>arp-unicast</td>
<td>Forwards ARP-unicast traffic to the controller</td>
</tr>
<tr>
<td>arp-broadcast</td>
<td>Forwards ARP-broadcast traffic to the controller</td>
</tr>
<tr>
<td>all</td>
<td>Forwards all traffic types to the controller</td>
</tr>
<tr>
<td>none</td>
<td>Forwards no traffic to the controller</td>
</tr>
</tbody>
</table>

Default: None

Configuration Mode: Config OpenFlow

History: 3.3.4200

Role: admin

Example:
```
switch (config openflow) # forward-to-controller all
switch (config openflow) #
```

Related Commands

Note: 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.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>table_id</th>
<th>OpenFlow table ID for adding/removing key values. Can be one ID or range. Valid values: 0-249.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>key_list</td>
<td>Key value(s)</td>
</tr>
</tbody>
</table>

| Default | TBD |

<table>
<thead>
<tr>
<th>Configuration Mode</th>
<th>Any Command Mode</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>History</th>
<th>3.6.3004</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Role</th>
<th>admin</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Example</th>
<th>switch (config) # openflow table 1 match-keys metadata ip_proto</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Related Commands</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Note</th>
<th>• OpenFlow match rules are installed according to the configured match keys</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• New match keys are configured only when the table is empty (i.e. does not contain any rules)</td>
</tr>
<tr>
<td></td>
<td>• This command is only supported on Spectrum™ based switch systems</td>
</tr>
</tbody>
</table>

---
show openflow

Displays general information about the OpenFlow protocol configuration.

### Syntax Description
N/A

### Default
None

### Configuration Mode
Any Command Mode

### History
- **3.3.4200**
- **3.3.4302** Removed flow-id parameter
- **3.6.1002** Updated Example

### Role
admin

### Example
```
switch (config) # show openflow
OpenFlow Version: OpenFlow 1.3
Datapath ID: ffff7cfe90e600c0
Controllers Information:

<table>
<thead>
<tr>
<th>Controller</th>
<th>State</th>
<th>Role</th>
<th>Changed (sec)</th>
<th>Last Error</th>
</tr>
</thead>
<tbody>
<tr>
<td>tcp:1.1.1.1:6633</td>
<td>BACKOFF</td>
<td>other</td>
<td>3</td>
<td>Connection timed out</td>
</tr>
<tr>
<td>tcp:10.10.10.10:6633</td>
<td>ACTIVE</td>
<td>other</td>
<td>2067</td>
<td>N/A</td>
</tr>
<tr>
<td>tcp:10.10.10.30:6633</td>
<td>ACTIVE</td>
<td>other</td>
<td>2067</td>
<td>N/A</td>
</tr>
</tbody>
</table>

Mapping of OpenFlow ports to their OpenFlow numbers:
```
```
<table>
<thead>
<tr>
<th>Interface</th>
<th>OF-Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>Eth1/12</td>
<td>OF107</td>
</tr>
<tr>
<td>Eth1/9</td>
<td>OF109</td>
</tr>
<tr>
<td>Eth1/10</td>
<td>OF111</td>
</tr>
<tr>
<td>Eth1/7</td>
<td>OF113</td>
</tr>
<tr>
<td>Eth1/8</td>
<td>OF115</td>
</tr>
<tr>
<td>Eth1/3</td>
<td>OF121</td>
</tr>
<tr>
<td>Eth1/4</td>
<td>OF123</td>
</tr>
</tbody>
</table>
```

### Related Commands

### Note
This command is only supported on Spectrum™ based switch systems
show openflow detail

Displays detailed information about the OpenFlow protocol.

**Syntax Description**
N/A

**Default**
None

**Configuration Mode**
Any Command Mode

**History**
3.3.4200
3.6.1002 Updated Example

**Role**
admin

**Example**
```
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
```

**Related Commands**

**Note**
This command is only supported on SwitchX based switch systems
show openflow flows

Displays information about the OpenFlow flows.

**Syntax Description**  
N/A

**Default**  
None

**Configuration Mode**  
Any Command Mode

**History**  
3.3.4302

3.6.1002 Updated Example

**Role**  
admin

**Example**

```
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=467.984s, table=0, n_packets=0, n_bytes=0, send_flow_rem priority=1000 actions=drop
  cookie=0x0, duration=467.984s, table=0, n_packets=0, n_bytes=0, send_flow_rem priority=1000 actions=drop
  cookie=0x0, duration=467.984s, table=0, n_packets=0, n_bytes=0, send_flow_rem priority=1000 actions=drop
  cookie=0x0, duration=467.984s, table=0, n_packets=0, n_bytes=0, send_flow_rem priority=1000 actions=drop
```

**Related Commands**

```

```
show openflow statistics

Displays information about the OpenFlow flows.

**Syntax Description**

N/A

**Default**

None

**Configuration Mode**

Any Command Mode

**History**

3.3.4302

3.6.1002 Updated Example

**Role**

admin

**Example**

switch (config) # show openflow statistics

**Related Commands**

**Note**

This command is only supported on SwitchX based switch systems
### show openflow tables

**Syntax Description**
Displays information about the OpenFlow tables (size, type, etc.).

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>None</td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Any Command Mode</td>
</tr>
<tr>
<td>History</td>
<td>3.3.4200</td>
</tr>
<tr>
<td></td>
<td>3.6.1002 Added Example</td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
</tr>
</tbody>
</table>
| Example            | switch (config) # show openflow tables  
|                    | Table id: 0  
|                    | Maximum table size: 1000, 0 in use  
|                    | Key: 12 tuple ACL  
|                    | Supported actions: Modify VID, Modify PCP, Strip VID |

**Related Commands**

- 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.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>detail</td>
<td>Displays detailed information about the OpenFlow protocol.</td>
</tr>
<tr>
<td>tables</td>
<td>Displays information about the OpenFlow tables (size, type, etc.).</td>
</tr>
<tr>
<td>flows &lt;id&gt;</td>
<td>Displays specific flows inside the OpenFlow tables. ID may be a range (e.g. 1-10).</td>
</tr>
<tr>
<td>statistics</td>
<td>Displays OpenFlow statistics.</td>
</tr>
</tbody>
</table>

**Default**

None

**Configuration Mode**

Any Command Mode

**History**

3.3.4200

3.3.4302

Removed flow-id parameter

Added “flows” and “statistics” parameters

**Role**

admin

**Example**

```
switch (config) # show openflow flows
```

**Related Commands**

- [Please list related commands here.]

**Note**

This command is only supported on SwitchX based switch systems
### show openflow groups

**show openflow groups**

Displays all the configured OpenFlow groups.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>N/A</td>
</tr>
<tr>
<td><strong>Configuration Mode</strong></td>
<td>Any Command Mode</td>
</tr>
<tr>
<td><strong>History</strong></td>
<td>3.6.3004</td>
</tr>
<tr>
<td><strong>Role</strong></td>
<td>admin</td>
</tr>
</tbody>
</table>
| **Example**        | 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 |
| **Related Commands** | |
| **Note**           | This command is only supported on Spectrum™ based switch systems |
**show openflow meters**

`show openflow meters [<ID>]`

Displays all/specified OpenFlow meters.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th></th>
<th>Requested meter ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>N/A</td>
<td></td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Any Command Mode</td>
<td></td>
</tr>
<tr>
<td>History</td>
<td>3.6.3004</td>
<td></td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
<td></td>
</tr>
</tbody>
</table>

**Example**

```
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
```

**Related Commands**

**Note**

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.

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>NUM</th>
<th>NUM range: 0-252</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>summary</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Displays given OpenFlow flow table summary</td>
</tr>
</tbody>
</table>

**Default**

N/A

**Configuration Mode**

Any Command Mode

**History**

3.6.3004

**Role**

admin

**Example**

```
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
```

**Related Commands**

**Note**

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.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>cookie</th>
<th>Requested cookie ID in the following format: cookie_id.cookie_id/mask_id (e.g. 0x2A, 0x12/0x2)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>N/A</td>
<td></td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Any Command Mode</td>
<td></td>
</tr>
<tr>
<td>History</td>
<td>3.6.3004</td>
<td></td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
<td></td>
</tr>
</tbody>
</table>
| Example            |        | switch (config) # show openflow flows cookie 0x11
OFFST_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
OFFST_FLOW reply (OF1.3) (xid=0x2):
cookie=0x22, duration=3.970s, table=1, n_packets=0, n_bytes=0,
in_port=127 actions=drop |

Related Commands

Note
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
**show openflow table match-keys**

*show openflow table <table_id>-<table_id> match-keys*

Displays configured ACL keys in OpenFlow table.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>table_id</th>
<th>OpenFlow table ID for adding/removing key values. Can be one ID or range. Valid values: 0-249.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>N/A</td>
<td></td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Any Command Mode</td>
<td></td>
</tr>
<tr>
<td>History</td>
<td>3.6.3004</td>
<td></td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
<td></td>
</tr>
<tr>
<td>Example</td>
<td></td>
<td>switch (config) # show openflow table 2 match-keys</td>
</tr>
</tbody>
</table>

```
Table: 2
Pending keys:

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
```

**Related Commands**

**Note**

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.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>table_id</th>
<th>OpenFlow table ID for adding/removing key values. Can be one ID or range. Valid values: 0-249.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>N/A</td>
<td></td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Any Command Mode</td>
<td></td>
</tr>
<tr>
<td>History</td>
<td>3.6.3004</td>
<td></td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
<td></td>
</tr>
<tr>
<td>Example</td>
<td>switch (config) # show openflow table 2 match-keys supported</td>
<td></td>
</tr>
</tbody>
</table>

<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>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>

Related Commands

Note This command is only supported on Spectrum™ based switch systems
5.11 Network Virtualization Edge

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 resources. 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.

5.11.1 Configuring VTEP

➢ To enable VTEP:

**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 Overlay 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. Create loopback interface and configure an IP address for it (this is the switch VTEP IP):

```
switch (config)# interface loopback 1
switch (config interface loopback 1)# ip address 1.2.3.4 255.255.255.255
```

Step 7. 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 8. Enable NVE protocol:

```
switch (config)# protocol nve
```

Step 9. Configure interface NVE:

```
switch (config)# interface nve 1
```

Step 10. Configure the source of the NVE interface to be the loopback create above:

```
switch (config)# interface nve 1 vxlan source interface loopback 1
```

Step 11. Start OVSDB server:

```
switch (config)# ovs ovsdb server
```

Step 12. Configure the OVSDB manager to an IP address of a controller:

```
switch (config)# ovs ovsdb manager remote ssl ip address 10.130.250.5
```

Step 13. Configure switch 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
```

## 5.11.2 VMware Network Virtualization and Security Platform (NSX) Configuration

### 5.11.2.1 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
5.11.2.2 Switch Configuration

Step 1. Configure jumbo frames on ESXi and Database server facing interfaces:

```bash
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):

```bash
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 OVDB 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.

5.11.3 NSX Manager Configuration

5.11.3.1 Adding Hosts to Replication Cluster

Step 1. In NSX Manager, go to "Service Definitions" -> "Hardware Devices"

Step 2. Under "Replication Cluster" click Edit

Step 3. 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.
5.11.3.2 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.

5.11.4 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
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.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>N/A</td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Config</td>
</tr>
<tr>
<td>History</td>
<td>3.6.3004</td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
</tr>
<tr>
<td>Example</td>
<td>switch (config) # protocol nve</td>
</tr>
</tbody>
</table>

Related Commands

Note
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.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>nve-id</th>
<th>NVE ID range: 1-64</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>N/A</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Configuration Mode</th>
<th>Config</th>
</tr>
</thead>
<tbody>
<tr>
<td>History</td>
<td>3.6.3004</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Role</th>
<th>admin</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>switch (config) # interface nve 1</td>
</tr>
<tr>
<td>switch (config interface nve 1) #</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Related Commands</th>
<th>protocol nve</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Note</th>
</tr>
</thead>
<tbody>
<tr>
<td>This command is only supported on Spectrum™ based switch systems</td>
</tr>
</tbody>
</table>
### shutdown

**shutdown**

**no shutdown**

Disables VXLAN tunnel.
The no form of the command enables VXLAN tunnel.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>Enabled</td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Config Interface NVE</td>
</tr>
<tr>
<td>History</td>
<td>3.6.3004</td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
</tr>
<tr>
<td>Example</td>
<td><code>switch (config interface nve 1) # shutdown</code></td>
</tr>
</tbody>
</table>
| Related Commands    | `interface nve`  
|                     | `protocol nve` |
| Note                | This command is only supported on Spectrum™ based switch systems |
vxlans source interface loopback

vxlans source interface loopback <loopback-id>
no vxlans 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.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>loopback-id</th>
<th>Loopback interface ID</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Valid range: 0-31</td>
</tr>
<tr>
<td>Default</td>
<td>N/A</td>
<td></td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Config Interface NVE</td>
<td></td>
</tr>
<tr>
<td>History</td>
<td>3.6.3004</td>
<td></td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
<td></td>
</tr>
<tr>
<td>Example</td>
<td>switch (config interface nve 1) # vxlans source interface loopback 14</td>
<td></td>
</tr>
<tr>
<td>Related Commands</td>
<td>interface nve</td>
<td></td>
</tr>
<tr>
<td></td>
<td>protocol nve</td>
<td></td>
</tr>
<tr>
<td>Note</td>
<td>The configured loopback interface becomes the VXLAN tunnel endpoint (VTEP)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>This command is only supported on Spectrum™ based switch systems</td>
<td></td>
</tr>
</tbody>
</table>
**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.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>force</th>
<th>Forces configuration while interface is admin up</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>Not in NVE mode</td>
<td></td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Config Interface Ethernet</td>
<td></td>
</tr>
<tr>
<td>History</td>
<td>3.6.3004</td>
<td></td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
<td></td>
</tr>
<tr>
<td>Example</td>
<td>switch (config interface ethernet 1/1) # nve mode only</td>
<td></td>
</tr>
<tr>
<td>Related Commands</td>
<td>interface ethernet</td>
<td></td>
</tr>
<tr>
<td>Note</td>
<td>This command is only supported on Spectrum™ based switch systems</td>
<td></td>
</tr>
</tbody>
</table>
## clear nve counters

clear nve counters

Clears NVE counters.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>N/A</td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Config Interface NVE</td>
</tr>
<tr>
<td>History</td>
<td>3.6.3004</td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
</tr>
<tr>
<td>Example</td>
<td><code>switch (config interface nve 1) # clear nve counters</code></td>
</tr>
<tr>
<td>Related Commands</td>
<td>interface nve</td>
</tr>
<tr>
<td></td>
<td>protocol nve</td>
</tr>
<tr>
<td>Note</td>
<td>This command is only supported on Spectrum™ based switch systems</td>
</tr>
</tbody>
</table>
### show interfaces nve

**show interfaces nve [<nve-id>]**

Displays information about NVE interfaces.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>nve-id</th>
<th>NVE ID range: 1-64</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Default</strong></td>
<td>N/A</td>
<td></td>
</tr>
<tr>
<td><strong>Configuration Mode</strong></td>
<td>Any Command Mode</td>
<td></td>
</tr>
<tr>
<td><strong>History</strong></td>
<td>3.6.3004</td>
<td></td>
</tr>
<tr>
<td><strong>Role</strong></td>
<td>admin</td>
<td></td>
</tr>
</tbody>
</table>

#### Example

```
switch (config) # show interface nve
```

<table>
<thead>
<tr>
<th>Remote Manager IP Address</th>
<th>Port</th>
<th>Connection Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.2.2.2</td>
<td>200</td>
<td>tcp</td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>nve-id</th>
<th>NVE ID range: 1-64</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>N/A</td>
<td></td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Any Command Mode</td>
<td></td>
</tr>
<tr>
<td>History</td>
<td>3.6.3004</td>
<td></td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
<td></td>
</tr>
</tbody>
</table>

**Example**

```
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
```

**Related Commands**

**Note**

This command is only supported on Spectrum™ based switch systems.
**show interfaces nve flood**

```
show interfaces nve <nve-id> flood [vni <vni-id>]
```

Displays remote VTEP endpoints configured for BUM (broadcast, unknown unicast, multicast) flooding.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>nve-id</th>
<th>NVE ID range: 1-64</th>
</tr>
</thead>
<tbody>
<tr>
<td>vni</td>
<td></td>
<td>Displays NVE flooding on specific VNI</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Default</th>
<th>N/A</th>
</tr>
</thead>
</table>

**Configuration Mode**

Any Command Mode

**History**

3.6.3004

**Role**

admin

**Example**

```
switch (config) # show interface nve 1 flood
```

<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>

**Related Commands**

This command is only supported on Spectrum™ based switch systems

**Note**

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.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>nve-id</th>
<th>NVE ID range: 1-64</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>vni</td>
<td>Displays MAC address table of NVE interface with specified VNI</td>
</tr>
</tbody>
</table>

Default: N/A

Configuration Mode: Any Command Mode

History: 3.6.3004

Role: admin

Example:

```
switch (config) # show interface nve 1 mac-address-table
```

<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>167777</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>167777</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>

Related Commands

Note: 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 <vni-id>]

Displays only the locally-learned unicast MAC addresses.

**Syntax Description**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>nve-id</td>
<td>NVE ID range: 1-64</td>
</tr>
<tr>
<td>vni</td>
<td>Displays MAC addresses on the bridge with the given VNI</td>
</tr>
</tbody>
</table>

**Default**

N/A

**Configuration Mode**

Any Command Mode

**History**

3.6.3004

**Role**

admin

**Example**

```
switch (config) # show interface nve 1 mac-address-table local learned unicast

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
```

**Related Commands**

**Note**

This command is only supported on Spectrum™ based switch systems
show interfaces nve mac-address-table remote configured multicast

```plaintext
show interfaces nve <nve-id> mac-address-table remote configured multicast [vni <vni-id>]
```
Displays only remotely-configured BUM addresses.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>nve-id</th>
<th>NVE ID range: 1-64</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>vni</td>
<td>Displays only MAC addresses on the bridge with the given VNI</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Default</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuration Mode</td>
<td>Any Command Mode</td>
</tr>
<tr>
<td>History</td>
<td>3.6.3004</td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
</tr>
<tr>
<td>Example</td>
<td>switch (config) # show interface nve 1 mac-address-table remote configured multicast</td>
</tr>
</tbody>
</table>

<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>

<table>
<thead>
<tr>
<th>Related Commands</th>
</tr>
</thead>
<tbody>
<tr>
<td>Note</td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>nve-id</td>
<td>NVE ID range: 1-64</td>
</tr>
<tr>
<td>vni</td>
<td>Displays only MAC addresses on the bridge with the given VNI</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Default</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuration Mode</td>
<td>Any Command Mode</td>
</tr>
<tr>
<td>History</td>
<td>3.6.3004</td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
</tr>
</tbody>
</table>

**Example**

```
switch (config) # show interface nve 1 mac-address-table remote configured unicast

<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>
```

**Related Commands**

**Note**

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.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>nve-id</td>
<td>NVE ID range: 1-64</td>
</tr>
<tr>
<td>vni</td>
<td>Displays NVE peers on specific VNI</td>
</tr>
</tbody>
</table>

| Default | N/A |

| Configuration Mode | Any Command Mode |

| History | 3.6.3004 |

| Role | admin |

| Example | switch (config) # show interface nve 1 peers |

<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>

| Related Commands |

| Note | This command is only supported on Spectrum™ based switch systems |

| Note |

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.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>N/A</td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Config</td>
</tr>
<tr>
<td>History</td>
<td>3.6.3004</td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
</tr>
<tr>
<td>Example</td>
<td><code>switch (config) # ovs ovsdb server</code></td>
</tr>
</tbody>
</table>

**Related Commands**

**Note**

This command is only supported on Spectrum™ based switch systems
**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.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>SSL</th>
<th>Connect with TCP protocol</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>TCP</td>
<td>Connect with SSL protocol</td>
</tr>
<tr>
<td>ip-address</td>
<td></td>
<td>IP address of remote manager</td>
</tr>
</tbody>
</table>

**Default**  
N/A

**Configuration Mode**  
Config

**History**  
3.6.3004

**Role**  
admin

**Example**  
switch (config) # ovs ovsdb manager remote tcp ip-address 10.10.10.10 port 20

**Related Commands**  
`ovs ovsdb server`

**Note**  
This command is only supported on Spectrum™ based switch systems
**ovs ovsdb server listen**

```bash
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.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>SSL</th>
<th>Connect with TCP protocol</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>TCP</td>
<td>Connect with SSL protocol</td>
</tr>
<tr>
<td>ip-address</td>
<td>IP address of a given port</td>
<td></td>
</tr>
</tbody>
</table>

**Default**: N/A

**Configuration Mode**: Config

**History**: 3.6.3004

**Role**: admin

**Example**

```
switch (config) # ovs ovsdb server listen tcp port 20 local ip-address 20.20.20.20
```

**Related Commands**

`ovs ovsdb server`

**Note**

This command is only supported on Spectrum™ based switch systems.
5.12 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.

5.12.1 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
```

5.12.2 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:

```bash
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:

```bash
switch (config) # interface ethernet 1/1
switch (config interface ethernet 1/1) # switchport mode trunk
```

Step 5. Change back to config mode. Run:

```bash
switch (config interface ethernet 1/1) # exit
switch (config) #
```

Step 6. Define the MRouter port on the VLAN. Run:

```bash
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:

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

Step 3. Enable IGMP snooping globally. Run:

```bash
switch (config) # ip igmp snooping
switch (config) #
```

Step 4. Create a VLAN. Run:

```bash
switch (config) # vlan 200
switch (config vlan 200) #
```

Step 5. Change back to config mode. Run:

```bash
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:

```bash
switch (config) # interface ethernet 1/36
switch (config interface ethernet 1/36) # switchport mode hybrid
```

Step 7. Attach the VLAN to the port’s interface. Run:

```bash
switch (config interface ethernet 1/36) # switchport mode hybrid allowed-vlan 200
switch (config interface ethernet 1/36) #
```

Step 8. Change to config mode again. Run:

```bash
switch (config interface ethernet 1/36) # exit
switch (config) #
```
Step 9. Define the MRouter port on the VLAN. Run:

```
switch (config) # vlan 200
switch (config vlan 200) # ip igmp mrouter interface ethernet 1/36
switch (config vlan 200) #
```

### 5.12.3 IGMP Snooping Querier

IGMP Snooping Querier compliments the IGMP snooping functionality. IGMP Snooping Querier is used to support IGMP snooping in a VLAN where PIM and IGMP are not configured because the multicast traffic does not need to be routed. When IGMP Snooping Querier is enabled, IGMP queries are sent out periodically by the switch through all ports in the VLAN and to which hosts wishing to receive IP multicast traffic respond with IGMP report messages. IGMP Snooping Querier must be used in conjunction with IGMP snooping as IGMP snooping listens to these IGMP reports to establish appropriate forwarding.

➢ To configure IGMP Snooping Querier:

**Step 1.** Enable the IGMP snooping on the switch. Run:

```
switch (config) # ip igmp snooping
```

**Step 2.** Enable the IGMP snooping querier on a specific VLAN. Run:

```
switch (config) # 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)#
```
5.12.4 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.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>IGMP snooping is disabled, globally and per VLAN.</td>
</tr>
</tbody>
</table>
| Configuration Mode | Config  
                        Config VLAN |
| History            | 3.1.1400 |
| Role               | admin |
| Example            | switch (config) # ip igmp snooping  
                        switch (config) # vlan 10  
                        switch (config vlan 10) # ip igmp snooping |
| Related Commands   | show ip igmp snooping |
| Note               | IGMP snooping has global admin state, and per VLAN admin state. Both states need to be enabled in order to enable the IGMP snooping on a specific VLAN. |
ip igmp snooping (config)

ip igmp snooping {last-member-query-interval <1-25> | proxy reporting mrouter-timeout <60-600> | port-purge-timeout <130-1225> | report-suppression-interval <1-25>}

no ip igmp snooping {last-member-query-interval | proxy reporting | mrouter-timeout | report-suppression-interval}

Configures IGMP global parameters.
The no form of the command resets the IGMP global parameters to default.

Syntax Description

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>last-member-query-interval &lt;1-25&gt;</td>
<td>Sets the time period (in seconds) with which the general queries are sent by the IGMP quarrier. After timeout expiration the port will be removed from the multicast group.</td>
</tr>
<tr>
<td>proxy reporting</td>
<td>Enables proxy reporting</td>
</tr>
<tr>
<td>mrouter-timeout &lt;60-600&gt;</td>
<td>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.</td>
</tr>
<tr>
<td>port-purge-timeout &lt;130-1225&gt;</td>
<td>Sets the IGMP snooping port purge time interval after which the port gets deleted if no IGMP reports are received.</td>
</tr>
<tr>
<td>report-suppression-interval &lt;1-25&gt;</td>
<td>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.</td>
</tr>
</tbody>
</table>

Default

last-member-query-interval – 1 second
proxy reporting is disabled
mrouter-timeout – 125
port-purge-timeout – 260 seconds
report-suppression-interval – 5 seconds

Configuration Mode                  Config
History                              3.1.1400
Role                                 admin
Example                             switch (config) # ip igmp snooping report-suppression-interval 3
Related Commands

- ip igmp snooping (admin)
- show ip igmp snooping

Note
ip igmp snooping clear counters

ip igmp snooping clear counters [vlan <vlan-id>]

Clears IGMP snooping counters.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan</td>
<td>Clears IGMP snooping counters per VLAN</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Default</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuration Mode</td>
<td>Config</td>
</tr>
<tr>
<td>History</td>
<td>3.6.1002</td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
</tr>
<tr>
<td>Example</td>
<td>switch (config) # ip igmp snooping clear counters vlan 2</td>
</tr>
</tbody>
</table>

Note
### ip igmp snooping fast-leave

**ip igmp snooping fast-leave**  
**no ip igmp snooping fast-leave**

Enables fast leave processing on a specific interface.  
The no form of the command disables fast leave processing on a specific interface.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Default</strong></td>
<td>Normal-leave is enabled.</td>
</tr>
</tbody>
</table>
| **Configuration Mode** | Config Interface Ethernet  
Config Interface Port Channel  
Config Interface MLAG Port Channel |
| **History**        | 3.1.1400  
3.3.4500 Added MLAG port-channel configuration mode |
| **Role**           | admin |
| **Example**        | switch (config interface ethernet 1/1) # ip igmp snooping fast-leave |
| **Related Commands** | show ip igmp snooping interfaces |
| **Note**           | |
**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.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>interface &lt;type&gt; &lt;number&gt;</td>
<td>Attaches the group to a specific interface. type - ethernet or port-channel.</td>
</tr>
</tbody>
</table>

| Default | No static mrouters are configured. |
| Configuration Mode | Config VLAN |
| History | 3.1.1400 |
| Role | admin |

**Example**

```
switch (config)# vlan 1
switch (config vlan 1)# ip igmp snooping mrouter interface ethernet 1/1
```

**Related Commands**

`show ip igmp snooping mrouter`

**Note**
The multicast router port can be created only if IGMP snooping is enabled both globally and on the VLAN.
ip igmp snooping 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.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP address</td>
<td>Multicast IP address &lt;224.x.x.x - 239.255.255.255&gt;</td>
</tr>
<tr>
<td>interface</td>
<td>Attach the group to a specific interface</td>
</tr>
<tr>
<td>type</td>
<td>Ethernet or port-channel</td>
</tr>
</tbody>
</table>
| source             | Source IP address
If omitted, a multicast group is created for all sources

Default: No static groups are configured.

Configuration Mode: Config VLAN

History:
3.1.1400
3.6.2100 Added “source” parameter

Role: admin

Example:
switch (config vlan 1) # ip igmp snooping static-group 230.0.0.1 interface ethernet 1/1

Related Commands: show ip igmp snooping groups

Note: If the deleted interface is the last port, it deletes the entire multicast group.
### ip igmp snooping unregistered multicast

**Syntax**

```plaintext
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.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>options</th>
<th>• flood</th>
<th>• forward-to-mrouter-ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>flood</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Config</td>
<td></td>
<td></td>
</tr>
<tr>
<td>History</td>
<td>3.2.0500</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

#### Example

```plaintext
switch (config) # ip igmp snooping unregistered multicast flood
```

#### Related Commands

- show ip igmp snooping

#### Note
ip igmp snooping version

ip igmp snooping version {2 | 3}

Configures the default operating version to be used for newly created IGMP snooping instances.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>2</th>
<th>Enables IGMPv2</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>3</td>
<td>Enables IGMPv3</td>
</tr>
</tbody>
</table>

**Default**: 3

**Configuration Mode**: Config

**Config VLAN**

**History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.6.1002</td>
<td></td>
</tr>
<tr>
<td>3.6.2100</td>
<td>Updated default</td>
</tr>
</tbody>
</table>

**Role**: admin

**Example**

switch (config vlan 2)# ip igmp snooping version 3

**Related Commands**

**Note**
### ip igmp snooping querier

- **ip igmp snooping querier**
- **no ip igmp snooping querier**

Enables the IGMP Snooping Querier on a VLAN. The no form of the command disables the IGMP Snooping Querier on a VLAN.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>Disable</td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Config VLAN</td>
</tr>
<tr>
<td>History</td>
<td>3.3.4200</td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
</tr>
</tbody>
</table>
| Example            | `switch (config vlan 1)# ip igmp snooping querier`  
                    | `switch (config vlan 1)#` |
| Related Commands   | igmp snooping querier query-interval  
                    | show ip igmp snooping querier |

**Note**
### igmp snooping querier query-interval

**Syntax**

```
igmp snooping querier query-interval <time>
no igmp snooping querier query-interval
```

Confirms the query interval.
The no form of the command rests the parameter to its default.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>time</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>125 seconds</td>
<td>Time interval between queries (in seconds).</td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Config VLAN</td>
<td>Configuration mode.</td>
</tr>
<tr>
<td>History</td>
<td>3.3.4200</td>
<td>Historical reference.</td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
<td>Role for configuration.</td>
</tr>
</tbody>
</table>
| Example            | switch (config vlan 1)# igmp snooping querier query-interval 20  
switch (config vlan 1)# | Example usage. |
| Related Commands   | igmp snooping querier query-interval  
show ip igmp snooping querier | Related commands. |

**Note**
show ip igmp snooping

Displays IGMP snooping information for all VLANs or a specific VLAN.

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>N/A</th>
</tr>
</thead>
</table>

**Default**

N/A

**Configuration Mode**

Any Command Mode

**History**

- 3.1.1400
- 3.6.1002 Added default IGMP version to output

**Role**

admin

**Example**

```
switch (config) # show ip igmp snooping

IGMP snooping global configuration:

IGMP snooping globally enabled
IGMP default version for new VLAN is V3
IGMP snooping operationally enabled
Proxy-reporting globally disabled
Last member query interval is 1 seconds
Mrouter timeout is 125 seconds
Port purge timeout is 260 seconds
Report suppression interval is 5 seconds
IGMP snooping unregistered multicast: flood

switch (config) #
```

**Related Commands**

**Note**
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.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan</td>
<td>VLAN ID</td>
</tr>
<tr>
<td>group</td>
<td>Multicast group IP address</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Default</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuration Mode</td>
<td>Any Command Mode</td>
</tr>
<tr>
<td>History</td>
<td>3.1.1400</td>
</tr>
<tr>
<td>3.6.1002</td>
<td>Updated Example</td>
</tr>
<tr>
<td>3.6.2100</td>
<td>Added “vlan” and “group” parameters and updated Example</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Role</th>
<th>admin</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>switch (config) # show ip igmp snooping groups</td>
</tr>
<tr>
<td>Vlan ID</td>
</tr>
<tr>
<td>---------</td>
</tr>
<tr>
<td>1</td>
</tr>
<tr>
<td>1</td>
</tr>
<tr>
<td>Total Num of Dynamic Group Addresses</td>
</tr>
<tr>
<td>Total Num of Static Group Addresses</td>
</tr>
</tbody>
</table>

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

| Related Commands |

| Note |
show ip igmp snooping interfaces

Displays IGMP snooping interface information.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>N/A</td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Any Command Mode</td>
</tr>
<tr>
<td>History</td>
<td>3.1.1400</td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
</tr>
</tbody>
</table>

**Example**

```
switch (config) # show ip igmp snooping interfaces
interface      leave-mode
--------------  ----------
1/1             Normal
1/2             Normal
1/3             Normal
1/4             Fast
...
switch (config) #
```

**Related Commands**

**Note**
### show ip igmp snooping membership

#### show ip igmp snooping membership [vlan <VID> [group <group IP>]]

Displays IGMP snooping querier counters.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan</td>
<td>Displays IGMP snooping querier counters on specific VLAN</td>
</tr>
<tr>
<td>group</td>
<td>Multicast group IP address</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Default</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuration Mode</td>
<td>Any Command Mode</td>
</tr>
<tr>
<td>History</td>
<td>3.6.2100</td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
</tr>
</tbody>
</table>

#### Example

```bash
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
```

#### Related Commands

**Note**
### show ip igmp snooping mrouter

**show ip igmp snooping mrouter**

Displays IGMP snooping multicast router information.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>N/A</td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Any Command Mode</td>
</tr>
<tr>
<td>History</td>
<td>3.1.1400</td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
</tr>
</tbody>
</table>
| Example             | switch (config) # show ip igmp snooping mrouter  
Vlan       Ports           
-------    ----------       
1           Eth1/1(static) 
switch (config) # |

### Related Commands

### Note
**show ip igmp snooping querier**

`show ip igmp snooping querier [vlan <num>]`

Displays running IGMP snooping querier configuration on the VLANs.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>vlan &lt;num&gt;</code></td>
<td>Displays the IGMP snooping querier configuration running on the specified VLAN.</td>
</tr>
</tbody>
</table>

**Default**

N/A

**Configuration Mode**

Any Command Mode

**History**

3.3.4200

3.6.2100 Updated Example

**Role**

admin

**Example**

```
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
```
show ip igmp snooping querier counters

show ip igmp snooping querier counters [vlan <num> [group <group-id>]]

Displays IGMP snooping querier counters.

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan</td>
<td>Displays IGMP snooping querier counters on specific VLAN</td>
</tr>
<tr>
<td>group</td>
<td>Multicast group IP address</td>
</tr>
</tbody>
</table>

**Default**

N/A

**Configuration Mode**

Any Command Mode

**History**

3.6.1002

**Role**

admin

**Example**

```
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
```

**Related Commands**

**Note**
show ip igmp snooping statistics

show ip igmp snooping statistics

Displays IGMP snooping statistical counters.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>N/A</td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Any Command Mode</td>
</tr>
<tr>
<td>History</td>
<td>3.1.1400</td>
</tr>
<tr>
<td></td>
<td>3.6.1002</td>
</tr>
<tr>
<td></td>
<td>3.6.2100</td>
</tr>
</tbody>
</table>

| Role         | admin |

<table>
<thead>
<tr>
<th>Example</th>
</tr>
</thead>
</table>
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

<table>
<thead>
<tr>
<th>Related Commands</th>
</tr>
</thead>
</table>

| Note |
**show ip igmp snooping vlan**

`show ip igmp snooping vlan {<vlan/vlan-range> | all}`

Displays IGMP configuration per VLAN or VLAN range.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan/vlan range</td>
<td>Displays IGMP VLAN configuration per specific VLAN or VLAN range.</td>
</tr>
<tr>
<td>all</td>
<td>Display IGMP VLAN configuration on all VLAN.</td>
</tr>
</tbody>
</table>

**Default**

N/A

**Configuration Mode**

Any Command Mode

**History**

3.1.1400

**Role**

admin

**Example**

```
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) #
```

**Related Commands**

**Note**
5.13 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.

5.13.1 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
```

Step 4. Enable LLDP per interface. Run:

```
switch (config interface ethernet 1/1) # lldp receive
switch (config interface ethernet 1/1) # lldp transmit
```

Step 5. Show LLDP local information. Run:

```
switch (config) # show lldp local
```

LLDP is Enabled

Local global configuration
Chassis sub type: macAddress (4)
Chassis id: 00:11:22:33:44:55
System Name: "switch-111111"
System Description: my-system-description
Supported capabilities: B
Supported capabilities enabled: B

Step 6. Show LLDP remote information. Run:

```
switch (config)# show lldp interfaces ethernet 1/1 remote
```

Ethernet 1/1
Remote Index: 1
Remote chassis id: 00:11:22:33:44:55 ; chassis id subtype: mac
Remote port-id: ethernet 1/2; port id subtype: local
Remote port description: ethernet 1/2
Remote system name: remote-system
Remote system description: remote-system-description
Remote system capabilities supported: B ; B
5.13.2 DCBX

Data Center Bridging (DCB) is an enabler for running the Ethernet network with lossless connectivity using priority-based flow control and enhanced transmission selection. DCBX (exchange) compliments the DCB implementation by offering a dynamic protocol that communicates DCB attributes between peering endpoint.

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.

5.13.3 Commands

lldp

Enables LLDP globally.

The no form of the command disables the LLDP.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>Disabled</td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Config</td>
</tr>
<tr>
<td>History</td>
<td>3.2.0300</td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
</tr>
</tbody>
</table>
| Example            | switch (config)# lldp
                   | switch (config)# |
| Related Commands   | show lldp local |
| Note               |       |
lldp reinit

lldp reinit <seconds>
no lldp reinit

Sets the delay in seconds from enabling the LLDP on the port until re-initialization will be attempted. The no form of the command sets the parameter to default.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>seconds</th>
<th>1-10</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Config</td>
<td></td>
</tr>
<tr>
<td>History</td>
<td>3.2.0300</td>
<td></td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
<td></td>
</tr>
</tbody>
</table>

Example

```
switch (config)# lldp reinit 10
switch (config)#
```

Related Commands

show lldp timers

Note
**lldp timer**

**lldp timer <seconds>**
**no lldp timer**

Sets the LLDP interval at which LLDP frames are transmitted. (lldpMessageTxInterval)
The no form of the command sets the parameter to default.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>seconds</th>
<th>5-32768</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>30</td>
<td></td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Config</td>
<td></td>
</tr>
<tr>
<td>History</td>
<td>3.2.0300</td>
<td></td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
<td></td>
</tr>
</tbody>
</table>
| Example            | switch (config)# lldp timer 10  
switch (config)# |         |
| Related Commands   | show lldp timers |         |
| Note               |         |         |
**lldp tx-delay**

**lldp tx-delay <seconds>**

**no lldp tx-delay**

Indicates the delay in seconds between successive LLDP frame transmissions. The no form of the command sets the parameter to default.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>seconds</th>
<th>1-8192</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Config</td>
<td></td>
</tr>
<tr>
<td>History</td>
<td>3.2.0300</td>
<td></td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
<td></td>
</tr>
</tbody>
</table>
| Example            | switch (config)# lldp tx-delay 10
switch (config)# |
| Related Commands   | show lldp timers |
| Note               | The recommended value for the tx-delay is set by the following formula: 1 <= lldp tx-delay <= (0.25 * 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.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>seconds</th>
<th>1-8192</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Config</td>
<td></td>
</tr>
<tr>
<td>History</td>
<td>3.2.0300</td>
<td></td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
<td></td>
</tr>
</tbody>
</table>
| Example            | switch (config)# lldp tx-hold-multiplier 10  
switch (config)# |
| Related Commands   | show lldp timers |
| Note               | The actual time-to-live value used in LLDP frames, can be expressed by the following formula: TTL = min(65535, (lldpMessageTxInterval * lldpMessageTxHoldMultiplier)) For example, if the value of lldpMessageTxInterval is '30', and the value of lldpMessageTxHoldMultiplier is '4', then the value '120' is encoded in the TTL field in the LLDP header. |
lldp (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.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>med-tlv-select</th>
<th>Enables LLDP media TLVs</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>receive</td>
<td>Enables LLDP receive on this port</td>
</tr>
<tr>
<td></td>
<td>tlv-select</td>
<td>Enables LLDP TLVs</td>
</tr>
<tr>
<td></td>
<td>transmit</td>
<td>Enables LLDP transmit on this port</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Default</th>
<th>Enabled for receive and transmit.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuration Mode</td>
<td>Config Interface Ethernet</td>
</tr>
<tr>
<td>History</td>
<td>3.2.0300</td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
</tr>
<tr>
<td>Example</td>
<td>switch (config interface ethernet 1/1)# lldp receive \n</td>
</tr>
<tr>
<td>Related Commands</td>
<td>show lldp interface</td>
</tr>
<tr>
<td>Note</td>
<td>The LLDP is disabled by default (globally)</td>
</tr>
</tbody>
</table>
**Ildp tlv-select**

Ildp tlv-select {[dcbx] [dcbx-cee] [port-description] [sys-name] [sys-description] [sys-capabilities] [management-address] [none] all}

Sets the LLDP basic TLVs to be transmitted on this port.

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>dcbx</td>
<td>Enables LLDP-DCBX TLVs.</td>
</tr>
<tr>
<td>dcbx-cee</td>
<td>Enables LLDP-DCBX CEE TLVs.</td>
</tr>
<tr>
<td>port-description</td>
<td>LLDP port description TLV.</td>
</tr>
<tr>
<td>sys-name</td>
<td>LLDP system name TLV.</td>
</tr>
<tr>
<td>sys-description</td>
<td>LLDP system description TLV.</td>
</tr>
<tr>
<td>sys-capabilities</td>
<td>LLDP system capabilities TLV.</td>
</tr>
<tr>
<td>management-address</td>
<td>LLDP management address TLV.</td>
</tr>
<tr>
<td>all</td>
<td>all above TLVs.</td>
</tr>
<tr>
<td>none</td>
<td>None of the above TLVs.</td>
</tr>
</tbody>
</table>

**Default**

all

**Configuration Mode**

Config Interface Ethernet

**History**

3.2.0300 Initial revision

3.3.0000 Added “none” parameter

3.3.4302 Added “dcbx” parameter

3.3.4402 Added “dcbx-cee” parameter

**Role**

admin

**Example**

switch (config interface ethernet 1/1)# lldp tlv-select port-description sys-name
switch (config interface ethernet 1/1)#

**Related Commands**

show lldp interface

**Note**
lldp med-tlv-select

**Syntax**

```plaintext
lldp med-tlv-select {all | media-capability | network-policy | none}
```

**Description**

Configures LLDP media TLV attributes.

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>all</td>
<td>Enables all LLDP media TLVs</td>
</tr>
<tr>
<td>media-capabilities</td>
<td>Enables Media Capabilities TLV</td>
</tr>
<tr>
<td>network-policy</td>
<td>Enables Network-Policy TLV</td>
</tr>
<tr>
<td>none</td>
<td>Disables all LLDP media TLVs</td>
</tr>
</tbody>
</table>

**Default**

Disabled

**Configuration Mode**

Config Interface Ethernet

**History**

3.6.1002

**Role**

admin

**Example**

```plaintext
switch (config interface ethernet 1/1)# lldp med-tlv-select all
switch (config interface ethernet 1/1)#
```

**Related Commands**

show lldp interface

**Note**

show lldp interface
### dcb application-priority

**dcb application-priority <selector> <protocol> <priority>**

Adds an application to the application priority table.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>selector</td>
<td>Protocol type: ethertype</td>
</tr>
<tr>
<td>protocol</td>
<td>Protocol field in hexadecimal notation (e.g. ‘0x8906’ for FCoE, ‘0x8914’ for FIP).</td>
</tr>
<tr>
<td>priority</td>
<td>Range: 0-7.</td>
</tr>
</tbody>
</table>

**Default**
No applications are available. The table is empty.

**Configuration Mode**
Config

**History**
3.3.4200
3.4.0008

**Role**
admin

**Example**
```
switch (config-if)# dcb application-priority ethertype 0x8906
switch (config-if)#
```

**Related Commands**
show lldp interface

**Note**
## show lldp local

The `show lldp local` command displays LLDP local information.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>N/A</td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Any Command Mode</td>
</tr>
<tr>
<td>History</td>
<td>3.2.0300</td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
</tr>
</tbody>
</table>
| Example             | switch (config)# show lldp local  

```plaintext
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
```

## Related Commands

Switch to a different command. For example:

```
switch (config)#
```

## Note

---
show lldp interfaces

show lldp interfaces [ethernet <inf> [med-cap | remote]]

Displays LLDP remote interface table information.

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>inf</td>
<td>Local interface number (e.g. 1/1)</td>
</tr>
<tr>
<td>med-cap</td>
<td>Displays local port media capabilities information</td>
</tr>
<tr>
<td>remote</td>
<td>Displays LLDP Ethernet remote configuration &amp; status</td>
</tr>
</tbody>
</table>

**Default**

N/A

**Configuration Mode**

Any Command Mode

**History**

- 3.2.0300 - First version
- 3.3.4200 - Updated Example
- 3.6.1002 - Updated Example

**Role**

admin

**Example**

```
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, FFC, AP, ETS-C, ETS-R
Eth1/3   Disabled  Disabled  PD, SN, SD, SC, MA, FFC, AP, ETS-C, ETS-R, MED-NWP
Eth1/4   Enabled   Enabled   PD, SN, SD, SC, MA, FFC, AP, ETS-C, ETS-R, MED-CAP, MED-NWP
Eth1/5   Enabled   Enabled   PD, SN, SD, SC, MA, FFC, AP, ETS-C, ETS-R
Eth1/6   Enabled   Enabled   PD, SN, SD, SC, MA, FFC, AP, ETS-C, ETS-R
Eth1/7   Enabled   Enabled   PD, SN, SD, SC, MA, FFC, AP, ETS-C, ETS-R
```

**Related Commands**

**Note**
show lldp remote

Displays LLDP remote information (remote device id, remote port id, remote system name).

Syntax Description
N/A

Default
N/A

Configuration Mode
Any Command Mode

History
3.6.3004

Role
admin

Example

```
switch (config)# show lldp remote

------------------------------------------------------------------------------
Local Interface      Device ID            Port ID              System Name
------------------------------------------------------------------------------
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
```

Related Commands

Note
**show lldp statistics [interface ethernet <inf>]**

Displays LLDP interface statistics.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>N/A</td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Any Command Mode</td>
</tr>
<tr>
<td>History</td>
<td>3.2.0300</td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
</tr>
</tbody>
</table>

**Example**

```
switch (config)# show lldp statistics interface ethernet 1/1
Interface Frames  In  In TLVs TLVs Ageout Out
-----------------------------  -----------------------------
Discarded Errors Total Discarded Unrecognized Frames
Eth 1/1 0 0 10 0 0 0 0
```

**Related Commands**

**Note**
show lldp statistics global

show lldp statistics global

Displays LLDP global statistics.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>N/A</td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Any Command Mode</td>
</tr>
<tr>
<td>History</td>
<td>3.2.0300</td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
</tr>
</tbody>
</table>

**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

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>N/A</td>
</tr>
<tr>
<td><strong>Configuration Mode</strong></td>
<td>Any Command Mode</td>
</tr>
<tr>
<td>History</td>
<td>3.2.0300</td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
</tr>
</tbody>
</table>

**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**

**Syntax Description**
N/A

**Default**
N/A

**Configuration Mode**
Any Command Mode

**History**
3.3.4200

**Role**
admin

**Example**

```
switch (config)# show dcb application-priority
Application priority configuration
Selector  Protocol  Priority
-----------------------------
Ethertype  0x8906   3
Ethertype  0x8914   3
```

**Related Commands**

**Note**
5.14 Quality of Service (QoS)

5.14.1 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.

5.14.1.1 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 53 and figure summarize the classification rules.

Table 53 - Packet Classification Rules

<table>
<thead>
<tr>
<th>Packet Type</th>
<th>IP/MPLS</th>
<th>VLAN</th>
<th>QoS Classification Config (per Interface)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td>Trust Both</td>
</tr>
<tr>
<td>IP/MPLS</td>
<td>Tagged</td>
<td>DSCP</td>
<td>DSCP</td>
</tr>
<tr>
<td>IP/MPLS</td>
<td>Untagged</td>
<td>DSCP</td>
<td>DSCP</td>
</tr>
<tr>
<td>non-IP/MPLS</td>
<td>Tagged</td>
<td>PCP,DEI</td>
<td>Port Default</td>
</tr>
<tr>
<td>non-IP/MPLS</td>
<td>Untagged</td>
<td>Port Default</td>
<td>Port Default</td>
</tr>
</tbody>
</table>

Default switch-priority is configured as trust L2.
5.14.1.2 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.

5.14.1.3 Default QoS Configuration

*Table 54 - Default QoS Configuration*

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Range</th>
<th>Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>Trust level</td>
<td>All ports</td>
<td>Trust L2</td>
</tr>
<tr>
<td>DSCP to switch-priority</td>
<td>0-7</td>
<td>0</td>
</tr>
<tr>
<td>DSCP to switch-priority</td>
<td>8-15</td>
<td>1</td>
</tr>
<tr>
<td>DSCP to switch-priority</td>
<td>16-23</td>
<td>2</td>
</tr>
<tr>
<td>DSCP to switch-priority</td>
<td>24-31</td>
<td>3</td>
</tr>
<tr>
<td>DSCP to switch-priority</td>
<td>32-39</td>
<td>4</td>
</tr>
<tr>
<td>DSCP to switch-priority</td>
<td>40-47</td>
<td>5</td>
</tr>
<tr>
<td>DSCP to switch-priority</td>
<td>48-55</td>
<td>6</td>
</tr>
<tr>
<td>DSCP to switch-priority</td>
<td>56-63</td>
<td>7</td>
</tr>
<tr>
<td>PCP to switch-priority</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>PCP to switch-priority</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>PCP to switch-priority</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>PCP to switch-priority</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>PCP to switch-priority</td>
<td>4</td>
<td>4</td>
</tr>
<tr>
<td>PCP to switch-priority</td>
<td>5</td>
<td>5</td>
</tr>
<tr>
<td>PCP to switch-priority</td>
<td>6</td>
<td>6</td>
</tr>
<tr>
<td>PCP to switch-priority</td>
<td>7</td>
<td>7</td>
</tr>
<tr>
<td>Port PCP,DEI default</td>
<td>All ports</td>
<td>0</td>
</tr>
<tr>
<td>Port switch-priority when “trust port” is enabled</td>
<td>All ports</td>
<td>0</td>
</tr>
<tr>
<td>Switch-priority to IEEE priority</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Switch-priority to IEEE priority</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Switch-priority to IEEE priority</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>Switch-priority to IEEE priority</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>Switch-priority to IEEE priority</td>
<td>4</td>
<td>4</td>
</tr>
<tr>
<td>Switch-priority to IEEE priority</td>
<td>5</td>
<td>5</td>
</tr>
<tr>
<td>Switch-priority to IEEE priority</td>
<td>6</td>
<td>6</td>
</tr>
</tbody>
</table>
5.14.2 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.

5.14.2.1 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.

5.14.2.2 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.

5.14.2.3 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.

5.14.2.4 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

---

**Table 54 - Default QoS Configuration**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Range</th>
<th>Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>Switch-priority to IEEE priority</td>
<td>7</td>
<td>7</td>
</tr>
</tbody>
</table>
5.14.3 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

ETS is enabled by default (scheduling is WRR).

➢ **To set the scheduling mode to Strict Priority:**

  **Step 1.** Run the command `dcb ets disable`.

  ```
  switch (config) # no dcb ets enable
  ```

➢ **To configure the WRR bandwidth percentage:**

  **Step 1.** Make sure ETS feature is enabled. Run:

  ```
  switch (config) # dcb ets enable
  ```

  **Step 2.** Choose the WRR bandwidth rate and distribution.

  By default the WRR distribution function is equal 25% per TC. Changing the WRR bandwidth rate will cause a change in the distribution function, for example if you wish to

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.
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

<table>
<thead>
<tr>
<th>TC</th>
<th>Bandwidth</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>30%</td>
</tr>
<tr>
<td>1</td>
<td>30%</td>
</tr>
<tr>
<td>2</td>
<td>30%</td>
</tr>
<tr>
<td>3</td>
<td>10%</td>
</tr>
</tbody>
</table>

Number of Traffic Class: 4
```

Step 3. Run the command `show dcb ets` to verify the configuration.

```
switch (config) # show dcb ets
ETS enabled

<table>
<thead>
<tr>
<th>TC</th>
<th>Bandwidth</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>30%</td>
</tr>
<tr>
<td>1</td>
<td>30%</td>
</tr>
<tr>
<td>2</td>
<td>10%</td>
</tr>
<tr>
<td>3</td>
<td>30%</td>
</tr>
</tbody>
</table>

Number of Traffic Class: 4
```

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.

5.14.4 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.
5.14.4.1 Traffic Class

The switch-priority of the packet assigns it to a specific traffic class (TC). The TC of the packet determines the packet path in the queuing structure. There are 8 TCs supported by the system.

5.14.4.2 Multicast Aware Traffic Class Mapping

Spectrum™ supports a mode of MC aware TC mapping if the mapping to the TCs is based also on the whether the packet is unicast or multicast. So, packets of the same switch-priority can be mapped to two different TCs, based on their traffic type. With MC aware mode enabled, MC traffic is mapped into 8 MC TCs in parallel to 8 unicast TCs. Unicast TC has strict priority over its parallel multicast TC.

5.14.4.3 Traffic Shapers

Maximum Shapers

TCs can be configured for rate shaping as described in the following:
- TC Class queues: shaper per TC Class queue
- Port: shaper per port (bytes only)

Shapers support the following configurations:
- Committed Incoming Rate (CIR) [bits/packets per second]
- Committed Burst Size (CBS) [bites/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.

5.14.4.4 Default Shaper Configuration

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Range</th>
<th>Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>Switch-priority to TC</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Switch-priority to TC</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Switch-priority to TC</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>Switch-priority to TC</td>
<td>3</td>
<td>3</td>
</tr>
</tbody>
</table>
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 23:

- Minimum – a threshold that defines the average queue length below which the packets are not dropped/marketed
- Maximum – a threshold that defines the average queue length above which the packets are always dropped/marketed

### 5.14.5 RED and ECN

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Range</th>
<th>Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>Switch-priority to TC 4</td>
<td>4</td>
<td>4</td>
</tr>
<tr>
<td>Switch-priority to TC 5</td>
<td>5</td>
<td>5</td>
</tr>
<tr>
<td>Switch-priority to TC 6</td>
<td>6</td>
<td>6</td>
</tr>
<tr>
<td>Switch-priority to TC 7</td>
<td>7</td>
<td>7</td>
</tr>
<tr>
<td>MC-aware TC mapping</td>
<td>All ports</td>
<td>True</td>
</tr>
<tr>
<td>Shaping</td>
<td>All ports</td>
<td>No max/min shaping configured</td>
</tr>
</tbody>
</table>
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.

5.14.6 Commands

5.14.6.1 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.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
<th>Range: 0-7</th>
</tr>
</thead>
<tbody>
<tr>
<td>priority</td>
<td>Range: 0-7</td>
<td></td>
</tr>
</tbody>
</table>

**Default**

0

**Configuration Mode**

Config Interface Ethernet
Config Interface Port Channel
Config Interface MLAG Port Channel

**History**

3.6.1002

**Role**

admin

**Example**

```
switch (config interface ethernet 1/1) # vlan default priority 0
```

**Related Commands**

N/A

**Notes**

This command is only supported on Spectrum™ based switch systems.
### vlan default dei

**Syntax**

```
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.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Default</strong></td>
<td>0</td>
</tr>
<tr>
<td><strong>Configuration Mode</strong></td>
<td>Config Interface Ethernet</td>
</tr>
<tr>
<td><strong>History</strong></td>
<td>3.6.1002</td>
</tr>
<tr>
<td><strong>Role</strong></td>
<td>admin</td>
</tr>
<tr>
<td><strong>Example</strong></td>
<td><code>switch (config interface ethernet 1/1) # vlan default dei 0</code></td>
</tr>
<tr>
<td><strong>Related Commands</strong></td>
<td>N/A</td>
</tr>
<tr>
<td><strong>Notes</strong></td>
<td>This command is only supported on Spectrum™ based switch systems</td>
</tr>
</tbody>
</table>
### qos trust

```plaintext
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.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>L2</td>
</tr>
</tbody>
</table>
| Configuration Mode | Config Interface Ethernet  
                         Config Interface Port Channel 
                         Config Interface MLAG Port Channel |
| History            | 3.6.1002 |
| Role               | admin |
| Example            | switch (config interface ethernet 1/1) # qos trust L2 |
| Related Commands   | N/A |
| Notes              | 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.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>switch-priority</th>
<th>Range: 0-7</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>0</td>
<td></td>
</tr>
</tbody>
</table>
| Configuration Mode  | Config Interface Ethernet  
                    | Config Interface Port Channel  
                    | Config Interface MLAG Port Channel |
| History             | 3.6.1002        |            |
| Role                | admin           |            |
| Example             | `switch (config interface ethernet 1/1) # qos default switch-priority 0` |
| Related Commands    | qos trust       |            |
| Notes               | 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.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>PCP to switch-priority mapping: 0 → 0</td>
</tr>
<tr>
<td></td>
<td>1 → 1</td>
</tr>
<tr>
<td></td>
<td>2 → 2</td>
</tr>
<tr>
<td></td>
<td>3 → 3</td>
</tr>
<tr>
<td></td>
<td>4 → 4</td>
</tr>
<tr>
<td></td>
<td>5 → 5</td>
</tr>
<tr>
<td></td>
<td>6 → 6</td>
</tr>
<tr>
<td></td>
<td>7 → 7</td>
</tr>
</tbody>
</table>

**Configuration Mode**
- Config Interface Ethernet
- Config Interface Port Channel
- Config Interface MLAG Port Channel

**History**
3.6.1002

**Role**
admin

**Example**
switch (config interface ethernet 1/1) # qos map pcp 5 dei 5

**Related Commands**
qos trust

**Notes**
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.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>switch-priority</th>
<th>Range: 0-7</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>dscp</td>
<td>Range: 0-63</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Default</th>
<th>DSCP to switch-priority mapping:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>0-7 → 0</td>
</tr>
<tr>
<td></td>
<td>8-15 → 1</td>
</tr>
<tr>
<td></td>
<td>16-23 → 2</td>
</tr>
<tr>
<td></td>
<td>24-31 → 3</td>
</tr>
<tr>
<td></td>
<td>32-39 → 4</td>
</tr>
<tr>
<td></td>
<td>40-47 → 5</td>
</tr>
<tr>
<td></td>
<td>48-55 → 6</td>
</tr>
<tr>
<td></td>
<td>56-63 → 7</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Configuration Mode</th>
<th>Config Interface Ethernet</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Config Interface Port Channel</td>
</tr>
<tr>
<td></td>
<td>Config Interface MLAG Port Channel</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>History</th>
<th>3.6.1002</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Role</th>
<th>admin</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Example</th>
<th>switch (config interface ethernet 1/1) # qos map dscp 45</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Related Commands</th>
<th>qos trust</th>
</tr>
</thead>
</table>

| Notes | This command is only supported on Spectrum™ based switch systems |
show qos

Syntax Description
N/A

Default
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

Configuration Mode
Any Command Mode

History
3.6.1002

Role
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.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>slot/port</td>
<td>Number of Ethernet interface in form of slot/port</td>
</tr>
<tr>
<td>priority</td>
<td>Valid priority values: 0-7 or all</td>
</tr>
</tbody>
</table>

| Default            | N/A                                             |
| Configuration Mode | Any Command Mode                                |
| History            | 3.6.3004                                        |
| Role               | admin                                           |

Example

switch (config) # show interfaces ethernet 1/1 counters tc 3

TC 3
0 packets
0 bytes
0 queue depth
0 unicast no buffer discard
0 WRED discard

Related Commands

Note
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.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>slot/port</th>
<th>Number of Ethernet interface in form of slot/port</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>priority</td>
<td>Valid priority values: 0-7 or all</td>
</tr>
</tbody>
</table>

| Default | N/A          |

<table>
<thead>
<tr>
<th>Configuration Mode</th>
<th>Any Command Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>History</td>
<td>3.6.3004</td>
</tr>
</tbody>
</table>

| Role | admin |

<table>
<thead>
<tr>
<th>Example</th>
<th>switch (config) # show interfaces ethernet 1/1 counters pg 4</th>
</tr>
</thead>
<tbody>
<tr>
<td>PG 4</td>
<td>packets bytes queue depth no buffer discard shared buffer discard</td>
</tr>
</tbody>
</table>

| Related Commands |

| Note | 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.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>slot/port</td>
<td>Number of Ethernet interface in form of slot/port</td>
</tr>
<tr>
<td>priority</td>
<td>Valid priority values: 0-7 or all</td>
</tr>
</tbody>
</table>

| Default | N/A |

| Configuration Mode | Any Command Mode |

| History | 3.6.3004 |

| Role | admin |

<table>
<thead>
<tr>
<th>Example</th>
<th>Switch (config) # show interfaces ethernet 1/1 counters pfc prio 1</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>PFC 1</td>
</tr>
<tr>
<td></td>
<td>Rx</td>
</tr>
<tr>
<td></td>
<td>0 pause packets</td>
</tr>
<tr>
<td></td>
<td>0 pause duration</td>
</tr>
<tr>
<td></td>
<td>Tx</td>
</tr>
<tr>
<td></td>
<td>0 pause packets</td>
</tr>
<tr>
<td></td>
<td>0 pause duration</td>
</tr>
</tbody>
</table>

| Related Commands |

| Note | This command is only supported on Spectrum™ based switch systems |
### 5.14.6.2 QoS Rewrite

**qos rewrite pcp**

- **qos rewrite pcp-enable**
- **qos rewrite pcp-disable**

Enables or disables PCP,DEI rewrite on the interface.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>Disabled</td>
</tr>
</tbody>
</table>
| **Configuration Mode** | Config Interface Ethernet  
                       | Config Interface Port Channel  
                       | Config Interface MLAG Port Channel |
| History            | 3.6.1002 |
| Role               | admin |
| **Example**        | `switch (config interface ethernet 1/1) # qos rewrite pcp-enable` |
| **Related Commands** | |
| Notes              | 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.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>Disabled</td>
</tr>
</tbody>
</table>
| Configuration Mode | Config Interface Ethernet  
|                    | Config Interface Port Channel  
|                    | Config Interface MLAG Port Channel  |
| History            | 3.6.1002          |
| Role               | admin             |
| Example            | switch (config interface ethernet 1/1) # qos rewrite dscp-enable |

**Related Commands**

**Notes**

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.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>switch-priority</th>
<th>Range: 0-7</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>pcp</td>
<td>Range: 0-7</td>
</tr>
<tr>
<td></td>
<td>dei</td>
<td>Value: 0</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Default</th>
<th>Switch priority to PCP,DEI mapping:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>0 → 0,0</td>
</tr>
<tr>
<td></td>
<td>1 → 1,0</td>
</tr>
<tr>
<td></td>
<td>2 → 2,0</td>
</tr>
<tr>
<td></td>
<td>3 → 3,0</td>
</tr>
<tr>
<td></td>
<td>4 → 4,0</td>
</tr>
<tr>
<td></td>
<td>5 → 5,0</td>
</tr>
<tr>
<td></td>
<td>6 → 6,0</td>
</tr>
<tr>
<td></td>
<td>7 → 7,0</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Configuration Mode</th>
<th>Config Interface Ethernet</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Config Interface Port Channel</td>
</tr>
<tr>
<td></td>
<td>Config Interface MLAG Port Channel</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>History</th>
<th>3.6.1002</th>
</tr>
</thead>
<tbody>
<tr>
<td>Role</td>
<td>admin</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Example</th>
<th>switch (config interface ethernet 1/1) # qos rewrite map switch-priority 11 pcp 7 dei 0</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Related Commands</th>
<th>N/A</th>
</tr>
</thead>
</table>

| Notes | This command is only supported on Spectrum™ based switch systems |
### qos rewrite map switch-priority dscp

**Syntax**
```
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.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>N/A</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Default</th>
<th>Switch priority to DSCP mapping:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>0 → 0</td>
</tr>
<tr>
<td></td>
<td>1 → 8</td>
</tr>
<tr>
<td></td>
<td>2 → 16</td>
</tr>
<tr>
<td></td>
<td>3 → 24</td>
</tr>
<tr>
<td></td>
<td>4 → 32</td>
</tr>
<tr>
<td></td>
<td>5 → 40</td>
</tr>
<tr>
<td></td>
<td>6 → 48</td>
</tr>
<tr>
<td></td>
<td>7 → 54</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Configuration Mode</th>
<th>Config Interface Ethernet</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Config Interface Port Channel</td>
</tr>
<tr>
<td></td>
<td>Config Interface MLAG Port Channel</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>History</th>
<th>3.6.1002</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Role</th>
<th>admin</th>
</tr>
</thead>
</table>

**Example**
```
switch (config interface ethernet 1/1) # qos rewrite map switch-priority 5 dscp 40
```

<table>
<thead>
<tr>
<th>Related Commands</th>
<th>N/A</th>
</tr>
</thead>
</table>

**Notes**
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.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>disable</th>
<th>No rewrite occurs</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>enable</td>
<td>PCP,DEI are rewritten based on the mapping configured on the egress port</td>
</tr>
<tr>
<td></td>
<td>preserve</td>
<td>Ingress interface configuration determines action</td>
</tr>
</tbody>
</table>

**Default**

- Default is “preserve” when router is disabled
- Default is “enable” when router is enabled
  (Router can be enabled/disabled using the “ip routing” command)

**Configuration Mode** Config

**History** 3.6.1002

**Role** admin

**Example**
```
switch (config) # qos ip rewrite pcp enable
```

**Related Commands** N/A

**Notes** The parameter “preserve” is only supported on Spectrum based switch systems
5.14.6.3 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.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>ETS is enabled</td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Config</td>
</tr>
<tr>
<td>History</td>
<td>3.1.0000</td>
</tr>
<tr>
<td></td>
<td>3.6.1002 Updated Note</td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
</tr>
</tbody>
</table>
| Example             | switch (config)# dcb ets enable
switch (config)# show dcb ets
ETS enabled
TC    Bandwidth
--------
0      25%
1      25%
2      25%
3      25%
Number of Traffic Class: 4
switch (config) # |

**Related Commands**

show dcb ets

**Note**
The show command output is from a SwitchX® based switch systems.
**dcb ets tc bandwidth**

```plaintext
dcb ets tc bandwidth <tc-0> <te-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.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>tc-i</th>
<th>0-100.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td></td>
<td>25% per traffic class</td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Config</td>
<td></td>
</tr>
<tr>
<td>History</td>
<td>3.1.0000</td>
<td></td>
</tr>
<tr>
<td></td>
<td>3.6.1002 Updated Note</td>
<td></td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
<td></td>
</tr>
</tbody>
</table>

**Example**

```
switch (config)# dcb ets tc bandwidth 20 20 30 30
switch (config) # show dcb ets

ETS enabled

<table>
<thead>
<tr>
<th>TC</th>
<th>Bandwidth</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>20%</td>
</tr>
<tr>
<td>1</td>
<td>20%</td>
</tr>
<tr>
<td>2</td>
<td>30%</td>
</tr>
<tr>
<td>3</td>
<td>30%</td>
</tr>
</tbody>
</table>

Number of Traffic Class: 4
```

**Related Commands**

- show dcb ets

**Note**

- The sum of all traffic class bandwidth must be equal to 100
- This command is only supported on SwitchX® based switch systems
### 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.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>N/A</th>
</tr>
</thead>
</table>

| Default              | Priority 0,1 mapped to tc 0  
Priority 2,3 mapped to tc 1  
Priority 4,5 mapped to tc 2  
Priority 6,7 mapped to tc 3 |
|----------------------|-----|

<table>
<thead>
<tr>
<th>Configuration Mode</th>
<th>Config Interface Ethernet</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>History</th>
<th>3.1.0000</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>3.6.1002 Updated Note</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Role</th>
<th>admin</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Example</th>
<th><code>switch (config interface ethernet 1/1) # vlan map-priority 1 traffic-class 2</code></th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Related Commands</th>
<th>show dcb ets interface</th>
</tr>
</thead>
</table>

| Note                 | This command is only supported on SwitchX® based switch systems       |
### show dcb ets (SwitchX)

**show dcb ets**

Displays ETS configuration and operational data.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>ETS is enabled.</td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Any Command Mode</td>
</tr>
<tr>
<td>History</td>
<td>3.1.0000</td>
</tr>
<tr>
<td></td>
<td>3.6.1002 Updated Note</td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
</tr>
</tbody>
</table>

**Example**

```
switch (config)# show dcb ets

ETS enabled

<table>
<thead>
<tr>
<th>TC</th>
<th>Bandwidth</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>25%</td>
</tr>
<tr>
<td>1</td>
<td>25%</td>
</tr>
<tr>
<td>2</td>
<td>25%</td>
</tr>
<tr>
<td>3</td>
<td>25%</td>
</tr>
</tbody>
</table>

Number of Traffic Class: 4
```

### Related Commands

**Note**

The show command output is from a SwitchX® based switch system.
show dcb ets interface

show dcb ets interface <type> <number>

Displays ETS configuration and operational data, per interface.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>type</td>
<td>ethernet or port-channel</td>
</tr>
<tr>
<td>number</td>
<td>interface number, i.e. 1/1</td>
</tr>
</tbody>
</table>

| Default             | ETS is enabled.                    |
| Configuration Mode  | Any Command Mode                   |
| History             | 3.1.0000                           |
| Role                | admin                              |
### Example

```bash
switch (config)# show dcb ets interface ethernet 1/1
```

<table>
<thead>
<tr>
<th>ETS Port Mode</th>
<th>ON MODE</th>
</tr>
</thead>
<tbody>
<tr>
<td>ETS Oper State</td>
<td>INIT STATE</td>
</tr>
<tr>
<td>ETS State Machine Type</td>
<td>Assymetric</td>
</tr>
</tbody>
</table>

ETS Local Port Info

**TC bandwidth table**

<table>
<thead>
<tr>
<th>TC</th>
<th>Bandwidth</th>
<th>RecomBandwidth</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>25%</td>
<td>25%</td>
</tr>
<tr>
<td>1</td>
<td>25%</td>
<td>25%</td>
</tr>
<tr>
<td>2</td>
<td>25%</td>
<td>25%</td>
</tr>
<tr>
<td>3</td>
<td>25%</td>
<td>25%</td>
</tr>
</tbody>
</table>

**priority assignment table**

<table>
<thead>
<tr>
<th>Priority</th>
<th>TC</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>3</td>
<td>1</td>
</tr>
<tr>
<td>4</td>
<td>2</td>
</tr>
<tr>
<td>5</td>
<td>2</td>
</tr>
<tr>
<td>6</td>
<td>3</td>
</tr>
<tr>
<td>7</td>
<td>3</td>
</tr>
</tbody>
</table>

Number of Traffic Class: 4

Willing Status: Disable

ETS Admin Port Info

**TC bandwidth table**

<table>
<thead>
<tr>
<th>TC</th>
<th>Bandwidth</th>
<th>RecomBandwidth</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>30%</td>
<td>30%</td>
</tr>
<tr>
<td>1</td>
<td>30%</td>
<td>30%</td>
</tr>
<tr>
<td>2</td>
<td>30%</td>
<td>30%</td>
</tr>
<tr>
<td>3</td>
<td>10%</td>
<td>10%</td>
</tr>
</tbody>
</table>

ETS Remote Port Info

No Remote Entry is Present

### Related Commands

### Note
**bind switch-priority**

```bash
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

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>Switch priority to traffic class mapping: 0 → 0 1 → 1 2 → 2 3 → 3 4 → 4 5 → 5 6 → 6 7 → 7</td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>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</td>
</tr>
<tr>
<td>History</td>
<td>3.6.1002</td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
</tr>
<tr>
<td>Example</td>
<td>switch (config interface ethernet 1/1 traffic-class 0) # bind switch-property 1</td>
</tr>
<tr>
<td>Related Commands</td>
<td>N/A</td>
</tr>
</tbody>
</table>
| Notes              | • Context is egress interface traffic class
• This command is only supported on Spectrum™ based switch systems |
## bandwidth guaranteed

**Syntax**

`bandwidth guaranteed [<rate>]`

`no bandwidth guaranteed [<rate>]`

Configures the minimum bandwidth for outbound traffic.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Rate in GbE</th>
</tr>
</thead>
<tbody>
<tr>
<td>rate</td>
<td></td>
</tr>
<tr>
<td>Range: 0 - max speed supported</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Default</th>
<th>0</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Configuration Mode</th>
<th>Config Interface Ethernet Traffic Class</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Config Interface Port Channel Traffic Class</td>
</tr>
<tr>
<td></td>
<td>Config Interface MLAG Port Channel Traffic Class</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>History</th>
<th>3.6.1002</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Role</th>
<th>admin</th>
</tr>
</thead>
</table>

**Example**

```
switch (config interface ethernet 1/1 traffic-class 0) # bandwidth
    guaranteed 0.4G
```

**Related Commands**

N/A

**Notes**

- Context is egress interface traffic class
- Bandwidth guaranteed rate determines the bandwidth guaranteed by the switch for outbound traffic assigned to this traffic class on this interface
- Bandwidth is in granularity of 0.2G
- This command is only supported on Spectrum™ based switch systems
**bandwidth shape**

```
bandwidth shape [<rate>]
no bandwidth shape [<rate>]
```

Configures the bandwidth shaper for outbound traffic.

| Syntax Description | rate | Rate in GbE
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Range: 0 - max speed supported</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Default</th>
<th>Maximum port rate (100GbE on Spectrum™ based switches)</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Configuration Mode</th>
<th>Config Interface Ethernet Traffic Class</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Config Interface Port Channel Traffic Class</td>
</tr>
<tr>
<td></td>
<td>Config Interface MLAG Port Channel Traffic Class</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>History</th>
<th>3.6.1002</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Role</th>
<th>admin</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Example</th>
<th>switch (config interface ethernet 1/1 traffic-class 7) # bandwidth shape 0.4G</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Related Commands</th>
<th>N/A</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Context is egress interface traffic class and/or port</td>
</tr>
<tr>
<td>• Bandwidth shape rate determines the bandwidth of the shaper for outbound traffic assigned to this traffic class on this interface</td>
</tr>
<tr>
<td>• Bandwidth is in granularity of 0.2G</td>
</tr>
<tr>
<td>• This command is only supported on Spectrum™ based switch systems</td>
</tr>
</tbody>
</table>

**dcb ets**

```
dcb ets [strict | wrr <weight>]
no dcb ets [strict | wrr <weight>]
```

Configures ETS mode to strict or WRR.

**Syntax Description**

- `weight`

**Default**

Default is WRR with the following default weights.

Traffic class to weight mapping:

<table>
<thead>
<tr>
<th>Traffic class</th>
<th>Weight</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>12</td>
</tr>
<tr>
<td>1</td>
<td>13</td>
</tr>
<tr>
<td>2</td>
<td>12</td>
</tr>
<tr>
<td>3</td>
<td>13</td>
</tr>
<tr>
<td>4</td>
<td>12</td>
</tr>
<tr>
<td>5</td>
<td>13</td>
</tr>
<tr>
<td>6</td>
<td>12</td>
</tr>
<tr>
<td>7</td>
<td>13</td>
</tr>
</tbody>
</table>

**Configuration Mode**

- Config Interface Ethernet Traffic Class
- Config Interface Port Channel Traffic Class
- Config Interface MLAG Port Channel Traffic Class

**History**

3.6.1002

**Role**

admin

**Example**

```
switch (config interface ethernet 1/1 traffic-class 1) # dcb ets wrr 50
```

**Related Commands**

N/A

**Notes**

- Context is egress interface traffic class
- This command is only supported on Spectrum™ based switch systems
mc-unaware tc binding

**mc-unaware tc binding**  
**no mc-unaware tc binding**

Configures the MC-unaware TC binding.  
The no form of the command disables MC-unaware TC binding.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>Disabled</td>
</tr>
</tbody>
</table>
| Configuration Mode | Config Interface Ethernet  
|                    | Config Interface Port Channel  
|                    | Config Interface MLAG Port Channel |
| History            | 3.6.1002 |
| Role               | admin |
| Example            | `switch (config interface ethernet 1/1) # mc-unaware tc binding` |
| Related Commands   | N/A |
| Notes              | • When the no form is configured, the multicast traffic of a switch-priority that is mapped to TC X is re-mapped to TC X+8  
|                    | • Context is egress interface  
|                    | • This command is only supported on Spectrum™ based switch systems |
show dcb ets (Spectrum)

    show dcb ets [interface {ethernet | mlag-port-channel | port-channel} <number>]

Displays ETS information.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>Disabled</td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Any Command Mode</td>
</tr>
<tr>
<td>History</td>
<td>3.6.1002</td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
</tr>
</tbody>
</table>
Example

```
switch (config) # show dcb ets interface ethernet 1/1
Eth1/1
Interface Bandwidth Shape [Mbps]: 100000
Multicast unaware mapping : disabled

ETS per TC :
TC Scheduling Mode Weight Weight (%)
-- --------------- ------ ----------
 0  WRR             12     12
 1  WRR             13     13
 2  WRR             12     12
 3  WRR             13     13
 4  WRR             12     12
 5  WRR             13     13
 6  WRR             12     12
 7  WRR             13     13

Bandwidth Shape per TC:
TC Bandwidth Shape [Mbps]
-- ----------------------
 0  100000
 1  100000
 2  100000
 3  100000
 4  100000
 5  100000
 6  100000
 7  100000

Bandwidth Guarantee per TC:
TC Bandwidth Guaranteed [Mbps]
-- ---------------------------
 0  0
 1  0
 2  0
 3  0
 4  0
 5  0
 6  0
 7  0

Switch Priority to TC mapping:
Switch Priority TC
--------------- --
 0               0
 1               1
 2               2
 3               3
 4               4
 5               5
 6               6
 7               7
```

Related Commands
N/A

Notes
The show command output is from a Spectrum™ based switch systems
5.14.6.4 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.

### Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>red</td>
<td>Enables random early detection for traffic class queue.</td>
</tr>
<tr>
<td>ecn</td>
<td>Enables explicit congestion notification for traffic class queue.</td>
</tr>
<tr>
<td>both</td>
<td>Enables both RED and ECN marking for traffic class queue.</td>
</tr>
<tr>
<td>minimum-absolute</td>
<td>Set minimum-absolute value (in KBs) for marking traffic-class queue</td>
</tr>
<tr>
<td>maximum-absolute</td>
<td>Set minimum-absolute value (in KBs) for marking traffic-class queue</td>
</tr>
<tr>
<td>minimum-relative</td>
<td>Set minimum-relative value (in percentage) for marking traffic-class queue</td>
</tr>
<tr>
<td>maximum-relative</td>
<td>Set maximum-relative value (in percentage) for marking traffic-class queue</td>
</tr>
</tbody>
</table>

### Default

Disabled

### Configuration Mode

Config Interface Ethernet

### History

3.5.1000

### Role

admin

### Example

```
switch (config interfaces ethernet 1/1)# traffic-class 0 congestion-control both minimum-relative 50 maximum-relative 80
```

### Related Commands

Note
### show interfaces ethernet congestion-control

 Displays specific interface congestion control information.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>N/A</td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Any Command Mode</td>
</tr>
<tr>
<td>History</td>
<td>3.5.1000</td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
</tr>
</tbody>
</table>

**Example**

```
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) #
```
<table>
<thead>
<tr>
<th>Related Commands</th>
</tr>
</thead>
<tbody>
<tr>
<td>Note</td>
</tr>
</tbody>
</table>
5.15 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.

5.15.1 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
```

5.15.2 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/mac access-list**
   b. Add access list rule using the command **deny/permit (action <action profile name>)**

Step 3. Bind the access-list to an interface using the command **ipv4/mac port access-group.**

```plaintext
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
```

### 5.15.3 Commands

**ipv4/mac access-list**

```plaintext
{ipv4 | mac} access-list <acl-name>
no {ipv4 | mac} access-list <acl-name>
```

Creates a MAC or IPv4 ACL and enter the ACL configuration mode. The no form of the command deletes the ACL.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>ipv4</th>
<th>mac</th>
<th>IPv4 or MAC – access list.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>acl-name</td>
<td>User defined string for the ACL.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Default</th>
<th>No ACL available by default.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuration Mode</td>
<td>Config</td>
</tr>
<tr>
<td>History</td>
<td>3.1.1400</td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
</tr>
</tbody>
</table>
| Example        | `switch (config)# mac access-list my-mac-list
switch (config mac access-list my-mac-list)#` |

**Related Commands**

- ipv4/port access-group

**Note**
ipv4/mac port access-group

{ipv4 | mac} port access-list <acl-name>
no {ipv4 | mac} port access-list <acl-name>

Binds an ACL to the interface.
The no form of the command unbinds the ACL from the interface.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>ipv4</th>
<th>mac IPv4 or MAC – access list.</th>
</tr>
</thead>
<tbody>
<tr>
<td>acl-name</td>
<td>acl-name ACL name.</td>
<td></td>
</tr>
</tbody>
</table>

Default
No ACL is bind by default.

Configuration Mode
Config Interface Ethernet
Config Interface Port Channel
Config Interface MLAG Port Channel

History
3.1.1400
3.3.4500 Added MLAG port-channel configuration mode

Role
admin

Example
switch (config interface ethernet 1/1) # mac port access-group my-list
switch (config interface ethernet 1/1) #

Related Commands
ipv4/mac access-list

Note
The access control list should be defined prior to the binding action.
deny/permit (MAC ACL rule)

[seq-number <sequence-number>] [deny|permit] [any | <source-mac> [mask <mac>]] [any | <destination-mac> [mask <mac>]] [protocol <protocol>] [cos <cos-value>] [vlan <vlan-id> | vlan-mask <vlan-mask>] [action <action-id>]
no <sequence-number>

Creates a rule for MAC ACL.
The no form of the command deletes a rule from the MAC ACL.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>sequence-number</th>
<th>Optional parameter to set a specific sequence number for the rule. The range is: 1-65535.</th>
</tr>
</thead>
<tbody>
<tr>
<td>deny</td>
<td>permit</td>
<td>Determines the type of the rule, denies or permits action.</td>
</tr>
<tr>
<td>{any</td>
<td>&lt;source-mac&gt; [mask &lt;mac&gt;]}</td>
<td>Sets source MAC and optionally sets a mask for that MAC. The “any” option will cause the rule not to check the source MAC.</td>
</tr>
<tr>
<td>{any</td>
<td>&lt;destination-mac&gt; [mask &lt;mac&gt;]}</td>
<td>Sets destination MAC and optionally sets a mask for that MAC. The “any” option will cause the rule not to check the destination MAC.</td>
</tr>
<tr>
<td>protocol</td>
<td>Sets the Ethertype filed value from the MAC address. Possible range is: 0x0000-0xffff.</td>
<td></td>
</tr>
<tr>
<td>cos-value</td>
<td>Sets the COS (priority bits) field, possible range is: 0-7.</td>
<td></td>
</tr>
<tr>
<td>vlan-id</td>
<td>Sets the VLAN ID field, possible range is 0-4095</td>
<td></td>
</tr>
<tr>
<td>vlan-mask &lt;vlan-mask&gt;</td>
<td>Sets VLAN group. Range: 0x0000-0x0FFF.</td>
<td></td>
</tr>
<tr>
<td>action</td>
<td>Action name (free string)</td>
<td></td>
</tr>
</tbody>
</table>

Default
No rule is added by default to access control list. Default sequence number is in multiple of 10.

Configuration Mode
Config MAC ACL

History
3.1.1400
3.3.4500 Added vlan-mask parameter
3.5.1000 Updated seq-number parameter

Role
admin

Example
switch (config mac access-list my-list) # seq-number 10 deny 0a:0a:0a:0a:0a mask ff:ff:ff:ff:ff any vlan 6 cos 2 protocol 80
switch (config mac access-list my-list) #
<table>
<thead>
<tr>
<th>Related Commands</th>
<th>ipv4/mac access-list</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>ipv4/mac port access-group</td>
</tr>
</tbody>
</table>

**Note**
deny/permit (IPv4 ACL rule)

```
[seq-number <sequence-number>] [permit | deny] ip [<source-ip> [mask <ip>] | [any]} \[dest-ip> [mask <ip>] | [any]} [action <action-id>]

no <sequence-number>
```

Creates a rule for IPv4 ACL.
The no form of the command deletes a rule from the IPv4 ACL.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>sequence-number</th>
<th>Optional parameter to set a specific sequence number for the rule. The range is:1-65535.</th>
</tr>
</thead>
<tbody>
<tr>
<td>deny</td>
<td>permit</td>
<td>Determines the type of the rule, deny or permit action.</td>
</tr>
<tr>
<td>{any</td>
<td>&lt;source-ip&gt; [mask &lt;ip&gt;]</td>
<td>Sets source IP and optionally sets a mask for that IP address. The “any” option causes the rule to not check the source IP. Valid mask values fall in the range 0-255.</td>
</tr>
<tr>
<td>{any</td>
<td>&lt;destination-ip&gt; [mask &lt;ip&gt;]</td>
<td>Sets destination IP and optionally sets a mask for that MAC. The “any” option causes the rule to not check the destination MAC.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Default</th>
<th>No rule is added by default to access control list. Default sequence number is in multiple of 10.</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Configuration Mode</th>
<th>Config IPv4 ACL</th>
</tr>
</thead>
</table>

**History**

| 3.1.1400 | First version |
| 3.3.4302 | Updated syntax description of mask <ip> parameter |
| 3.5.1000 | Updated seq-number parameter |

<table>
<thead>
<tr>
<th>Role</th>
<th>admin</th>
</tr>
</thead>
</table>

**Example**

```
switch (config ipv4 access-list my-list) # seq-number 51 deny ip 1.1.1.1 mask 123.12.13.53 45.45.45.0 mask 123.132.21.123
switch (config ipv4 access-list my-list) #
```

**Related Commands**

- ipv4/mac access-list
- ipv4/mac port access-group

**Note**
deny/permit (IPv4 TCP/UDP/ICMP ACL rule)

[seq-number <sequence-number>] [permit | deny] [tcp | udp | icmp] {<source-ip> [mask <ip>] | [any]} {<dest-ip> [mask <ip>] | [any]} [eq-source <port-number>] [eq-destination <port-number>] [action <action-id>] [eq-code <icmp-code>] [eq-type <icmp-type>]

no <sequence-number>

Creates a rule for IPv4 UDP/TCP/ICMP ACL.
The no form of the command deletes a rule from the ACL.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>sequence-number</th>
<th>Optional parameter to set a specific sequence number for the rule. The range is 1-65535.</th>
</tr>
</thead>
<tbody>
<tr>
<td>deny</td>
<td>permit</td>
<td>Determines the type of the rule, deny or permit action.</td>
</tr>
<tr>
<td>tcp</td>
<td>udp</td>
<td>icmp</td>
</tr>
<tr>
<td>{any</td>
<td>&lt;source-ip&gt; [mask &lt;ip&gt;]</td>
<td>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.</td>
</tr>
<tr>
<td>{any</td>
<td>&lt;destination-ip&gt; [mask &lt;ip&gt;]</td>
<td>Sets destination IP and optionally sets a mask for that IP. The “any” option will cause the rule not to check the destination IP.</td>
</tr>
<tr>
<td>[eq-source &lt;port-number&gt;]</td>
<td>TCP/UDP/ICMP source port number Range is 0-65535</td>
<td></td>
</tr>
<tr>
<td>[eq-destination &lt;port-number&gt;]</td>
<td>TCP/UDP/ICMP destination port number Range is 0-65535</td>
<td></td>
</tr>
<tr>
<td>eq-code &lt;icmp-code&gt;</td>
<td>Range: 0-255</td>
<td></td>
</tr>
<tr>
<td>eq-type &lt;icmp-type&gt;</td>
<td>Range: 0-255</td>
<td></td>
</tr>
</tbody>
</table>

Default
No rule is added by default to access control list
Default sequence number is in multiple of 10

Configuration Mode
Config IPv4 ACL

History
3.1.1400
3.5.1000 Updated seq-number parameter
3.6.2002 Added ICMP options and Notes section

Role
admin

Example
switch (config ipv4 access-list my-list) # seq-number 10 deny tcp any any eq-source 1200
switch (config ipv4 access-list my-list) #
### Related Commands
- `ipv4/mac access-list`
- `ipv4/mac port access-group`

### 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.
- The parameters “eq-source” and “eq-destination” are not applicable with ICMP
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.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>action-profile-name</th>
<th>given name for the profile.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>N/A</td>
<td></td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Config</td>
<td></td>
</tr>
<tr>
<td>History</td>
<td>3.2.0230</td>
<td></td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
<td></td>
</tr>
</tbody>
</table>

Example

switch (config)# access-list action my-action
switch (config access-list action my-action)# show access-list action my-action
Access-list Action my-action
Mapped_VLAN_ID | Mapped_port | Counter_set | Policer_ID |
-----------------------------------------------
N/A | N/A | N/A | N/A |

Related Commands

Note
**vlan-map**

`vlan-map <vlan-id>`
`no vlan-map`

Adds action to map a new VLAN to the packet (in the ingress port or VLAN). The `no` form of the command removes the action to map a new VLAN.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>vlan-id</code></td>
<td>N/A</td>
<td>0-4095</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Default</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuration Mode</td>
<td>Config ACL Action</td>
</tr>
<tr>
<td>History</td>
<td>3.2.0230</td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
</tr>
</tbody>
</table>

**Example**

```
switch (config access-list action my-action)# vlan-map 10
switch (config access-list action my-action)# show access-list action my-action
Access-list Action my-action
Mapped_Vlan_ID | Mapped_port | Counter_set | Policer_ID |
-----------------------------------------------
10 | N/A | N/A | N/A |
switch (config access-list action my-action)#
```

**Related Commands**

**Note**
**vlan-pop**

Pops VLAN frames from traffic.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan-id</td>
<td>VLAN ID: 0-4095.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Default</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuration Mode</td>
<td>Config ACL Action</td>
</tr>
<tr>
<td>History</td>
<td>3.4.3000</td>
</tr>
</tbody>
</table>

**Example**

```
switch (config access-list action my-action)# vlan-pop
switch (config access-list action my-action)# show access-list action my-action
Access-list Action my-action
Popped_VLAN_ID | Mapped_port | Counter_set | Policer_ID |
```

```
N/A | N/A | N/A | N/A |
```

**Related Commands**

**Note**
**vlan-push**

`vlan-push <vlan-id>`

Pushes (or adds) VLAN frames to traffic.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>vlan-id</code></td>
<td>VLAN ID: 0-4095</td>
</tr>
</tbody>
</table>

**Default**

N/A

**Configuration Mode**

Config ACL Action

**History**

3.4.3000

**Role**

admin

**Example**

```
switch (config access-list action my-action)# vlan-push 10
switch (config access-list action my-action)# show access-list action my-action
Access-list Action my-action
Mapped_VLAN_ID |Mapped_port |Counter_set |Policer_ID |
---------------------------------------------------------
10              |N/A         |N/A         |N/A       |

switch (config access-list action my-action)#
```
show access-list action

```
show access-list action {<action-profile-name> | summary}
```

Displays the access-list action profiles summary.

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>action-profile-name</td>
<td>Filter the table according to the action profile name.</td>
</tr>
<tr>
<td>summary</td>
<td>Display summary of the action list.</td>
</tr>
</tbody>
</table>

**Default**

N/A

**Configuration Mode**

Any Command Mode

**History**

3.2.0230

**Role**

admin

**Example**

```
switch (config)# show access-list action my-action
Access-list Action my-action
Mapped_Vlan_ID |Mapped_port |Counter_set |Policer_ID |
---------------------------------------------------------------
10 |N/A         |N/A         |N/A        |
```

**Related Commands**

**Note**
**show mac/ipv4 access-lists**

```
show [mac |ipv4 |] access-lists <access-list-name>
```

Displays the list of rules for the MAC/IPv4 ACL.

### Syntax Description

<table>
<thead>
<tr>
<th>Access List Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>mac</td>
<td>IPv4 or MAC - access list.</td>
</tr>
<tr>
<td>access-list-name</td>
<td>ACL name.</td>
</tr>
</tbody>
</table>

### Default

N/A

### Configuration Mode

Any Command Mode

### History

3.1.1400

Updated output

### Role

admin

### Example

```
switch (config mac access-list my-list) # show mac access-lists my-list
mac access-list my-list
seq-number|p/d   |smac |dmac |protocol|cos  |vlan |vlan-mask|action|
-----------------------------------------------
10       |deny  |any  |any  |0800    |3    |3    |0x0FFF  |none  |
20       |deny  |any  |any  |80      |2    |6    |0x0000  |none  |
30       |deny  |any  |any  |any     |any  |any  |0x0ACB  |none  |
40       |deny  |any  |any  |any     |any  |any  |N/A     |none  |
switch (config mac access-list my-list) #
```

### Related Commands

- deny/permit (MAC ACL rule)
- deny/permit (IPv4 ACL rule)
- deny/permit (IPv4 TCP/UDP ACL rule)
- ipv4/mac access-list
- ipv4/mac port access-group

### Note
## show mac/ipv4 access-lists summary

```bash
show [mac | ipv4 |] access-lists summary
```

Displays the summary of number of rules per ACL, and the interfaces attached.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>ipv4</th>
<th>mac</th>
<th>IPv4 or MAC - Access list</th>
</tr>
</thead>
<tbody>
<tr>
<td>access-list-name</td>
<td></td>
<td></td>
<td>ACL name</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Default</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuration Mode</td>
<td>Any Command Mode</td>
</tr>
<tr>
<td>History</td>
<td>3.1.1400</td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
</tr>
</tbody>
</table>

**Example**

```
switch (config) # show mac access-lists summary
mac access-list my-list
  Total ACEs Configured: 2
  Configured on interfaces:
    Ethernet 1/1
    Ethernet 1/2
switch (config) #
```

**Related Commands**

deny/permit (MAC ACL rule)
deny/permit (IPv4 ACL rule)
deny/permit (IPv4 TCP/UDP ACL rule)
ipv4/mac access-list
ipv4/mac port access-group

**Note**
5.16 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 24 provides an overview of the 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.

5.16.1 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.
A mirroring session is a monitoring configuration mode that has the following parameters:

**Table 56 - Mirroring Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Access</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source interface(s)</td>
<td>List of source interfaces to be mirrored.</td>
<td>RW</td>
</tr>
<tr>
<td>Destination interface</td>
<td>A single analyzer port through which all mirrored traffic egress.</td>
<td>RW</td>
</tr>
<tr>
<td>Header format</td>
<td>The format and encapsulation of the mirrored traffic when sent to analyzer.</td>
<td>RW</td>
</tr>
<tr>
<td>Truncation</td>
<td>Enabling truncation segments each mirrored packet to 64 bytes.</td>
<td>RW</td>
</tr>
<tr>
<td>Congestion control</td>
<td>Controls the behavior of the source port when destination port is congested.</td>
<td>RW</td>
</tr>
<tr>
<td>Admin state</td>
<td>Administrative state of the monitoring session.</td>
<td>RW</td>
</tr>
</tbody>
</table>

### 5.16.1.1 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.
5.16.1.2 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).

5.16.1.3 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.
5.16.1.4 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.

5.16.1.5 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.

5.16.2 Configuring Mirroring Sessions

Figure 27 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 con-
nectivity 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 27: 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
```
Step 7. Enable the session. Run:

```
switch (config monitor session 1) # no shutdown
```
5.16.3 Verifying Mirroring Sessions

➢ To verify the attributes of a specific mirroring session:

```bash
switch (config) # show monitor session 1
Admin: Enable
Status: Up
Truncate: Enable
Destination interface: eth1/2
Congestion type: pause-excessive-frames
Header format: add-ethernet-header
  - traffic class 2
  - vlan 10
  - priority 5
  - destination-mac 00:0d:ec:f1:a9:c8

Source interfaces
  Interface   direction
  -----------
  eth1/1     both
```

➢ To verify the attributes of running mirroring sessions:

```bash
switch (config) # show monitor session summary
Session  Admin  Status  Mode      Destination   Source
       1   Enable  Up    add-eth  eth1/2     eth1/1(b)
       2  Disable  Down  add-vlan  eth1/2     eth1/8(i), po1(e)
       3   Enable  Up    add-eth  eth1/5     eth1/18(e)
       7  Disable  Down  local          
```

5.16.4 Commands

5.16.4.1 Config

monitor session

```bash
monitor session <session-id>
no monitor session <session-id>
```

Creates session and enters monitor session configuration mode upon using this command for the first time.
The no form of the command deletes the session.

**Syntax Description**

- **session-id**: The monitor session ID.
  - Range is:
    - 1-7 for SwitchX®
    - 1-2 for Spectrum™

**Default**

- N/A

**Configuration Mode**

- Config
<table>
<thead>
<tr>
<th>History</th>
<th>3.3.3500</th>
</tr>
</thead>
<tbody>
<tr>
<td>Role</td>
<td>admin</td>
</tr>
<tr>
<td>Example</td>
<td><code>switch (config)# monitor session 1</code>&lt;br&gt;<code>switch (config monitor session 1)#</code></td>
</tr>
</tbody>
</table>

**Related Commands**

**Note**
5.16.4.2 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.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>interface &lt;type&gt; &lt;number&gt;</td>
<td>Sets the interface type and number (e.g. ethernet 1/2)</td>
</tr>
<tr>
<td>force</td>
<td>The user does not need to shutdown the port prior the operation.</td>
</tr>
</tbody>
</table>

**Default**
no destination interface

**Configuration Mode**
Config Monitor Session

**History**

- 3.3.3500 First version
- 3.3.4100 Added force argument

**Role**
admin

**Example**

```
switch (config monitor session 1) # destination interface ethernet 1/2
switch (config monitor session 1)#
```

**Related Commands**

**Note**
**shutdown**

```plaintext
shutdown
no shutdown
```

Disables the session. The no form of the command enables the session.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>Disabled</td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Config Monitor Session</td>
</tr>
<tr>
<td>History</td>
<td>3.3.3500</td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
</tr>
</tbody>
</table>
| Example            | switch (config monitor session 1) # no shutdown
                   | switch (config monitor session 1)# |

**Related Commands**

**Note**
add source interface

add source interface <type> <number> direction <d-type>
no source interface <type> <number>

Adds a source interface to the mirrored session. The no form of the command deletes the source interface.

Syntax Description

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>interface &lt;type&gt; &lt;number&gt;</td>
<td>Configures interface as “ethernet” or “port-channel”.</td>
</tr>
</tbody>
</table>
| direction <d-type> | Configures the direction of the mirrored traffic. The options are as follows:  
  • egress – sets the egress traffic to be monitored  
  • ingress – sets the ingress traffic to be monitored  
  • both – sets egress and ingress traffic to be monitored |

Default

N/A

Configuration Mode

Config Monitor Session

History

3.3.3500

3.5.1000 Updated

Role

admin

Example

switch (config monitor session 1) # add source interface ethernet 1/1 direction ingress
switch (config monitor session 1) #

Related Commands

Note

• If mirroring is configured in one direction (e.g. ingress) on an interface and then is configured in the other direction (e.g. egress), then the ultimate setting is “both”
• Spectrum™ based switch systems only support mirroring ingress traffic
header-format

header-format {local [traffic-class <tc>] | add-vlan <vlan-id> [priority <prio>] [traffic-class <tc>] | switch-priority <sp> | add-ethernet-header destination-mac <mac-address> [add-vlan <vlan-id> [priority <prio>]] [traffic-class <tc>]

no header-format

Sets the header format of the mirrored traffic.
The no form of the command resets the parameter values back to default.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>local</td>
<td>The mirrored header of the frame is not changed.</td>
</tr>
<tr>
<td>traffic-class &lt;tc&gt;</td>
<td>Changes the egress traffic class of the frame.</td>
</tr>
<tr>
<td></td>
<td>Range: 0-3.</td>
</tr>
<tr>
<td>switch-priority &lt;sp&gt;</td>
<td>Changes the egress switch priority of the frame.</td>
</tr>
<tr>
<td></td>
<td>Range: 0-15.</td>
</tr>
<tr>
<td>add-vlan &lt;vlan-id&gt;</td>
<td>An 802.1q VLAN tag is added to the frame.</td>
</tr>
<tr>
<td>priority &lt;prio&gt;</td>
<td>The priority to be added to the Ethernet header.</td>
</tr>
<tr>
<td></td>
<td>Range: 0-7.</td>
</tr>
<tr>
<td>add-ethernet-header</td>
<td>Adds an Ethernet header to the mirrored frame.</td>
</tr>
<tr>
<td>destination-mac</td>
<td>The destination MAC address of the added Ethernet frame.</td>
</tr>
</tbody>
</table>

Default

no-change
vlan 1
priority 0
traffic-class 0

Configuration Mode

Config Monitor Session

History

3.3.3500
3.5.1000 Added switch-priority parameter

Role

admin

Example

```
switch (config monitor session 1) # header-format add-ethernet-header destination-mac 00:0d:ec:f1:a9:c8 add-vlan 10 priority 5 traffic-class 2
switch (config monitor session 1)#
```
## Related Commands

### Note
- If add-ethernet-header is used, the source MAC address is the one attached to the switch
- The parameter traffic-class is only available on SwitchX® based switch systems
- The parameter switch-priority is only available on Spectrum™ based switch systems
### truncate

**Syntax**

- **truncate**
- **no truncate**

Truncates the mirrored frames to 64-byte packets. The no form of the command disables truncation.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>no truncate</td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Config Monitor Session</td>
</tr>
<tr>
<td>History</td>
<td>3.3.3500</td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
</tr>
</tbody>
</table>
| Example            | switch (config monitor session 1) # truncate  
switch (config monitor session 1)# |
| Related Commands   | This command applies for all sessions on the same analyzer port. |
| Note               | |
### 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.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>drop-excessive-frames</td>
<td>Drops excessive frames.</td>
</tr>
<tr>
<td>pause-excessive-frames</td>
<td>Pauses excessive frames.</td>
</tr>
</tbody>
</table>

**Default**

drop-excessive-frames

**Configuration Mode**

Config Monitor Session

**History**

3.3.3500

3.3.4000 Added Syntax Description.

**Role**

admin

**Example**

switch (config monitor session 1) # congestion pause-excessive-frames
switch (config monitor session 1)#

**Related Commands**

This command applies for all sessions on the same analyzer port.
show monitor session

show monitor session <session-id>

Displays monitor session configuration and status.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>session-id</th>
<th>The monitor session ID. Range is 1-7.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>N/A</td>
<td></td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Any Command Mode</td>
<td></td>
</tr>
<tr>
<td>History</td>
<td>3.3.3500</td>
<td></td>
</tr>
<tr>
<td></td>
<td>3.5.1000</td>
<td>Updated Note section</td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
<td></td>
</tr>
</tbody>
</table>

Example

```
switch (config) # show monitor session 1
Admin: Enable
Status: Up
Truncate: Enable
Destination interface: eth1/2
Congestion type: pause-excessive-frames
Header format: add-ethernet-header
  - traffic class 2
  - vlan 10
  - priority 5
  - destination-mac 00:0d:ec:f1:a9:c8
Source interfaces
Interface direction
-------------------------
eth1/1 both
switch (config) #
```

Related Commands

Note

The output provided is from a SwitchX® based switch system.
show monitor session summary

Displays monitor session configuration and status summary.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>N/A</td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Any Command Mode</td>
</tr>
<tr>
<td>History</td>
<td>3.3.3500</td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
</tr>
</tbody>
</table>

**Example**

```
switch (config) # show monitor session summary
Session  Admin  Status  Mode  Destination  Source
1        Enable Up    add-eth eth1/2  eth1/1(b)
2        Disable Down add-vlan eth1/2  eth1/8(i), po1(e)
3        Enable Up    add-eth eth1/5  eth1/18(e)
7        Disable Down local  Source
switch (config) #
```

**Related Commands**

**Note**
5.17 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 28: sFlow Functionality Overview**

5.17.1 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.
5.17.2 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 57 - List of Statistical Counters

<table>
<thead>
<tr>
<th>Counter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total packets</td>
<td>The number of packets that pass through sFlow-enabled ports.</td>
</tr>
<tr>
<td>Number of flow samples</td>
<td>The number of packets that are captured by the sampling mechanism.</td>
</tr>
<tr>
<td>Number of statistic samples</td>
<td>The number of statistical samples.</td>
</tr>
<tr>
<td>Number of discarded samples</td>
<td>The number of samples that were discarded.</td>
</tr>
<tr>
<td>Number of datagrams</td>
<td>The number of datagrams that were sent to the collector.</td>
</tr>
</tbody>
</table>

5.17.3 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.

5.17.4 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.

5.17.5 Configuring sFlow

➢ To configure the sFlow agent:

Step 1. Unlock the sFlow commands. Run:

```
switch (config) # protocol sflow
```

Step 2. Enable sFlow on the system. Run:

```
switch (config) # sflow enable
```

Step 3. Enter sFlow configuration mode. Run:

```
switch (config) # sflow
switch (config sflow) #
```
Step 4. Set the central collector’s IP. Run:

```
switch (config sflow) # collector-ip 10.10.10.10
```

Step 5. Set the agent-ip used in the sFlow header. Run:

```
switch (config sflow) # agent-ip 20.20.20.20
```

Step 6. (Optional) Set the sampling rate of the mechanism. Run:

```
switch (config sflow) # sampling-rate 16000
```

This means that one every 16000 packet gets collected for sampling.

Step 7. (Optional) Set the maximum size of the data path sample. Run:

```
switch (config sflow) # max-sample-size 156
```

Step 8. (Optional) Set the frequency in which counters are polled. Run:

```
switch (config sflow) # counter-poll-interval 19
```

Step 9. (Optional) Set the maximum size of the datagrams sent to the central collector. Run:

```
switch (config sflow) # max-datagram-size 1500
```

Step 10. Enable the sFlow agent on the desired interfaces. Run:

```
switch (config interface ethernet 1/1)# sflow enable
switch (config interface port-channel 1)# sflow enable
```
5.17.6 Verifying sFlow

➢ To verify the attributes of the sFlow agent:

switch (config)# show sflow

sflow protocol enabled
sflow enabled
sampling-rate 16000
max-sampled-size 156
counter-poll-interval 19
max-datagram-size 1500
collector-ip 10.10.10.10
collector-port 6343
agent-ip 20.20.20.20
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

5.17.7 Commands

5.17.7.1 Config

protocol sflow

no protocol sflow

Unhides the sFlow commands.
The no form of the command deletes sFlow configuration and hides the sFlow commands.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>Disabled</td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Config</td>
</tr>
<tr>
<td>History</td>
<td>3.3.3500</td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
</tr>
</tbody>
</table>
| Example            | switch (config) # protocol sflow
switch (config) # |
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.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>N/A</td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Config</td>
</tr>
<tr>
<td>History</td>
<td>3.3.3500</td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
</tr>
</tbody>
</table>

Example

```
switch (config) # sflow
switch (config sflow) #
```

Related Commands

Note
### 5.17.7.2 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.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>rate</th>
<th>Sets the number of packets passed before selecting one for sampling. The range is 4000-16777215. Zero disables sampling.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>16000</td>
<td></td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Config sFlow</td>
<td></td>
</tr>
<tr>
<td>History</td>
<td>3.3.3500</td>
<td></td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
<td></td>
</tr>
<tr>
<td>Example</td>
<td>switch (config sflow) # sampling-rate 16111</td>
<td></td>
</tr>
</tbody>
</table>

**Related Commands**

Note
**max-sample-size**

```
max-sample-size <packet-size>
no max-sample-size
```

Sets the maximum size of sampled packets by sFlow. The `no` form of the command resets the parameter to its default value.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>packet-size</th>
<th>The sampled packet size. The range is 64-256 bytes.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>128 bytes</td>
<td></td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Config sFlow</td>
<td></td>
</tr>
<tr>
<td>History</td>
<td>3.3.3500</td>
<td></td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
<td></td>
</tr>
<tr>
<td>Example</td>
<td></td>
<td>switch (config sflow) # max-sample-size 165</td>
</tr>
<tr>
<td></td>
<td></td>
<td>switch (config sflow) #</td>
</tr>
<tr>
<td>Related Commands</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Note</td>
<td></td>
<td>Sampled payload beyond the configured size is discarded.</td>
</tr>
</tbody>
</table>

Sampled payload beyond the configured size is discarded.
**counter-poll-interval**

```plaintext
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.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>seconds</td>
<td>The sFlow statistics polling interval in seconds. Range is 5-3600 seconds. Zero disables the statistic polling.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>20 seconds</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Configuration Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>Config sFlow</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>History</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.3.3500</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>admin</td>
</tr>
</tbody>
</table>

**Example**

```
switch (config sflow) # counter-poll-interval 30
switch (config sflow) #
```

**Related Commands**

**Note**
**max-datagram-size**

```bash
max-datagram-size <packet-size>
no max-datagram-size
```

Sets the maximum sFlow packet size to be sent to the collector. The no form of the command resets the parameter to its default value.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>packet-size</th>
<th>The packet size of the packet being sent to the collector. The range is 200-9216 bytes.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>1400 bytes</td>
<td></td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Config sFlow</td>
<td></td>
</tr>
<tr>
<td>History</td>
<td>3.3.3500</td>
<td></td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
<td></td>
</tr>
<tr>
<td>Example</td>
<td></td>
<td>switch (config sflow) # max-datagram-size 9216</td>
</tr>
<tr>
<td></td>
<td></td>
<td>switch (config sflow) #</td>
</tr>
</tbody>
</table>

**Related Commands**

**Note**

This packet contains the data sample as well as the statistical counter data.
**collector-ip**

`collector-ip <ip-address> [udp-port <udp-port-number>]`  
`no collector-ip [<ip-address> udp-port]`

Sets the collector’s IP.  
The no form of the command resets the parameters to their default values.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>ip-address</th>
<th>The collector IP address.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>udp-port &lt;udp-port-number&gt;</td>
<td>Sets the collector UDP port number.</td>
</tr>
</tbody>
</table>

| Default            | ip-address: 0.0.0.0  
|                   | udp-port-number: 6343 |

<table>
<thead>
<tr>
<th>Configuration Mode</th>
<th>Config sFlow</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>History</th>
<th>3.3.3500</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Role</th>
<th>admin</th>
</tr>
</thead>
</table>

**Example**  
```
switch (config sflow) # collector-ip 10.10.10.10
```

**Related Commands**  
```
switch (config sflow) #
```

**Note**
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.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>interface</td>
<td>Configures a specific ethernet/port-channel interface’s agent IP.</td>
</tr>
<tr>
<td>if-name</td>
<td>Interface name (e.g. mgmt0, mgmt1).</td>
</tr>
<tr>
<td>ip-address</td>
<td>The sFlow agent’s IP address (i.e. the source IP of the packet).</td>
</tr>
<tr>
<td>loopback &lt;number&gt;</td>
<td>Loopback interface number. Range: 1-32.</td>
</tr>
<tr>
<td>vlan &lt;id&gt;</td>
<td>Interface VLAN. Range: 1-4094.</td>
</tr>
</tbody>
</table>

Default: ip-address: 0.0.0.0

Configuration Mode: Config sFlow

History:
3.3.3500
3.3.5200 Updated “interface” parameters

Role: admin

Example:
switch (config sflow) # agent-ip 20.20.20.20
switch (config sflow) #

Related Commands

Note: The IP address here is used in the sFlow header.
## clear counters

Clears sFlow counters.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>N/A</td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Config sFlow</td>
</tr>
<tr>
<td>History</td>
<td>3.3.3500</td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
</tr>
</tbody>
</table>

### 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.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>N/A</th>
</tr>
</thead>
</table>
| Default            | disable  
no view-port-channel member |
| Configuration Mode | Config Interface Ethernet  
Config Interface Port Channel  
Config Interface MLAG Port Channel |
| History            | 3.3.3500  
3.3.4500 Added MLAG port-channel configuration mode |
| Role               | admin |
| Example            | switch(config interface ethernet 1/1)# sflow enable  
...  
switch(config interface port-channel 1)# sflow enable |
| Related Commands   |     |
| Note               |     |
### show sflow

**show sflow**

Displays sFlow configuration and counters.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>N/A</td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Any Command Mode</td>
</tr>
<tr>
<td>History</td>
<td>3.3.3500</td>
</tr>
<tr>
<td></td>
<td>3.6.3004 Updated output example</td>
</tr>
</tbody>
</table>

**Role**

admin

**Example**

```bash
switch (config)# show sflow
sflow protocol enabled
sflow enabled
sampling-rate 16000
max-sampled-size 156
counter-poll-interval 19
max-datagram-size 1500
collector-ip 10.10.10.10
collector-port 6343
agent-ip 20.20.20.20
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
```

**Related Commands**

**Note**
5.18 Transport Applications

5.18.1 RDMA over Converged Ethernet (RoCE)

5.18.1.1 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.

5.18.1.1.1 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 29: 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 way¹.

**Figure 30: RoCEv2 Protocol Stack**

5.18.1.2 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:


¹. Standard RDMA APIs are IP based already for all existing RDMA technologies
5.18.1.2.1 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”.

5.18.1.2.2 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.

5.18.1.2.2.1 Using Global Pause Flow Control (GFC)

To use Global Pause Flow Control (GFC) mode, disable QoS and Priority:

```
PS > Disable-NetQosFlowControl
PS > Disable-NetAdapterQos
```

5.18.1.3 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

5.18.1.4 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.

5.18.1.4.1 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.

5.18.1.5 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:
    ```powershell
    Set-MlnxDriverCoreSetting -RoceMode 1
    ```

- **To enable RoCEv2 using the PowerShell:**
  - Open the PowerShell and run:
    ```powershell
    Set-MlnxDriverCoreSetting -RoceMode 2
    ```

- **To disable any version of RoCE using the PowerShell:**
  - Open the PowerShell and run:
    ```powershell
    Set-MlnxDriverCoreSetting -RoceMode 0
    ```

- **To check current version of RoCE using the PowerShell:**
  
  **Step 1.** Open the PowerShell and run:
  ```powershell
  Get-MlnxDriverCoreSetting
  ```

  **Step 2.** Example output:

  ```plaintext
  Caption               : DriverCoreSettingData 'mlx4_bus'
  Description           : Mellanox Driver Option Settings
  
  RoceMode              : 0
  ```
5.19 802.1x 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.

5.19.1 802.1x 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 unau-
thenticated. 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.

5.19.2 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)#
```
### 5.19.3 Commands

**protocol dot1x**

- **protocol dot1x**
- **no protocol dot1x**

Enables 802.1x EAPOL protocol.
The no form of the command disables 802.1x EAPOL protocol.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>Disabled</td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Config</td>
</tr>
<tr>
<td>History</td>
<td>3.4.2008</td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
</tr>
<tr>
<td>Example</td>
<td>switch (config)# protocol dot1x</td>
</tr>
<tr>
<td>Related Commands</td>
<td></td>
</tr>
<tr>
<td>Note</td>
<td></td>
</tr>
</tbody>
</table>
**dot1x clear-statistics**

- **Syntax Description**: N/A
- **Default**: N/A
- **Configuration Mode**: Config
  - Config Interface Ethernet
- **History**: 3.4.2008
- **Role**: admin
- **Example**: `switch (config)# dot1x clear-statistics`
- **Related Commands**
- **Note**
**dot1x pae authenticator**

**Syntax**

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.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>Disabled</td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Config Interface Ethernet</td>
</tr>
<tr>
<td>History</td>
<td>3.4.2008</td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
</tr>
<tr>
<td>Example</td>
<td>switch (config interface ethernet 1/2)# dot1x system-auth-control</td>
</tr>
</tbody>
</table>

**Note**
**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.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>multi-host</th>
<th>Sets the interface to operate in a port-based mode</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>single-host</td>
<td>Sets the interface to operate in a MAC-based mode with support of a single supplicant per interface</td>
</tr>
</tbody>
</table>

**Default**

single-host

**Configuration Mode**

Config Interface Ethernet

**History**

3.4.2008

3.4.2300 Added “single-host” option

**Role**

admin

**Example**

```
switch (config interface ethernet 1/2)# dot1x host-mode single-host
```

**Related Commands**

**Note**
**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.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>auto</th>
<th>The authenticator uses PAE authentication services to allow or block the port traffic</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>force-authorized</td>
<td>Allows traffic on this port regardless of supplicant authorization</td>
</tr>
<tr>
<td></td>
<td>force-unauthorized</td>
<td>Blocks traffic on this port regardless of supplicant authorization</td>
</tr>
</tbody>
</table>

**Default**

Force-authorized

**Configuration Mode**

Config Interface Ethernet

**History**

3.4.2008

**Role**

admin

**Example**

```
switch (config interface ethernet 1/2)# dot1x port-control auto
```
**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.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>auth-port</td>
<td>Sets 802.1x RADIUS port to use with this server. Range: 1-65535.</td>
</tr>
<tr>
<td>enable</td>
<td>Sets 802.1x RADIUS as administratively enabled</td>
</tr>
<tr>
<td>key</td>
<td>Configures 802.1x global RADIUS shared secret for servers.</td>
</tr>
<tr>
<td>prompt-key</td>
<td>Prompts for key, rather than entering on command line</td>
</tr>
<tr>
<td>retransmit</td>
<td>Configure 802.1x global RADIUS retransmit count for servers. The time configured is in seconds. Range: 0-5.</td>
</tr>
<tr>
<td>timeout</td>
<td>Configures 802.1x global RADIUS timeout value for servers. The time configured is in seconds. Range: 1-60.</td>
</tr>
</tbody>
</table>

**Default**

- auth-port: 1812
- key: empty string
- retransmit: 1
- timeout: 3

**Configuration Mode**

Config

**History**

3.4.2008

**Role**

admin

**Example**

```
switch (config)# dot1x radius-server host 10.10.10.10 auth-port 65535 prompt-key enable
```

**Related Commands**

**Note**

- The no form of the various parameters resets them to their default values as indicated in the Default section above.
- It is possible to configure up to 5 RADIUS servers.
- It is possible to configure only 1 authentication port per RADIUS server IP.
**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.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>No re-authentication</td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Config Interface Ethernet</td>
</tr>
<tr>
<td>History</td>
<td>3.4.2008</td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
</tr>
<tr>
<td>Example</td>
<td>switch (config interface ethernet 1/2)# dot1x reauthenticate</td>
</tr>
</tbody>
</table>

**Related Commands**

**Note**
**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.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>Disabled</td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Config</td>
</tr>
<tr>
<td>History</td>
<td>3.4.2008</td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
</tr>
<tr>
<td>Example</td>
<td>switch (config)# dot1x system-auth-control</td>
</tr>
<tr>
<td>Related Commands</td>
<td></td>
</tr>
<tr>
<td>Note</td>
<td></td>
</tr>
</tbody>
</table>
**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.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
</table>

**Default**

3600 seconds

**Configuration Mode**

Config Interface Ethernet

**History**

3.4.2008

**Role**

admin

**Example**

```
switch (config interface ethernet 1/2)# dot1x timeout reauthentication 3600
```

**Related Commands**

Note

---

Mellanox Technologies Confidential
**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.

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td></td>
<td>60 seconds</td>
</tr>
<tr>
<td>Configuration Mode</td>
<td></td>
<td>Config Interface Ethernet</td>
</tr>
<tr>
<td>History</td>
<td></td>
<td>3.4.2008</td>
</tr>
<tr>
<td>Role</td>
<td></td>
<td>admin</td>
</tr>
<tr>
<td>Example</td>
<td></td>
<td>switch (config interface ethernet 1/2)# dot1x timeout quiet-period 60</td>
</tr>
</tbody>
</table>

**Note**
**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.

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>30 seconds</td>
<td></td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Config Interface Ethernet</td>
<td></td>
</tr>
<tr>
<td>History</td>
<td>3.4.2008</td>
<td></td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
<td></td>
</tr>
<tr>
<td>Example</td>
<td>switch (config interface ethernet 1/2)# dot1x timeout quiet-period 30</td>
<td></td>
</tr>
</tbody>
</table>

**Related Commands**

**Note**

**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.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>retries</td>
<td>The number of request retries. Range: 1-10.</td>
</tr>
</tbody>
</table>

**Default**

2

**Configuration Mode**

Config Interface Ethernet

**History**

3.4.2008

**Role**

admin

**Example**

`switch (config interface ethernet 1/2)# dot1x max-req 2`

**Related Commands**

**Note**
show dot1x

show dot1x

Displays 802.1x information on all interfaces.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>N/A</td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Any Command Mode</td>
</tr>
<tr>
<td>History</td>
<td>3.4.2008</td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
</tr>
</tbody>
</table>

Example

```
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           |
| ...            |          |               |                 |                |
```

Related Commands

Note
show dot1x interfaces ethernet

show dot1x interfaces ethernet <slot>/<port>

Displays 802.1x interface information.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>&lt;slot&gt;/&lt;port&gt;</th>
<th>Ethernet interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>N/A</td>
<td></td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Any Command Mode</td>
<td></td>
</tr>
<tr>
<td>History</td>
<td>3.4.2008</td>
<td></td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
<td></td>
</tr>
</tbody>
</table>

Example

```
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)#
```

Related Commands

Note
### show dot1x interfaces ethernet statistics

**Syntax**
```
show dot1x interfaces ethernet <slot>/<port> statistics
```

**Description**
Displays 802.1x interface information.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>&lt;slot&gt;/&lt;port&gt;</th>
<th>Ethernet interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>N/A</td>
<td></td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Any Command Mode</td>
<td></td>
</tr>
<tr>
<td>History</td>
<td>3.4.2008</td>
<td></td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
<td></td>
</tr>
</tbody>
</table>

**Example**
```
switch (config)# show dot1x interfaces ethernet 1/2 statistics

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
```

**Related Commands**

**Note**
**show dot1x radius**

**show dot1x radius**

Displays 802.1x RADIUS settings.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>N/A</td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Any Command Mode</td>
</tr>
<tr>
<td>History</td>
<td>3.4.2008</td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
</tr>
</tbody>
</table>

**Example**

```plaintext
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**
5.20 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 priority 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.

### 5.20.1 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.
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 5.21, “Shared Buffers,” on page 948 for more information on flow control.

5.20.2 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.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>force</th>
<th>Forces operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>PFC is disabled.</td>
<td></td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Config</td>
<td></td>
</tr>
<tr>
<td>History</td>
<td>3.1.0000</td>
<td></td>
</tr>
<tr>
<td></td>
<td>3.3.0000 Updated Example</td>
<td></td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
<td></td>
</tr>
</tbody>
</table>
Example

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 : 0 1 2 3 4 5 6 7
Priority Disabled List   : 0 1 2 3 4 5 6 7

<table>
<thead>
<tr>
<th>TC</th>
<th>Lossless</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>N</td>
</tr>
<tr>
<td>1</td>
<td>Y</td>
</tr>
<tr>
<td>2</td>
<td>Y</td>
</tr>
<tr>
<td>3</td>
<td>N</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Interface</th>
<th>PFC admin</th>
<th>PFC oper</th>
</tr>
</thead>
<tbody>
<tr>
<td>1/1</td>
<td>Disabled</td>
<td>Disabled</td>
</tr>
<tr>
<td>1/2</td>
<td>Disabled</td>
<td>Disabled</td>
</tr>
<tr>
<td>1/3</td>
<td>Disabled</td>
<td>Disabled</td>
</tr>
<tr>
<td>1/4</td>
<td>Disabled</td>
<td>Disabled</td>
</tr>
<tr>
<td>...</td>
<td>...</td>
<td>...</td>
</tr>
</tbody>
</table>

switch (config) #

Related Commands

show dcb priority-flow-control

Note

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**

```bash
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.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
<th>Default</th>
<th>Configuration Mode</th>
<th>History</th>
<th>Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>prio</td>
<td>0-7.</td>
<td>PFC is disabled for all priorities.</td>
<td>Config</td>
<td>3.1.0000</td>
<td>admin</td>
</tr>
</tbody>
</table>

**Example**

```bash
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
...

```

**Related Commands**

- `show dcb priority-flow-control`

**Note**
**dcb priority-flow-control mode on**

```
dcb priority-flow-control mode on [force]  
nodcb priority-flow-control mode
```

Enables PFC per interface.  
The no form of the command disables PFC per interface.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>force</th>
<th>Force command implementation.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td></td>
<td>PFC is disabled for all interfaces.</td>
</tr>
<tr>
<td>Configuration Mode</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Config Interface Ethernet</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Config Interface Port Channel</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Config Interface MLAG Port Channel</td>
<td></td>
<td></td>
</tr>
<tr>
<td>History</td>
<td>3.1.0000</td>
<td></td>
</tr>
<tr>
<td></td>
<td>3.3.4500</td>
<td>Added MLAG port-channel configuration mode</td>
</tr>
<tr>
<td>Role</td>
<td></td>
<td>admin</td>
</tr>
</tbody>
</table>
| Example            |       | 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

<table>
<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>

```
switch (config) #
```

**Related Commands**

`show dcb priority-flow-control`

**Note**
5.21 Shared Buffers

**show dcb priority-flow-control**

show dcb priority-flow-control [interface <type> <inf>] [detail]

Displays DCB priority flow control configuration and status.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
</table>
| type               | - ethernet  
                     - port-channel |
| inf                | The interface number. |
| detail             | Adds details information to the show output. |

<table>
<thead>
<tr>
<th>Default</th>
<th>N/A</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Configuration Mode</th>
<th>Any Command Mode</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>History</th>
<th>3.1.0000</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Role</th>
<th>admin</th>
</tr>
</thead>
</table>

**Example**

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

<table>
<thead>
<tr>
<th>TC</th>
<th>Lossless</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>N</td>
</tr>
<tr>
<td>1</td>
<td>Y</td>
</tr>
<tr>
<td>2</td>
<td>Y</td>
</tr>
<tr>
<td>3</td>
<td>N</td>
</tr>
</tbody>
</table>

<table>
<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>

**Related Commands**

<table>
<thead>
<tr>
<th>Note</th>
<th></th>
</tr>
</thead>
</table>

This section is relevant only for 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.

### 5.21.1 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 on which the packet is going to be transmitted

- **Priority**
  - Switch priority (SP) – internal identifier of the packet priority which is used as a key for several internal switch functions and decisions, specifically 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.
  - 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.

Buffers configuration mechanism is providing a way to allocate buffer space for specific traffic types based on the following classification parameters.

- iPort – traffic that arrived on a specific port
- iPort.PG – traffic that arrived on a specific port and mapped to a specific PG
- ePort – traffic that is going to be transmitted on a specific port
- ePort.TC – traffic that is going to be transmitted on a specific port and mapped to a specific TC

By default, multicast packets (including flooding and broadcast) are counted on the egress side. However, multicast packets consume the physical memory space of a single packet and, hence, using native buffering calculations, the multicast packet may negatively affect buffer utilization. Counting multicast traffic only once is not possible since, unlike unicast traffic where the TC is used as the region indicator of egress traffic, multicast traffic can be transmitted using different TCs on different ports. Therefore, instead of using TC as an egress region indicator, SP is used. Thus, the egress region for multicast traffic is named MC.SP. Hence the following classification parameters for multicast traffic are used.
• MC – traffic to be transmitted as multicast
• MC.SP – traffic to be transmitted as multicast on a specific SP

5.21.2 Buffering 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 (cannot be configured for {iPort}, {ePort}, or {MC})

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). When PG buffer occupancy reaches the threshold, the specific flow control packet is sent.

If there is a physical buffer space for an arriving packet, it is temporarily stored for processing. After processing its egress port, TC and ingress PG are defined. Then, it can be evaluated for eligibility for being stored in the buffer space until it is forwarded.

Buffer eligibility is defined based on the following conditions:

• There is available quota within at least one of the four reserved allocation regions

  • For lossy traffic: iPort.PG.usage < iPort.PG.reserved || iPort.usage < iPort.reserved || ePort.TC.usage < ePort.TC.reserved || ePort.usage < ePort.reserved
  • For lossless traffic: ePort.TC.usage < ePort.TC.reserved || ePort.usage < ePort.reserved

Note: Ingress check is not performed since all the ingress reserved space is allocated for headroom.

• If a packet is below the all aforementioned four shared allocation thresholds:
  iPort.PG.usage < iPort.PG.shared && iPort.usage < iPort.shared && ePort.TC.usage < ePort.TC.shared && ePort.usage < ePort.shared

If a packet is not eligible for buffering:

• For lossy traffic: Packet is dropped
• For lossless traffic: Packet stays in headroom
The eligible packet is counted in usage for the egress regions (ePort, ePort,tc or MC, MC,SP). A packet in lossy traffic is counted for usage in the ingress regions (iPort, iPort,PG). An eligible packet in lossless traffic is counted for usage in the ingress iPort region also, but if it is not eligible and stayed in the headroom, it is counted in its ingress region (iPort,PG) causing it to reach closer to the Xoff threshold.

5.21.3 Pools

Shared buffer space can be statically divided among multiple pools. Each region (iPort, ePort, MC, iPort,PG, ePort,TC and MC,SP) is mapped to specific pools. The pools are divided to ingress pools (iPools) and egress pools (ePools).

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.

  **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. It is configured in percentage out of the bounded pool size.

  - **Dynamic** – each region has a dynamic maximal threshold defined as alpha (α) which is the ratio between the current region usage and the pool’s free space (equal to the pool usage subtracted from pool size):

    - α accepts the following values: 0, 1/128, 1/64, …1/2,1,2,…,64, infinity

    - Buffer acceptance condition is: region usage < α*free pool space

The port region is counted against the pool that the PG/TC region of the packet is mapped to.

5.21.4 Default Configurations

5.21.4.1 Default Lossy Configuration

The default, out-of-box configuration provides the following settings:

- Pool allocation for ingress control and data packets

  - Each port has a reserved quota and in addition shared buffers
  - A single buffer (PG) per port for data packets
  - A single buffer (PG) per port for control packets – cannot be configured by the user

- Pool allocation for egress control and data packets

  - Each port has a (small) reserved quota and in addition shared buffers
  - 8 TC per port for data packets
• A single buffer per port for control packets – cannot be configured by the user
• Pool allocation for egress CPU traffic
  • Each TC has a reserved quota and in addition shared buffers
• Only iPort.PG and ePort.TC enforcement is used, not iPort and ePort enforcement

All the switch-priorities are mapped to ingress PG 0. Each switch-priority \( i \) is mapped into a corresponding traffic class \( i \).

5.21.4.2 Default Lossless Configuration

One can switch from lossy to lossless defaults by disabling/enabling global flow control.

The lossless buffer allocation is identical to the lossy default allocation with different shared buffer dynamic thresholds and with an addition of flow control thresholds.

The default Xon and Xoff thresholds are both set to 17KB. The reserved buffer is set to 90KB. It allows having a 100 meter lossless link working at 100GbE, supporting 9KB MTU packets.

5.21.5 Configuration Example

The following example exhibits how to divide the buffer among traffic priorities. Assuming that over an out-of-box lossy default configuration is set, the user here configures buffering configuration for lossless traffic classified to switch-priority 3.

The changes on the default configuration are summarized in the following:

• Ingress:
  • Default reserved PG buffer is reduced from 90KB to 20KB, freeing 70KB for lossless traffic

• Egress:
  • TC3 shared \( \alpha \) is configured to infinite, as recommended for TCs with lossless traffic.

Example:

```bash
// Setting PFC on priority 3
switch (config) # dcb priority-flow-control enable force
switch (config) # dcb priority-flow-control priority 3 enable
switch (config) # interface ethernet <id> dcb priority-flow-control mode on force

// Reducing default PG size
switch (config)# interface ethernet <id> ingress-buffer iPort.pg0 map pool ipool0 type lossy reserved 20K shared alpha 8
switch (config)# interface ethernet <id> ingress-buffer iPort.pg3 map pool ipool0 type lossless reserved 70K xoff 17K xon 17K shared alpha 2
switch (config)# interface ethernet <id> egress-buffer ePort.tc3 map pool ePool0 reserved 4K shared alpha inf

// Mapping switch priority 3 to lossless ingress PG buffer
(config)# interface ethernet <id> ingress-buffer iPort.pg3 bind switch-priority 3
```

If the user wants to allocate a separate pool for the new lossless traffic. The changes needed are as follows:
• Ingress:
  - Default reserved PG buffer is reduced from 90KB to 20KB, freeing up more than 70KB for lossless traffic
  - Default pool is reduced from 7960K to 3000K. The rest is allocated to the new pool.

• Egress:
  - TC3 shared alpha is configured to infinite as recommended for TCs with lossless traffic. Default pool is reduced from 14232KB to 4888K. The rest is allocated to the new pool.

Example:

```bash
// Setting PFC on priority 3
switch (config)# dcb priority-flow-control enable force
switch (config)# dcb priority-flow-control priority 3 enable
switch (config)# interface ethernet <id> dcb priority-flow-control mode on force

// Reducing default PG size
switch (config)# interface ethernet <id> ingress-buffer iPort.pg0 map pool ipool0 type lossy reserved 20K shared alpha 8

// Setting separate pool for lossless traffic
// Reducing data pool
switch (config)# pool ipool0 direction ingress size 3000 type dynamic
switch (config)# pool ePool0 direction egress size 4888 type dynamic

// Defining lossless pool #1
switch (config)# pool ipool1 direction ingress size 7768 type dynamic
switch (config)# pool ePool1 direction egress size 7768 type dynamic

// Setting lossless ingress buffer PG3 and lossless egress TC3
// Setting ipool1 for infinite alpha
switch (config)# interface ethernet <id> ingress-buffer iPort.pg3 map pool ipool1 type lossless reserved 70K xoff 17K xon 17K shared alpha 2
switch (config)# interface ethernet <id> ingress-buffer iPort.pool ipool1 reserved 0K shared alpha inf
switch (config)# interface ethernet <id> egress-buffer ePort.tc3 map pool epool1 reserved 4K shared alpha inf

// Mapping switch priority 3 to lossless ingress PG buffer
switch (config)# interface ethernet <id> ingress-buffer iport.pg3 bind switch-priority 3
```

When the egress traffic class (TC) region buffer size exceeds the TX α (max) threshold, the non-eligible packet is dropped (does not stay in the headroom) regardless whether it belongs to a lossy or lossless ingress buffer. Therefore, the recommendation is to map lossless traffic to separate TCs than lossy traffic and to configure egress α (max) threshold of these TCs to infinity in order to avoid dropping lossless traffic.
### 5.21.6 Commands

**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.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>buffer-name</th>
<th>Name of ingress buffer</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>N/A</td>
<td></td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Config Interface Ethernet</td>
<td></td>
</tr>
<tr>
<td>History</td>
<td>3.6.1002</td>
<td></td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
<td></td>
</tr>
<tr>
<td>Example</td>
<td><code>switch (config interface ethernet 1/1)# ingress-buffer iPort.pg1</code> <code>switch (config interface ethernet 1/1 ingress-buffer iPort.pg1)#</code></td>
<td></td>
</tr>
</tbody>
</table>

**Related Commands**

**Note**

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.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>buffer-name</th>
<th>Name of egress buffer</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>N/A</td>
<td></td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Config Interface Ethernet</td>
<td></td>
</tr>
<tr>
<td>History</td>
<td>3.6.1002</td>
<td></td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
<td></td>
</tr>
</tbody>
</table>
| Example            | switch (config interface ethernet 1/1)# egress-buffer ePort.tc4  
switch (config interface ethernet 1/1 egress-buffer ePort.tc4)# | |
| Related Commands   |             |                       |
| Note               | ePort.tc16 is reserved for control traffic and hence cannot be edited | |
pool reserved

pool <pool-name> reserved <reserved> shared {alpha | max} <shared>
no pool <pool-name>

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

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>pool-name Possible values: iPool0, iPool1, iPool2, iPool3</th>
</tr>
</thead>
<tbody>
<tr>
<td>reserved</td>
<td>Amount of reserved memory for the buffer in bytes</td>
</tr>
<tr>
<td>shared</td>
<td>The amount of shared memory for this buffer</td>
</tr>
<tr>
<td></td>
<td>• When working in alpha mode, alpha can have the values 0, 1/128, 1/64 … 1, 2, 4, … 64, inf</td>
</tr>
<tr>
<td></td>
<td>• When working in max mode, the shared size is defined as a percentage from the pool size</td>
</tr>
</tbody>
</table>

Default According to system default OOB configuration

Configuration Mode
- Config Interface Ethernet Egress Buffer
- Config Interface Ethernet Ingress Buffer

History 3.6.1002

Role admin

Example
  switch (config interface ethernet 1/1 ingress-buffer iPort)# pool iPool0 reserved 90K shared alpha 1/8

Related Commands

Note
**map pool**

```
map pool <pool-name> type <type> reserved <reserved> [xoff <xoff> xon [<xon>]
shared {alpha | max} <shared>
```

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

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>pool-name</td>
<td>Possible values: iP00l0, iP00l1, iP00l2, iP00l3</td>
</tr>
<tr>
<td>reserved</td>
<td>Amount of reserved memory for the buffer in bytes</td>
</tr>
<tr>
<td>xoff</td>
<td>Relevant only on lossless type, Xoff threshold in bytes</td>
</tr>
<tr>
<td>xon</td>
<td>Relevant only on lossless type, Xon threshold in bytes</td>
</tr>
<tr>
<td>shared</td>
<td>The amount of shared memory for this buffer</td>
</tr>
<tr>
<td></td>
<td>• When working in alpha mode, alpha can have the values 0, 1/128, 1/64 … 1, 2, 4, … 64, inf</td>
</tr>
<tr>
<td></td>
<td>• When working in max mode, the shared size is defined as a percentage from the pool size</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Default</th>
<th>According to system default OOB configuration</th>
</tr>
</thead>
</table>

**Configuration Mode**

Config Interface Ethernet Egress Buffer  
Config Interface Ethernet Ingress Buffer

**History**

3.6.1002

**Role**

admin

**Example**

```
switch (config interface ethernet 1/1 ingress-buffer iPort.pg0)# map pool
iPool0 type lossless reserved 90K xoff 17K xon 17K shared alpha 1/8
```

**Related Commands**

**Note**
**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.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>list-of-switch-priorities Possible values: 0-7</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>According to system default OOB configuration</td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Config Interface Ethernet Egress Buffer Config Interface Ethernet Ingress Buffer</td>
</tr>
<tr>
<td>History</td>
<td>3.6.1002</td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
</tr>
<tr>
<td>Example</td>
<td>switch (config interface ethernet 1/1 ingress-buffer iPort.pgl)# bind switch-priority 0 1</td>
</tr>
</tbody>
</table>

**Related Commands**

**Note**
**description**

`description <description>`

Configures buffer description. The no form of the command resets the values to their default.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
<th>Text string</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td><code>&quot;&quot;</code></td>
<td></td>
</tr>
</tbody>
</table>
| Configuration Mode | Config Interface Ethernet Egress Buffer  
                    | Config Interface Ethernet Ingress Buffer |
| History            | 3.6.1002    |             |
| Role               | admin       |             |
| Example            | switch (config interface ethernet 1/1 ingress-buffer iPort.pgl)#
                    | description example |

**Note**
pool direction

pool <pool-name> direction <direction> size <size> type <type>

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

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>pool</th>
<th>Possible values: iPool0, iPool1, iPool2, iPool3</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>direction</td>
<td>Ingress or egress traffic</td>
</tr>
<tr>
<td></td>
<td>size</td>
<td>Size of pool in bytes</td>
</tr>
<tr>
<td></td>
<td>type</td>
<td>Static or dynamic</td>
</tr>
</tbody>
</table>

| Default             | N/A                         |

<table>
<thead>
<tr>
<th>Configuration Mode</th>
<th>Config Interface Ethernet Egress Buffer</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Config Interface Ethernet Ingress Buffer</td>
</tr>
</tbody>
</table>

| History             | 3.6.1002                        |

| Role                | admin                            |

| Example             | switch (config interface ethernet 1/1 ingress-buffer iPort.pg1)# pool iPool1 direction ingress size 1M type dynamic |

| Related Commands    |                                |

| Note                |                                |
### pool mc-buffer

```
pool <pool-name> mc-buffer <buffer> reserved <reserved> shared {alpha | max}
no pool <pool-name>
```

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

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>mc-buffer</th>
<th>Buffer can have the values mc.sp0, mc.sp1…mc.sp14</th>
</tr>
</thead>
<tbody>
<tr>
<td>reserved</td>
<td>reserved</td>
<td>The amount of shared memory for this buffer</td>
</tr>
<tr>
<td>shared</td>
<td>shared</td>
<td>The amount of shared memory for this buffer</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• When working in alpha mode, alpha can have the values 0, 1/128, 1/64 … 1, 2, 4, … 64, inf</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• When working in max mode, the shared size is defined as a percentage from the pool size</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Default</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuration Mode</td>
<td>Config Interface Ethernet Egress Buffer</td>
</tr>
<tr>
<td>History</td>
<td>3.6.1002</td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
</tr>
<tr>
<td>Example</td>
<td>switch (config interface ethernet 1/1 egress-buffer ePort.tc4)# pool iPooll mc-buffer mx.sp0 reserved 90K shared alpha 1/8</td>
</tr>
</tbody>
</table>

**Related Commands**

**Note**
pool description

pool <pool-name> description <description>
no pool <pool-name>

Configures the buffer description of a specific pool-name.
The no form of the command resets the values to their default.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>description</th>
<th>String text</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>&quot;&quot;</td>
<td></td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Config Interface Ethernet Egress Buffer &lt;description&gt; Config Interface Ethernet Ingress Buffer</td>
<td></td>
</tr>
<tr>
<td>History</td>
<td>3.6.1002</td>
<td></td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
<td></td>
</tr>
<tr>
<td>Example</td>
<td>switch (config interface ethernet 1/1 ingress-buffer iPort.pgl)# pool iPooll description myDescription</td>
<td></td>
</tr>
</tbody>
</table>

Related Commands

Note
**show buffers status**

**show buffers status interfaces ethernet <slot>/<port>**

Displays buffer status

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>&lt;slot&gt;/&lt;port&gt;</th>
<th>Ethernet interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>N/A</td>
<td></td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Config</td>
<td></td>
</tr>
<tr>
<td>History</td>
<td>3.6.1002</td>
<td></td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
<td></td>
</tr>
</tbody>
</table>

**Example**

```
switch (config)# show buffers status 1/25

<table>
<thead>
<tr>
<th>Interface</th>
<th>Buffer</th>
<th>Resv</th>
<th>Shared</th>
<th>Usage</th>
<th>MaxUsage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Eth1/25</td>
<td>iPort</td>
<td>192</td>
<td>1/128</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>iPort</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>iPort</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>iPort</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>iPort.pg0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>iPort.pg1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>iPort.pg2</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>iPort.pg3</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>iPort.pg4</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>iPort.pg5</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>iPort.pg6</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>iPort.pg7</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>iPort.pg9</td>
<td>19.5K</td>
<td>inf</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>ePort</td>
<td>0</td>
<td>inf</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>ePort</td>
<td>0</td>
<td>inf</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>ePort</td>
<td>0</td>
<td>inf</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>ePort</td>
<td>0</td>
<td>inf</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>ePort.tc0</td>
<td>1.5K</td>
<td>2</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>ePort.tc1</td>
<td>1.5K</td>
<td>2</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>ePort.tc2</td>
<td>1.5K</td>
<td>2</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>ePort.tc3</td>
<td>1.5K</td>
<td>2</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>ePort.tc4</td>
<td>1.5K</td>
<td>2</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>ePort.tc5</td>
<td>1.5K</td>
<td>2</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>ePort.tc6</td>
<td>1.5K</td>
<td>2</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>ePort.tc7</td>
<td>1.5K</td>
<td>2</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>ePort.tc8</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>ePort.tc9</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>ePort.tc10</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>ePort.tc11</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>ePort.tc12</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>ePort.tc13</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>ePort.tc14</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>ePort.tc15</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>ePort.tc16</td>
<td>96</td>
<td>inf</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>
```
Related Commands

Note
show buffers details

show buffers details interfaces ethernet <slot>/<port>

Displays buffer status in details.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>&lt;slot&gt;/&lt;port&gt;</th>
<th>Ethernet interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>N/A</td>
<td></td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Config</td>
<td></td>
</tr>
<tr>
<td>History</td>
<td>3.6.1002</td>
<td></td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
<td></td>
</tr>
</tbody>
</table>
Example

```
Example
```

```
switch (config)# show buffers details interfaces ethernet 1/25
Flags: Y - Lossy, L - Lossless
S - Static, D - Dynamic
Shared size is in Bytes for static pool and in alphas for dynamic pool.
```

<table>
<thead>
<tr>
<th>Buffer</th>
<th>Resv [Byte]</th>
<th>Xoff [Byte]</th>
<th>Xon [%/a]</th>
<th>Shared</th>
<th>Pool</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>iPort(Y)</td>
<td>192</td>
<td>-</td>
<td>-</td>
<td>1/128</td>
<td>iPool0(D)</td>
<td></td>
</tr>
<tr>
<td>iPort(Y)</td>
<td>0</td>
<td>-</td>
<td>-</td>
<td>0</td>
<td>iPool1(D)</td>
<td></td>
</tr>
<tr>
<td>iPort(Y)</td>
<td>0</td>
<td>-</td>
<td>-</td>
<td>0</td>
<td>iPool2(D)</td>
<td></td>
</tr>
<tr>
<td>iPort(Y)</td>
<td>0</td>
<td>-</td>
<td>-</td>
<td>0</td>
<td>iPool3(D)</td>
<td></td>
</tr>
<tr>
<td>iPort.pg0(Y)</td>
<td>0</td>
<td>-</td>
<td>-</td>
<td>0</td>
<td>iPool0(D) Data</td>
<td></td>
</tr>
<tr>
<td>iPort.pg1(Y)</td>
<td>0</td>
<td>-</td>
<td>-</td>
<td>0</td>
<td>iPool0(D)</td>
<td></td>
</tr>
<tr>
<td>iPort.pg2(Y)</td>
<td>0</td>
<td>-</td>
<td>-</td>
<td>0</td>
<td>iPool0(D)</td>
<td></td>
</tr>
<tr>
<td>iPort.pg9(Y)</td>
<td>19.5K</td>
<td>-</td>
<td>-</td>
<td>inf</td>
<td>iPool0(D) Control</td>
<td></td>
</tr>
<tr>
<td>ePort</td>
<td>0</td>
<td>-</td>
<td>-</td>
<td>inf</td>
<td>ePool0(D)</td>
<td></td>
</tr>
<tr>
<td>ePort</td>
<td>0</td>
<td>-</td>
<td>-</td>
<td>inf</td>
<td>ePool1(D)</td>
<td></td>
</tr>
<tr>
<td>ePort</td>
<td>0</td>
<td>-</td>
<td>-</td>
<td>inf</td>
<td>ePool2(D)</td>
<td></td>
</tr>
<tr>
<td>ePort</td>
<td>0</td>
<td>-</td>
<td>-</td>
<td>inf</td>
<td>ePool3(D)</td>
<td></td>
</tr>
<tr>
<td>ePort.tc0</td>
<td>1.5K</td>
<td>-</td>
<td>-</td>
<td>2</td>
<td>ePool0(D)</td>
<td></td>
</tr>
<tr>
<td>ePort.tc1</td>
<td>1.5K</td>
<td>-</td>
<td>-</td>
<td>2</td>
<td>ePool0(D)</td>
<td></td>
</tr>
<tr>
<td>ePort.tc2</td>
<td>1.5K</td>
<td>-</td>
<td>-</td>
<td>2</td>
<td>ePool0(D)</td>
<td></td>
</tr>
<tr>
<td>ePort.tc6</td>
<td>1.5K</td>
<td>-</td>
<td>-</td>
<td>2</td>
<td>ePool0(D)</td>
<td></td>
</tr>
<tr>
<td>ePort.tc7</td>
<td>1.5K</td>
<td>-</td>
<td>-</td>
<td>2</td>
<td>ePool0(D)</td>
<td></td>
</tr>
<tr>
<td>ePort.tc8</td>
<td>0</td>
<td>-</td>
<td>-</td>
<td>0</td>
<td>ePool0(D)</td>
<td></td>
</tr>
<tr>
<td>ePort.tc9</td>
<td>0</td>
<td>-</td>
<td>-</td>
<td>0</td>
<td>ePool0(D)</td>
<td></td>
</tr>
<tr>
<td>ePort.tc15</td>
<td>0</td>
<td>-</td>
<td>-</td>
<td>0</td>
<td>ePool0(D)</td>
<td></td>
</tr>
<tr>
<td>ePort.tc16</td>
<td>96</td>
<td>-</td>
<td>-</td>
<td>inf</td>
<td>ePool0(D) Control</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Switch-priority</th>
<th>Buffer</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>iPort.pg0</td>
</tr>
<tr>
<td>1</td>
<td>iPort.pg0</td>
</tr>
<tr>
<td>2</td>
<td>iPort.pg0</td>
</tr>
<tr>
<td>3</td>
<td>iPort.pg0</td>
</tr>
<tr>
<td>4</td>
<td>iPort.pg0</td>
</tr>
<tr>
<td>...</td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>iPort.pg0</td>
</tr>
<tr>
<td>11</td>
<td>iPort.pg0</td>
</tr>
<tr>
<td>12</td>
<td>iPort.pg0</td>
</tr>
<tr>
<td>13</td>
<td>iPort.pg0</td>
</tr>
<tr>
<td>14</td>
<td>iPort.pg0</td>
</tr>
</tbody>
</table>

Related Commands

Note
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

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:

```bash
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”.

```bash
switch (config)# show interface ethernet 1/1 status
```

<table>
<thead>
<tr>
<th>Port</th>
<th>Operational state</th>
<th>Speed</th>
<th>Negotiation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Eth1/1</td>
<td>Up</td>
<td>40 Gbps</td>
<td>No-Negotiation</td>
</tr>
</tbody>
</table>

Step 4. Create a VLAN interface that matches the VLAN. Run:

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

Step 5. Configure an IP address and a network mask to the interface. Run:

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

Step 6. Verify VLAN interface configuration. Run:

```bash
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:

```bash
switch (config)# interface loopback 2
switch (config interface loopback 2)#
```

Step 2. Configure an IP address on the loopback interface. Run:

```bash
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 a 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
```
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 32, 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 32: ECMP](image)

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:

<table>
<thead>
<tr>
<th>Rx</th>
</tr>
</thead>
<tbody>
<tr>
<td>packets</td>
</tr>
<tr>
<td>0</td>
</tr>
<tr>
<td>unicast packets</td>
</tr>
<tr>
<td>0</td>
</tr>
<tr>
<td>multicast packets</td>
</tr>
<tr>
<td>0</td>
</tr>
<tr>
<td>broadcast packets</td>
</tr>
<tr>
<td>0</td>
</tr>
<tr>
<td>bytes</td>
</tr>
<tr>
<td>0</td>
</tr>
<tr>
<td>error packets</td>
</tr>
<tr>
<td>0</td>
</tr>
<tr>
<td>discard packets</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Tx</th>
</tr>
</thead>
<tbody>
<tr>
<td>packets</td>
</tr>
<tr>
<td>0</td>
</tr>
<tr>
<td>unicast packets</td>
</tr>
<tr>
<td>0</td>
</tr>
<tr>
<td>multicast packets</td>
</tr>
<tr>
<td>0</td>
</tr>
<tr>
<td>broadcast packets</td>
</tr>
<tr>
<td>0</td>
</tr>
<tr>
<td>bytes</td>
</tr>
<tr>
<td>0</td>
</tr>
<tr>
<td>discard packets</td>
</tr>
<tr>
<td>0</td>
</tr>
</tbody>
</table>
• 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 33: Multiple Hash Functions
6.1.3 Virtual Routing and Forwarding

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.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>If operating with Ethernet system profile: L3</td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Config</td>
</tr>
<tr>
<td>History</td>
<td>3.4.1802</td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
</tr>
</tbody>
</table>
| Example            | switch (config) # ip l3 force
|                    | switch (config) # |
| Related Commands   | N/A |
| Note               | N/A |
**vrf definition**

```
vrf definition <vrf-name>
```

Creates the VRF.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>vrf-name</th>
<th>VRF session name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>N/A</td>
<td></td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Config</td>
<td></td>
</tr>
<tr>
<td>History</td>
<td>3.4.2008</td>
<td></td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
<td></td>
</tr>
</tbody>
</table>

**Example**

```bash
switch (config) # vrf definition my-vrf
switch (config vrf definition my-vrf) #
```

**Related Commands**

N/A

**Notes**

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.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vrf-name</td>
<td>VRF session name</td>
</tr>
</tbody>
</table>

Default: N/A

Configuration Mode: Config

History: 3.4.2008

Role: admin

Example:

```
switch (config) # routing-context vrf my-vrf
switch (config) #
```

Related Commands: N/A

Notes:
- 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.
- If no routing-context is configured and the user does not specify the VRF name, default VRF is used.
**ip routing**

```
ip routing [vrf <vrf-name>]  
```

Enables L3 forwarding between high speed interfaces.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>vrf-name</th>
<th>VRF session name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>N/A</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Configuration Mode</th>
<th>Config</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>History</td>
<td>3.4.1802</td>
<td></td>
</tr>
<tr>
<td></td>
<td>3.4.2008</td>
<td>Added VRF parameter</td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
<td></td>
</tr>
</tbody>
</table>

**Example**

```
switch (config) # ip routing vrf my-vrf
switch (config) #
```

<table>
<thead>
<tr>
<th>Related Commands</th>
<th>N/A</th>
<th></th>
</tr>
</thead>
</table>

**Notes**

- RD must be configured to enable IP routing on the VRF
- If no routing-context is specified, the “routing-context” VRF is automatically configured.
**description**

```
description <description>
no description force
```

Creates the VRF.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>description</th>
<th>Text string</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>force</td>
<td>Forces deletion (no confirmation needed if configuration exists inside the VRF)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Default</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuration Mode</td>
<td>Config VRF Definition</td>
</tr>
<tr>
<td>History</td>
<td>3.4.2008</td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
</tr>
</tbody>
</table>
| Example | switch (config vrf definition my-vrf) # description vrf-description
switch (config vrf definition my-vrf) # |
| Related Commands | N/A |
| Notes | N/A |
### 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.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>ip-addr</th>
<th>IPv4 address</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>AS Number</td>
<td>Asynchronous machine number</td>
</tr>
<tr>
<td>Default</td>
<td>N/A</td>
<td></td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Config VRF Definition</td>
<td></td>
</tr>
<tr>
<td>History</td>
<td>3.4.2008</td>
<td></td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
<td></td>
</tr>
</tbody>
</table>
| Example            | switch (config vrf definition my-vrf) # rd 10.10.10.10:2  
                    | switch (config vrf definition my-vrf) # |
| Related Commands   | N/A      |
| Notes              | • 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.  
                    • An RD must be defined to enable IP routing on the VRF |
# vrf forwarding

**vrf forwarding <vrf-name>**

Maps an interface to VRF.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>vrf-name</th>
<th>VRF session name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>N/A</td>
<td></td>
</tr>
</tbody>
</table>
| Configuration Mode | Config Interface Ethernet set as router port interface  
                     Config Interface VLAN  
                     Config Interface Loopback |
| History            | 3.4.2008 |                  |
| Role               | admin    |                  |
| Example            | switch (config interface ethernet 1/2) # vrf forwarding my-vrf  
                     switch (config interface ethernet 1/2) # |
| Related Commands   | N/A      |                  |
| Notes              |          |                  |
show ip routing

show ip routing [vrf <vrf-name> | all]

Displays IP routing information per VRF.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>vrf</th>
<th>Displays information for specific VRF</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>all</td>
<td>Displays information on all VRFs</td>
</tr>
</tbody>
</table>

**Default**

N/A

**Configuration Mode**

Any Command Mode

**History**

3.2.0230

3.4.2008 Added VRF parameter

**Role**

admin

**Example**

switch (config) # show ip routing vrf all

VRF Name: my-vrf
---------------------------
IP routing: disabled

VRF Name: default
---------------------------
IP routing: enabled
switch (config) #

**Related Commands**

N/A

**Notes**

If no routing-context is specified, the “routing-context” VRF is automatically displayed.
show routing-context vrf

Displays VRF active context.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>N/A</td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Any Command Mode</td>
</tr>
<tr>
<td>History</td>
<td>3.4.2008</td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
</tr>
</tbody>
</table>
| Example            | switch (config) # show routing-context vrf
                     VRF active context: my-vrf
                     switch (config) # |
| Related Commands   | N/A |
| Notes              |     |
## show vrf

```
show vrf [<vrf-name> | all]
```

Displays VRF information.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>all</th>
<th>Displays information for all VRF instances</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>vrf-name</td>
<td>Name of VRF instance</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Default</th>
<th>N/A</th>
</tr>
</thead>
</table>

**Configuration Mode**

Any Command Mode

**History**

3.4.2008

**Role**

admin

**Example**

```
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) #
```

**Related Commands**

N/A

**Notes**

If no routing-context is specified, the “routing-context” VRF is automatically displayed.
### switchport

**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.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>force</th>
<th>Forces configuration even if the interface’s admin state is enabled.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>N/A</td>
<td></td>
</tr>
</tbody>
</table>
| Configuration Mode | Config Interface Ethernet  
                    | Config Interface Port Channel                                    |
| History            | 3.3.5200 |                                                                    |
| Role               | admin  |                                                                     |
| Example            | `switch (config interface ethernet 1/10)# no switchport force`     |

**Related Commands**

**Note**
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.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan-id</td>
<td>Enables L2 802.1Q encapsulation of traffic on a router port interface in a VLAN</td>
</tr>
<tr>
<td>force</td>
<td>Forces admin state down</td>
</tr>
</tbody>
</table>

| Default            | N/A          |
| Configuration Mode | Config Interface Ethernet |
| History            | 3.3.5200     |
| Role               | admin        |

Example

```
switch (config interface ethernet 1/10)# encapsulation dot1q vlan 10
```

Related Commands

Note
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.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan-id</td>
<td>A numeric range of 1-4094</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Default</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuration Mode</td>
<td>Config</td>
</tr>
<tr>
<td>History</td>
<td>3.2.0230</td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
</tr>
</tbody>
</table>

Example

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

Related Commands

- ip routing
- vlan <vlan-id>
- switchport mode
- switchport access
- show interfaces vlan

Note

- Make sure the VLAN was created, using the command “vlan <vlan-id>” in the global configuration mode
- The VLAN must be assigned to one of the L2 interfaces. To do so, run the command “switchport ...”
- At least one interface belong to that VLAN must be in UP state
### ip address

**Syntax**

```plaintext
ip address <ip-address> <mask>
no ip address <ip-address> <mask>
```

Enters user-defined description for the interface.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip-address</td>
<td>IPv4 address</td>
</tr>
<tr>
<td>mask</td>
<td>There are two possible ways to the mask:</td>
</tr>
<tr>
<td></td>
<td>• /length (i.e. /24)</td>
</tr>
<tr>
<td></td>
<td>• Network address (i.e. 255.255.255.0)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Default</th>
<th>0.0.0.0/0</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuration Mode</td>
<td>Config Interface VLAN</td>
</tr>
<tr>
<td>History</td>
<td>3.2.0230</td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
</tr>
</tbody>
</table>
| Example            | switch (config interface vlan 10) # ip address 10.10.10.10 /24  
switch (config interface vlan 10) # |
| Related Commands   | interface vlan  
show interfaces vlan |

**Note**
### ip address dhcp

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>Disabled</td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Config Interface VLAN</td>
</tr>
<tr>
<td>History</td>
<td>3.4.2008</td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
</tr>
</tbody>
</table>

#### Example

```bash
switch (config interface vlan 10) # ip address dhcp
switch (config interface vlan 10) #
```

#### Related Commands

- interface vlan
- show interfaces vlan

#### Note
counters

counters
no counters

Enables counters on the IP interface.
The no form of the command disables counters gathering on the IP interface.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>counters are disabled.</td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Config Interface VLAN</td>
</tr>
<tr>
<td>History</td>
<td>3.2.0230</td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
</tr>
</tbody>
</table>
| Example            | switch (config interface vlan 10) # counters
switch (config interface vlan 10) # |
| Related Commands   | counters
interface vlan
show interfaces vlan |
| Note               | • Enabling counters for the router interface adds delay to the traffic stream
• There are maximum of 16 counter sets |
**description**

```
description <string>
no description
```

Enters a description for the interface.
The no form of the command sets the description to default.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
<th>User defined string</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>&quot;&quot;</td>
<td></td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Config Interface VLAN</td>
<td></td>
</tr>
<tr>
<td>History</td>
<td>3.2.0230</td>
<td></td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
<td></td>
</tr>
</tbody>
</table>
| Example            | switch (config interface vlan 10) # description my-ip-interface  
switch (config interface vlan 10) #                   |
| Related Commands   | interface vlan       |                     |
|                    | show interfaces vlan |                     |
| Note               |                      |                     |
mtu

```
mtu <size> [force]
no mtu
```

Sets the MTU for the interface. The no form of the command sets the MTU to default.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>size</td>
<td>1500-9216.</td>
</tr>
<tr>
<td>force</td>
<td>Forces command implementation.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Default</th>
<th>1522</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuration Mode</td>
<td>Config Interface VLAN</td>
</tr>
<tr>
<td>History</td>
<td>3.2.0230</td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
</tr>
</tbody>
</table>

**Example**

```
switch (config interface vlan 10)# mtu 9216
switch (config interface vlan 10)#
```

**Related Commands**

- interface vlan
- show interfaces vlan

**Note**
## shutdown

**shutdown**

**no shutdown**

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

### Syntax Description

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>N/A</th>
</tr>
</thead>
</table>

### Default

The interface is enabled.

<table>
<thead>
<tr>
<th>Configuration Mode</th>
<th>Config Interface VLAN</th>
</tr>
</thead>
</table>

### History

3.1.0000

### Role

admin

### Example

```
switch (config interface vlan 20) # shutdown
switch (config interface vlan 20) #
```

### Related Commands

interface vlan

### Note
clear counters

clear counters

Clears the interface counters.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>N/A</td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Config Interface VLAN</td>
</tr>
<tr>
<td>History</td>
<td>3.2.0230</td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
</tr>
</tbody>
</table>

Example

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

Related Commands

interface vlan counters

Note
ip icmp redirect

No ip icmp redirect

Enables ICMP redirect.
The no form of the command disables ICMP redirect.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>Enabled</td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Config Interface VLAN</td>
</tr>
<tr>
<td>History</td>
<td>3.4.0010</td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
</tr>
<tr>
<td>Example</td>
<td>switch (config interface vlan 10) # no ip icmp redirect</td>
</tr>
<tr>
<td>Related Commands</td>
<td>interface vlan counters</td>
</tr>
<tr>
<td>Note</td>
<td>• ICMP redirect transmits messages to hosts alerting them about the existence of more efficient routes to a specific destination</td>
</tr>
</tbody>
</table>
### show ip interface

**show ip interface [vrf <vrf-name> | all] [brief]**

Displays IP interfaces information per VRF.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>all</td>
<td>Displays information on all VRFs</td>
</tr>
<tr>
<td>brief</td>
<td>Displays IP interfaces information in a shortened form</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Default</th>
<th>N/A</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Configuration Mode</th>
<th>Any Command Mode</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>History</th>
<th>3.4.2008</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Role</th>
<th>admin</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>switch (config) # show ip interface vrf all brief</td>
</tr>
</tbody>
</table>

```
<table>
<thead>
<tr>
<th>Interface</th>
<th>Address/Mask</th>
<th>Admin-state</th>
<th>Oper-state</th>
<th>MTU</th>
<th>VRF</th>
</tr>
</thead>
<tbody>
<tr>
<td>mgmt0</td>
<td>10.224.22.27/24</td>
<td>Enabled</td>
<td>Up</td>
<td>1500</td>
<td>default</td>
</tr>
<tr>
<td>mgmt1</td>
<td>0.0.0.0/0</td>
<td>Enabled</td>
<td>Down</td>
<td>1500</td>
<td>default</td>
</tr>
<tr>
<td>Vlan 20</td>
<td>20.20.20.1/24</td>
<td>Enabled</td>
<td>Down</td>
<td>1500</td>
<td>my-vrf</td>
</tr>
<tr>
<td>Eth1/1</td>
<td>1.1.1.1/24</td>
<td>Enabled</td>
<td>Down</td>
<td>1500</td>
<td>my-vrf</td>
</tr>
<tr>
<td>Loopback 10</td>
<td>10.10.10.1/32</td>
<td>Enabled</td>
<td>Up</td>
<td>1500</td>
<td>my-vrf</td>
</tr>
<tr>
<td>Vlan 30</td>
<td>30.30.30.1/24</td>
<td>Enabled</td>
<td>Down</td>
<td>1500</td>
<td>default</td>
</tr>
<tr>
<td>Eth1/2</td>
<td>2.2.2.2/24</td>
<td>Enabled</td>
<td>Down</td>
<td>1500</td>
<td>default</td>
</tr>
<tr>
<td>Loopback 11</td>
<td>11.11.11.1/32</td>
<td>Enabled</td>
<td>Up</td>
<td>1500</td>
<td>default</td>
</tr>
</tbody>
</table>
```

```
switch (config) # show ip interface vrf my-vrf brief
```

```
<table>
<thead>
<tr>
<th>Interface</th>
<th>Address/Mask</th>
<th>Admin-state</th>
<th>Oper-state</th>
<th>MTU</th>
<th>VRF</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vlan 20</td>
<td>20.20.20.1/24</td>
<td>Enabled</td>
<td>Down</td>
<td>1500</td>
<td>my-vrf</td>
</tr>
<tr>
<td>Eth1/1</td>
<td>1.1.1.1/24</td>
<td>Enabled</td>
<td>Down</td>
<td>1500</td>
<td>my-vrf</td>
</tr>
<tr>
<td>Loopback 10</td>
<td>10.10.10.1/32</td>
<td>Enabled</td>
<td>Up</td>
<td>1500</td>
<td>my-vrf</td>
</tr>
</tbody>
</table>
```

```
switch (config) # show ip interface vrf default brief
```

```
<table>
<thead>
<tr>
<th>Interface</th>
<th>Address/Mask</th>
<th>Admin-state</th>
<th>Oper-state</th>
<th>MTU</th>
<th>VRF</th>
</tr>
</thead>
<tbody>
<tr>
<td>mgmt0</td>
<td>10.224.22.27/24</td>
<td>Enabled</td>
<td>Up</td>
<td>1500</td>
<td>default</td>
</tr>
<tr>
<td>mgmt1</td>
<td>0.0.0.0/0</td>
<td>Enabled</td>
<td>Down</td>
<td>1500</td>
<td>default</td>
</tr>
<tr>
<td>Vlan 30</td>
<td>30.30.30.1/24</td>
<td>Enabled</td>
<td>Down</td>
<td>1500</td>
<td>default</td>
</tr>
<tr>
<td>Eth1/2</td>
<td>2.2.2.2/24</td>
<td>Enabled</td>
<td>Down</td>
<td>1500</td>
<td>default</td>
</tr>
<tr>
<td>Loopback 11</td>
<td>11.11.11.1/32</td>
<td>Enabled</td>
<td>Up</td>
<td>1500</td>
<td>default</td>
</tr>
</tbody>
</table>
```

<table>
<thead>
<tr>
<th>Related Commands</th>
<th>N/A</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>If no routing-context is specified, the “routing-context” VRF is automatically displayed.</td>
</tr>
</tbody>
</table>
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.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>id</th>
<th>A numeric range of 0-31</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>N/A</td>
<td></td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Config</td>
<td></td>
</tr>
<tr>
<td>History</td>
<td>3.2.3000</td>
<td></td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
<td></td>
</tr>
</tbody>
</table>
| Example            | switch (config) # interface loopback 10
                     switch (config interface loopback 10) # |

**Related Commands**

**Note**

- Up to 32 loopback interfaces can be configured
- Within the loopback configuration mode, you can configure description and ip-address
- MTU cannot be configured on the loopback interface
### ip address

**Syntax**

```plaintext
ip address <ip-address> <mask>
no ip address <ip-address> <mask>
```

Enters user-defined description for the interface.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>ip-address</th>
<th>IPv4 address.</th>
</tr>
</thead>
<tbody>
<tr>
<td>mask</td>
<td></td>
<td>There are two possible ways to the mask:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- /length – only /32 is possible</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Network address (i.e. 255.255.255.0)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Default</th>
<th>0.0.0.0/0</th>
</tr>
</thead>
</table>

**Configuration Mode**

Config Interface Loopback

**History**

3.3.5006

**Role**

admin

**Example**

```plaintext
switch (config interface loopback 10) # ip address 10.10.10.10 /32
```

**Related Commands**

interface loopback

**Note**
description

description <string>
no description

Enters a description for the interface.
The no form of the command sets the description to default.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>string</th>
<th>User defined string.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>&quot;&quot;</td>
<td></td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Config Interface Loopback</td>
<td></td>
</tr>
<tr>
<td>History</td>
<td>3.3.5006</td>
<td></td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
<td></td>
</tr>
<tr>
<td>Example</td>
<td>switch (config interface loopback 10) # description my-ip-interface</td>
<td></td>
</tr>
<tr>
<td>Related Commands</td>
<td>interface loopback</td>
<td></td>
</tr>
<tr>
<td>Note</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
**show interfaces loopback**

**show interface loopback <id>**

Shows the attribute of the interface loopback.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>id</td>
<td>A numeric range of 1-32</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Default</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuration Mode</td>
<td>Config</td>
</tr>
<tr>
<td>History</td>
<td>3.2.3000</td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
</tr>
</tbody>
</table>

**Example**

```
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) #
```

**Related Commands**

- None

**Note**

- None
### ip route

**Syntax**
```
ip route [vrf <vrf-name>] <IP prefix> <netmask> <next hop IP address>
oip 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.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>vrf-name</th>
<th>VRF session name</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>ip prefix</td>
<td>IP address</td>
</tr>
<tr>
<td></td>
<td>netmask</td>
<td>There are two possible ways to the mask:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• /length (i.e. /24)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Network address (i.e. 255.255.255.0)</td>
</tr>
<tr>
<td>next hop IP address</td>
<td></td>
<td>IP address of the next hop.</td>
</tr>
</tbody>
</table>

**Default**
N/A

**Configuration Mode**
Config

**History**
- 3.1.0000
- 3.4.2008 Added VRF parameter

**Role**
admin

**Example**
```
switch (config) # ip route vrf my-vrf 80.80.80.0 /24 20.20.20.2
```

**Related Commands**
N/A

**Notes**
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.

<table>
<thead>
<tr>
<th><strong>Syntax Description</strong></th>
<th><strong>type</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• source-ip-port – source ip and TCP/UDP port</td>
</tr>
<tr>
<td></td>
<td>• destination-ip-port – destination ip and TCP/UDP port</td>
</tr>
<tr>
<td></td>
<td>• source-destination-ip-port – source &amp; destination ip and TCP/UDP port</td>
</tr>
<tr>
<td></td>
<td>• traffic-class – traffic class</td>
</tr>
<tr>
<td></td>
<td>• flow-label – flow label</td>
</tr>
<tr>
<td></td>
<td>• all – all options</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Default</strong></th>
<th><strong>all</strong></th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th><strong>Configuration Mode</strong></th>
<th><strong>Config</strong></th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th><strong>History</strong></th>
<th><strong>3.2.0230</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>3.5.1000</td>
<td>Added flow-label parameter and updated Note section</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Role</strong></th>
<th><strong>admin</strong></th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th><strong>Example</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>switch (config) # ip load-sharing all</td>
</tr>
<tr>
<td>switch (config) # show ip load-sharing</td>
</tr>
<tr>
<td>Load sharing: all</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Related Commands</strong></th>
<th><strong>ip route</strong></th>
</tr>
</thead>
</table>

| **Note** | 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.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>all</td>
<td>Displays routing tables for all VRF instances</td>
</tr>
<tr>
<td>-a</td>
<td>Displays static routes currently inactive due to the interface being down</td>
</tr>
<tr>
<td>static</td>
<td>Displays static route</td>
</tr>
<tr>
<td>summary</td>
<td>Displays route summary</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Default</th>
<th>N/A</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Configuration Mode</th>
<th>Any Command Mode</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>History</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.1.0000</td>
<td>First version</td>
</tr>
<tr>
<td>3.3.3500</td>
<td>Added Distance/Metric column</td>
</tr>
<tr>
<td>3.4.0000</td>
<td>Added -a parameter</td>
</tr>
<tr>
<td>3.4.2008</td>
<td>Added VRF parameter</td>
</tr>
<tr>
<td>3.4.3000</td>
<td>Updated Notes section</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Role</th>
<th>admin</th>
</tr>
</thead>
</table>
Example

```bash
switch (config) # show ip route vrf my-vrf

VRF Name: my-vrf

<table>
<thead>
<tr>
<th>Destination</th>
<th>Mask</th>
<th>Gateway</th>
<th>Interface</th>
<th>Source</th>
<th>Distance/Metric</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.10.10.1</td>
<td>255.255.255.255</td>
<td>0.0.0.0</td>
<td>loopback10</td>
<td>direct</td>
<td>0/0</td>
</tr>
<tr>
<td>20.20.20.0</td>
<td>255.255.255.0</td>
<td>0.0.0.0</td>
<td>vlan20</td>
<td>direct</td>
<td>0/0</td>
</tr>
<tr>
<td>80.80.80.0</td>
<td>255.255.255.0</td>
<td>20.20.20.2</td>
<td>vlan20</td>
<td>static</td>
<td>1/0</td>
</tr>
</tbody>
</table>

switch (config) # show ip route vrf my-vrf static

VRF Name: my-vrf

<table>
<thead>
<tr>
<th>Destination</th>
<th>Mask</th>
<th>Gateway</th>
<th>Interface</th>
<th>Source</th>
<th>Distance/Metric</th>
</tr>
</thead>
<tbody>
<tr>
<td>80.80.80.0</td>
<td>255.255.255.0</td>
<td>20.20.20.2</td>
<td>vlan20</td>
<td>static</td>
<td>1/0</td>
</tr>
</tbody>
</table>

switch (config) # show ip route vrf my-vrf summary

VRF Name: my-vrf

<table>
<thead>
<tr>
<th>Route Source</th>
<th>Routes</th>
</tr>
</thead>
<tbody>
<tr>
<td>direct</td>
<td>2</td>
</tr>
<tr>
<td>static</td>
<td>1</td>
</tr>
<tr>
<td>ospf</td>
<td>0</td>
</tr>
<tr>
<td>bgp</td>
<td>0</td>
</tr>
<tr>
<td>DHCP</td>
<td>0</td>
</tr>
<tr>
<td>Total</td>
<td>3</td>
</tr>
</tbody>
</table>

switch (config) # show ip route vrf my-vrf -a

VRF Name: my-vrf

<table>
<thead>
<tr>
<th>Destination</th>
<th>Mask</th>
<th>Gateway</th>
<th>Interface</th>
<th>Source</th>
<th>Distance/Metric</th>
</tr>
</thead>
<tbody>
<tr>
<td>90.90.90.0</td>
<td>255.255.255.0</td>
<td>1.1.1.2</td>
<td>NA</td>
<td>static</td>
<td>1/0</td>
</tr>
</tbody>
</table>
```

Related Commands

- `ip route`

Notes

- 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
**show ip load-sharing**

`show ip load-sharing`

Displays ECMP hash attribute.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>N/A</td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Any Command Mode</td>
</tr>
<tr>
<td>History</td>
<td>3.2.0230</td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
</tr>
</tbody>
</table>
| Example            | `switch (config) # show ip load-sharing
Load sharing: all
switch (config) #` |
| Related Commands   | ip load-sharing |
| Note               | |
### 6.1.4.6 Network to Media Resolution (ARP)

#### ip arp

```bash
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.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vrf-name</td>
<td>VRF session name</td>
</tr>
<tr>
<td>IP address</td>
<td>IPv4 address</td>
</tr>
<tr>
<td>mac-address</td>
<td>MAC address (format XX:XX:XX:XX:XX:XX)</td>
</tr>
</tbody>
</table>

**Default**
N/A

**Configuration Mode**
Config

**History**
3.4.2008

**Role**
admin

**Example**
```
switch (config) # ip arp vrf my-vrf 20.20.20.2 aa:bb:cc:dd:ee:ff
```

**Related Commands**
N/A

**Notes**
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.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>timeout-value</th>
<th>Time (in seconds) that an entry remains in the ARP cache. Range: 240-28800.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>1500 seconds</td>
<td></td>
</tr>
</tbody>
</table>
| Configuration Mode  | Config Interface Ethernet  
                      Config Interface VLAN  
                      Config Interface Port Channel  |
| History             | 3.2.0230      | Updated Note section                                               |
| Role                | admin         |                                                                 |
| Example             | switch (config) # ip arp timeout 2000  
                      switch (config) # show ip arp  |
|                     | ARP Timeout: 2000  
                      Total number of entries: 55  
                      IP Address          MAC Address         Interface  
                      1.0.0.2               00:02:c9:5c:30:40       Vlan11  
                      1.0.0.3               00:11:22:33:44:55       Vlan11  
                      2.0.0.2               00:02:c9:5c:30:40       Vlan12  
                      3.0.0.2               00:02:c9:5c:30:40       Vlan13  
                      4.0.0.2               00:02:c9:5c:30:40       Vlan14  |

| Related Commands | ip arp  
                      show ip arp  |

| Note              | • This configuration may take up to 5 minutes to take effect  
                      • The time interval after which each ARP entry becomes stale may actually vary from 50-150% of the configured value |
### clear ip arp

**clear ip arp [vrf <vrf-name>] [interface <type> | <IP-address>]**

Clears the dynamic ARP cache for the specific VRF session.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vrf-name</td>
<td>VRF session name</td>
</tr>
<tr>
<td>interface</td>
<td>Clears dynamic ARP entries for a interface</td>
</tr>
<tr>
<td>ip-address</td>
<td>Clears dynamic ARP entries for a specific IP address</td>
</tr>
</tbody>
</table>

**Default**: N/A

**Configuration Mode**: Config

**History**

3.2.0230

Added VRF parameter

**Role**: admin

**Example**

```
switch (config) # clear ip arp vrf my-vrf
switch (config) #
```

**Related Commands**

- ip arp
- show ip arp

**Notes**

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.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>all</td>
<td>Displays all ARP information for all VRF</td>
</tr>
<tr>
<td>interface</td>
<td>Displays all ARP information for specific interface</td>
</tr>
<tr>
<td>count</td>
<td>Displays number of ARPs for specific VRF</td>
</tr>
</tbody>
</table>

**Default**

N/A

**Configuration Mode**

Any Command Mode

**History**

3.3.3000

3.4.2008 Added VRF parameter

**Role**

admin

**Example**

```
switch (config) # show ip arp vrf my-vrf

VRF Name: my-vrf
--
Total number of entries: 2

Address     Type      Hardware Address Interface
------------- ----------- ------------------ ------------
 1.1.1.2     Static ETH 00:11:22:33:44:55       eth 1/1

switch (config) # show ip arp vrf my-vrf interface ethernet 1/1

VRF Name: my-vrf
--
Total number of entries: 1

Address     Type      Hardware Address Interface
------------- ----------- ------------------ ------------
 1.1.1.2     Static ETH 00:11:22:33:44:55       eth 1/1

switch (config) # show ip arp vrf my-vrf interface vlan 20

VRF Name: my-vrf
--
Total number of entries: 1

Address     Type      Hardware Address Interface
------------- ----------- ------------------ ------------

switch (config) #
```
<table>
<thead>
<tr>
<th>Related Commands</th>
<th>ip arp</th>
</tr>
</thead>
<tbody>
<tr>
<td>Notes</td>
<td>If no routing-context is specified, the “routing-context” VRF is automatically displayed.</td>
</tr>
</tbody>
</table>
### 6.1.4.7 IP Diagnostic Tools

#### ping


Sends ICMP echo requests to a specified host.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Linux Ping options</th>
</tr>
</thead>
<tbody>
<tr>
<td>vrf</td>
<td>Specifies VRF instance name</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Default</th>
<th>N/A</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Configuration Mode</th>
<th>Config</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>History</th>
<th>3.1.0000</th>
</tr>
</thead>
</table>

Role

<table>
<thead>
<tr>
<th>Role</th>
<th>admin</th>
</tr>
</thead>
</table>

Example

```bash
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
```

Related Commands

| Related Commands | traceroute |

Note

When using `-I` option use the interface name + interface number, for example “ping -I vlan10”
traceroute


Traces the route packets take to a destination.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vrf</td>
<td>Specifies VRF instance name</td>
</tr>
<tr>
<td>-4</td>
<td>Uses IPv4.</td>
</tr>
<tr>
<td>-6</td>
<td>Use IPv6.</td>
</tr>
<tr>
<td>-d</td>
<td>Enables socket level debugging.</td>
</tr>
<tr>
<td>-F</td>
<td>Sets DF (“do not fragment” bit) on.</td>
</tr>
<tr>
<td>-I</td>
<td>Uses ICMP ECHO for tracerouting.</td>
</tr>
<tr>
<td>-T</td>
<td>Uses TCP SYN for tracerouting.</td>
</tr>
<tr>
<td>-U</td>
<td>Uses UDP datagram (default) for tracerouting.</td>
</tr>
<tr>
<td>-n</td>
<td>Does not resolve IP addresses to their domain names.</td>
</tr>
<tr>
<td>-r</td>
<td>Bypasses the normal routing and send directly to a host on an attached network.</td>
</tr>
<tr>
<td>-A</td>
<td>Performs AS path lookups in routing registries and print results directly after the corresponding addresses.</td>
</tr>
<tr>
<td>-V</td>
<td>Prints version info and exit.</td>
</tr>
<tr>
<td>-f</td>
<td>Starts from the first_ttl hop (instead from 1).</td>
</tr>
<tr>
<td>-g</td>
<td>Routes packets throw the specified gateway (maximum 8 for IPv4 and 127 for IPv6).</td>
</tr>
<tr>
<td>-i</td>
<td>Specifies a network interface to operate with.</td>
</tr>
<tr>
<td>-m</td>
<td>Sets the max number of hops (max TTL to be reached). Default is 30.</td>
</tr>
<tr>
<td>-N</td>
<td>Sets the number of probes to be tried simultaneously (default is 16).</td>
</tr>
</tbody>
</table>
-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).

<table>
<thead>
<tr>
<th>Default</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuration Mode</td>
<td>Config</td>
</tr>
<tr>
<td>History</td>
<td>3.1.0000</td>
</tr>
<tr>
<td></td>
<td>3.4.2008 Added VRF parameter</td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
</tr>
</tbody>
</table>

Example

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

Related Commands

Note

- The following flags are not supported: -6, -l, -A
- When using -i option use the interface name + interface number, for example “traceroute -i vlan10”
**tcpdump**

```
```

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

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>vrf</th>
<th>Specifies VRF instance name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>N/A</td>
<td></td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Config</td>
<td></td>
</tr>
<tr>
<td>History</td>
<td>3.1.0000</td>
<td></td>
</tr>
<tr>
<td></td>
<td>3.4.2008</td>
<td>Added VRF parameter</td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
<td></td>
</tr>
</tbody>
</table>
| Example            | switch (config) # tcpdump
|                    | 09:37:38.678812 IP 192.168.10.7.ssh > 192.168.10.1.54155: P
|                    | 1494624:1494800(176) ack 625 win 90
|                    | <nop,nop,timestamp 5842763 858672398>
|                    | 09:37:38.678860 IP 192.168.10.7.ssh > 192.168.10.1.54155: P
|                    | 1494800:1495104(304) ack 625 win 90
|                    | <nop,nop,timestamp 5842763 858672398>
|                    | ... |
|                    | 9141 packets captured |
|                    | 9142 packets received by filter |
|                    | 0 packets dropped by kernel |
|                    | switch (config) # |
| Related Commands   | N/A |                              |
| Note               | • When using -i option use the interface name + interface number, for example “tcpdump -i vlan10” |
|                    | • For all flag options of this command refer to the linux ‘man page’ of tcpdump. |
**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.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>Disabled.</td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Config</td>
</tr>
<tr>
<td>History</td>
<td>3.3.4000</td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
</tr>
</tbody>
</table>
| Example            | `switch (config) # qos map dscp-to-pcp preserve-pcp
switch (config) #` |

**Related Commands**

**Note**
6.2 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.

6.2.1 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

6.2.2 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.

### 6.2.3 Configuring OSPF

![OSPF Basic Topology](image)

**Figure 34: OSPF Basic Topology**

**Precondition steps:**

1. The following configuration example refers to Router 2 in Figure 34. The remainder of the routers in the figure are configured similarly.

2. 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 2.4, “Licenses,” on page 54.

**Step 2.** Enable IP routing functionality. Run:

```bash
switch (config)# ip routing
```

**Step 3.** Enable the desired VLAN. Run:

```bash
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
```

### 6.2.4 Verifying OSPF

- To verify OSPF configuration and status:

Step 1. Verify OSPF configuration and status. Run:

```
switch (config) # show ip ospf
```
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) #
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
```
Step 3. Verify the OSPF Interface configuration and status run:

```
switch (config) #

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) #
```
6.2.5 Commands

6.2.5.1 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.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>OSPF feature is disabled.</td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Config</td>
</tr>
<tr>
<td>History</td>
<td>3.3.3500</td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
</tr>
<tr>
<td>Example</td>
<td>switch (config)# protocol ospf</td>
</tr>
<tr>
<td>Related Commands</td>
<td>ip routing</td>
</tr>
<tr>
<td>Note</td>
<td></td>
</tr>
</tbody>
</table>
### router ospf

**Syntax:**
```
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.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>process-id</th>
<th>OSPF instance ID</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>vrf</td>
<td>VRF name (e.g. default)</td>
</tr>
</tbody>
</table>

| Default | Process ID: 1  
          | VRF: Active VRF routing-context |

| Configuration Mode | Config |

| History | 3.3.3500  
          | 3.6.1002  
          | Added VRF and process ID parameters and updated Example |

| Role | admin |

**Example**
```
switch (config)# router ospf 2 vrf myvrf
switch (config router ospf 2)#
```

| Related Commands | N/A |

**Note**
Only one OSPF instance is supported
6.2.5.2 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**

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>ip-address</th>
<th>The Router id in IP address format.</th>
</tr>
</thead>
</table>

**Default**

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.

**Configuration Mode**

Config OSPF Router

**History**

3.3.3500

**Role**

admin

**Example**

```
switch (config router ospf)# router-id 10.10.10.10
```

**Related Commands**

N/A

**Note**
### shutdown

**shutdown**
**no shutdown**

Disables the OSPF instance. The no form of the command enables the OSPF instance.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>Enable (no shutdown)</td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Config OSPF Router</td>
</tr>
<tr>
<td>History</td>
<td>3.3.3500</td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
</tr>
<tr>
<td>Example</td>
<td><code>switch (config router ospf)# shutdown</code></td>
</tr>
<tr>
<td>Related Commands</td>
<td>N/A</td>
</tr>
<tr>
<td>Note</td>
<td></td>
</tr>
</tbody>
</table>
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.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>ref-bw</th>
<th>Range: 1-4294</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Gbps</td>
<td>Value in Gbps (default if not specified)</td>
</tr>
<tr>
<td></td>
<td>Mbps</td>
<td>Value in Mbps</td>
</tr>
</tbody>
</table>

Default 40 Gbps

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.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>value</td>
<td>OSPF administrative distance. Range is 1-255.</td>
</tr>
</tbody>
</table>

| Default | 110 |

<table>
<thead>
<tr>
<th>Configuration Mode</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Config OSPF Router</td>
<td></td>
</tr>
</tbody>
</table>

| History | 3.3.3500 |

| Role | admin |

| Example | switch (config router ospf)# distance 100 |

| Related Commands | N/A |

| Note | |


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.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>direct</td>
<td>Redistribute directly connected routes.</td>
</tr>
<tr>
<td>bgp</td>
<td>Redistribute routes from BGP protocol.</td>
</tr>
<tr>
<td>ibgp</td>
<td>Redistribute IBGP routes</td>
</tr>
<tr>
<td>ebgp</td>
<td>Redistribute EBGP routes</td>
</tr>
<tr>
<td>static</td>
<td>Redistribute static configured routes.</td>
</tr>
</tbody>
</table>

**Default**
Disable (no redistribution)

**Configuration Mode**
Config OSPF Router

**History**
3.6.3504
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.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>spf-delay</td>
<td>The interval by which SPF calculations delayed after a topology change reception. Range is 0-100 milliseconds.</td>
</tr>
<tr>
<td>spf-hold</td>
<td>The minimum delay between two consecutive delay calculations. Range is 0-1000 milliseconds.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Default</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>spf-delay: 1 millisecond</td>
<td></td>
</tr>
<tr>
<td>spf-hold: 10 millisecond</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Configuration Mode</th>
<th>Config OSPF Router</th>
</tr>
</thead>
</table>

| History         | 3.3.3500 |
| Role            | admin    |

**Example**

```
switch (config router ospf)# timers throttle spf 100 1000
```

**Related Commands**

N/A

**Note**
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.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>area-id</td>
<td>OSPF area-id. Range is 0-4294967295.</td>
</tr>
<tr>
<td>cost</td>
<td>The cost for the default summary route. Range is 1-16777215.</td>
</tr>
</tbody>
</table>

**Default**
The summary route cost is based on the area border router that generated the summary route.

**Configuration Mode**
Config OSPF Router

**History**
3.3.3500

**Role**
admin

**Example**
switch (config router ospf)# area 0 default-cost 100

**Related Commands**
N/A

**Note**
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.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>area-id</td>
<td>OSPF area-ID. Range is 0-4294967295.</td>
</tr>
<tr>
<td>ip-address</td>
<td>IP Address.</td>
</tr>
<tr>
<td>not-advertise</td>
<td>Suppresses routes that match the specified IP address.</td>
</tr>
<tr>
<td>prefix</td>
<td>Network prefix (in the format of /24, or 255.255.255.0 for example).</td>
</tr>
</tbody>
</table>

**Default**

Disabled

**Configuration Mode**

Config OSPF Router

**History**

3.3.3500

**Role**

admin

**Example**

```
switch (config router ospf)# area 0 range 10.10.10.10 /24
```

**Related Commands**

N/A

**Note**

---
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).

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>area-id</th>
<th>OSPF area-ID. Range is 0-4294967295.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>no-summary</td>
<td>Summary route will not be advertised into the stub area.</td>
</tr>
</tbody>
</table>

**Default**
- Summary route will be advertised.

**Configuration Mode**
- Config OSPF Router

**History**
- 3.3.3500

**Role**
- admin

**Example**
- `switch (config router ospf)# area 0 stub`

**Related Commands**
- N/A

**Note**
**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.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>area-id</td>
<td>OSPF area ID. Range is 0-4294967295.</td>
</tr>
<tr>
<td>default-information-</td>
<td>A default type7 LSA (Link State Advertisements) is generated into the NSSA</td>
</tr>
<tr>
<td>originate</td>
<td>area.</td>
</tr>
<tr>
<td>m-type</td>
<td>Metric type for OSPF. Range is 1-2.</td>
</tr>
<tr>
<td>m-value</td>
<td>Metric value for OSPF. Range is 1-65535.</td>
</tr>
<tr>
<td>no-summary</td>
<td>Summary route will not be advertised into the NSSA area.</td>
</tr>
<tr>
<td>translate type7 always</td>
<td>Type7 LSAs is translated to type5 LSAs (Link State Advertisements).</td>
</tr>
</tbody>
</table>

**Default**

- Default m-type:2
- Default m-value:10

**Configuration Mode**

- Config OSPF Router

**History**

- 3.3.3500

**Role**

- admin

**Example**

```
switch (config router ospf)# area 0 nssa
```

**Related Commands**

- N/A

**Note**

An area can be either stub, NSSA or normal.
**no area**

**no area <area-id>**

Deletes OSPF area and its related configuration.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>area-id</th>
<th>OSPF area ID</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Range is 0-4294967295</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Default</th>
<th>N/A</th>
</tr>
</thead>
</table>

**Configuration Mode**

Config OSPF Router

**History**

3.3.3500

**Role**

admin

**Example**

switch (config router ospf)# no area 1

**Related Commands**

N/A

**Note**

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.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip-address</td>
<td>The summary IP address.</td>
</tr>
<tr>
<td>not-advertise</td>
<td>Suppresses routes that match the specified ip-address.</td>
</tr>
<tr>
<td>prefix</td>
<td>Network prefix (in the format of /24 or 255.255.255.0, for example).</td>
</tr>
</tbody>
</table>

**Default**

N/A

**Configuration Mode**

Config OSPF Router

**History**

3.3.3500

**Role**

admin

**Example**

```
switch (config router ospf)# summary-address 10.10.10.10 /24
```

**Related Commands**

N/A

**Note**

Maximum of 1500 summarized IP addresses can be configured.
6.2.5.3 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.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>cost</th>
<th>The Interface cost used by the OSPF. Range is 1-65535.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>1</td>
<td></td>
</tr>
</tbody>
</table>
| 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            | 3.3.3500 |                                               |
| Role               | admin |                                                       |
| Example            | switch (config interface vlan 10)# ip ospf cost 100 |                          |
| Related Commands   | N/A  |                                                       |
| Note               |      |                                                       |
**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.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>seconds</th>
<th>The dead-interval timer, in seconds. Range is 1-65535.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>40</td>
<td></td>
</tr>
</tbody>
</table>
| 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             | 3.3.3500 |                                                       |
| Role                | admin   |                                                       |
| Example             | switch (config interface vlan 10)# ip ospf dean-interval 10  
                     |  
                     | N/A                                                       |
| Note                | 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.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>seconds</th>
<th>The Hello interval timer, in seconds. Range is 1-65535.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>10</td>
<td></td>
</tr>
</tbody>
</table>
| 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            | 3.3.3500 |                                                       |
| Role               | admin   |                                                       |
| Example            | switch (config interface vlan 10)# ip ospf hello-interval 20 |
| Related Commands   | N/A     |                                                       |
| Note               | 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.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>number</th>
<th>The Interface priority used by the OSPF protocol. Range is 0-255</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>1</td>
<td></td>
</tr>
</tbody>
</table>
| 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            | 3.3.3500 |                                                               |
| Role               | admin  |                                                                   |
| Example            | switch (config interface vlan 10)# ip ospf priority 100       |
| Related Commands   | N/A    |                                                                   |

**Note**

- 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.
- 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.
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.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>type</th>
<th>The network type on this interface. The options are ‘broadcast’ or ‘point-to-point’.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td></td>
<td>broadcast</td>
</tr>
</tbody>
</table>
| 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            | 3.3.3500 |                                                                                               |
| Role               |      | admin                                                                                         |
| Example            |      | switch (config interface vlan 10) ip ospf network point-to-point                               |
| Related Commands   | N/A  |                                                                                               |
| Note               |      | • 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.
• All routers on the same network should have the same network type. |
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.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>seconds</th>
<th>The retransmit interval in seconds. Range is 0-3600.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>5</td>
<td></td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Config Interface VLAN Config Interface Ethernet configured as a router port interface Config Interface Port Channel configured as a router port interface</td>
<td></td>
</tr>
<tr>
<td>History</td>
<td>3.3.3500</td>
<td></td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
<td></td>
</tr>
<tr>
<td>Example</td>
<td>switch (config interface vlan 10)# ip ospf retransmit-interval 10</td>
<td></td>
</tr>
<tr>
<td>Related Commands</td>
<td>N/A</td>
<td></td>
</tr>
<tr>
<td>Note</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
**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.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>Active interface (no ip ospf passive-interface)</td>
</tr>
</tbody>
</table>
| 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            | 3.3.3500 |
| Role               | admin |
| Example            | switch (config interface vlan 10)# ip ospf passive-interface |
| Related Commands   | N/A |
| Note               | N/A |
### 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.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>seconds</th>
<th>The transmit-delay interval in seconds. Range is 0-3600.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Default</strong></td>
<td>1</td>
<td></td>
</tr>
</tbody>
</table>
| **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**        | 3.3.3500 |                                                       |
| **Role**           | admin   |                                                        |
| **Example**        | switch (config interface vlan 10)# ip ospf transmit-delay 2 |
| **Related Commands** | N/A     |                                                        |
| **Note**           |         |                                                        |
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.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>Enabled (no shutdown)</td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Config Interface VLAN</td>
</tr>
<tr>
<td></td>
<td>Config Interface Ethernet configured as a router port interface</td>
</tr>
<tr>
<td></td>
<td>Config Interface Port Channel configured as a router port interface</td>
</tr>
<tr>
<td>History</td>
<td>3.3.3500</td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
</tr>
<tr>
<td>Example</td>
<td><code>switch (config interface vlan 10)# ip ospf shutdown</code></td>
</tr>
<tr>
<td>Related Commands</td>
<td>N/A</td>
</tr>
<tr>
<td>Note</td>
<td>N/A</td>
</tr>
</tbody>
</table>
**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.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>message-digest</th>
<th>Specifies that message-digest authentication (MD5) is used.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>Disabled (no)</td>
<td></td>
</tr>
</tbody>
</table>
| 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            | 3.3.3500       |                                                           |
| Role               | admin          |                                                           |
| Example            | switch (config interface vlan 10)# ip ospf authentication |
| Related Commands   | N/A            |                                                           |
| Note               | • Without message-digest option, a simple password authentication will be used.  
|                    | • Message-digest authentication can be enabled only if a key is configured.  |
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.

### Syntax Description

| Syntax Description | auth-type | The authentication type:
|                    |          | 0 – unencrypted password
|                    |          | 7 – MD5 key
| password           |          | Authentication password (up to 8 alphanumeric string)

### Default

Unencrypted password

### 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

3.3.3500

### Role

admin

### Example

switch (config interface vlan 10)# ip ospf authentication-key 0
mycleartextpassword

### Related Commands

N/A

### Note

- When selecting an encrypted password “7”, the user must input a password encrypted with an MD5 key.
- When selecting an unencrypted password “0”, the user must input a cleartext password. Then when examining the running-config, it exhibits the encrypted password.
### ip ospf message-digest-key

- **Syntax:**
  - `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.

- **Syntax Description**
  - **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.

- **Default**
  - Unencrypted (no)

- **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**
  - 3.3.3500

- **Role**
  - admin

- **Example**
  - `switch (config interface vlan 10) # ip ospf message-digest-key mykeyid md5 7 mykey`

- **Related Commands**
  - N/A

- **Note**
  - 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.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>area-id</th>
<th>OSPF area ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>N/A</td>
<td>Range is 0-4294967295</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Configuration Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>Config Interface VLAN</td>
</tr>
<tr>
<td>Config Interface Ethernet configured as a router port interface</td>
</tr>
<tr>
<td>Config Interface Port Channel configured as a router port interface</td>
</tr>
<tr>
<td>Config Interface Loopback</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>History</th>
<th>3.3.3500</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Role</th>
<th>admin</th>
</tr>
</thead>
</table>

**Example**

```
switch (config interface vlan 10)# ip ospf area 0
```

**Related Commands**

N/A

**Note**

N/A
### show ip ospf

**show ip ospf [<process-id> [vrf <vrf-name>]]**

Displays general OSPF configuration on specific VRF and status.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>process-id</td>
<td>OSPF instance ID</td>
</tr>
<tr>
<td>vrf</td>
<td>VRF instance</td>
</tr>
</tbody>
</table>

**Default**

- Process ID: 1
- VRF: Active VRF routing-context

**Configuration Mode**

Any Command Mode

**History**

- 3.3.3500
- 3.6.1002 Added VRF and process ID parameters and updated Example

**Role**

admin

**Example**

```
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 msecs
SPF Hold time 5000 msecs
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
```

**Related Commands**

N/A

**Note**

-
### show ip ospf border-routers

**show ip ospf border-routers [vrf <vrf-name>]**

Displays routing table entries to an Area Border Routers.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>vrf</th>
<th>OSPF routing table entries to an Area Border Routers on specific VRF.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td></td>
<td>VRF: Active VRF routing-context</td>
</tr>
<tr>
<td>Configuration Mode</td>
<td></td>
<td>Any Command Mode</td>
</tr>
<tr>
<td>History</td>
<td></td>
<td>3.3.3500</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3.6.1002 Added VRF parameter and updated Example</td>
</tr>
<tr>
<td>Role</td>
<td></td>
<td>admin</td>
</tr>
<tr>
<td>Example</td>
<td></td>
<td>switch (config)# show ip ospf border-routers vrf myvrf</td>
</tr>
<tr>
<td></td>
<td></td>
<td>OSPF Process ID 2, vrf myvrf Internal Routing Table</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Codes: i - Intra-area route, I - Inter-area route</td>
</tr>
<tr>
<td></td>
<td></td>
<td>i 1.1.1.1 [0] ABR Area: 0.0.0.0, Next Hop: 21.21.21.1</td>
</tr>
<tr>
<td>Related Commands</td>
<td></td>
<td>N/A</td>
</tr>
<tr>
<td>Note</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
show ip ospf database

show ip ospf database [summary] [process-id <process-id> | area-id <area-id> | link-state-id <link-state-id>] [adv-router <ip-address> | self-originated] [vrf <vrf-name>]

Displays the OSPF database.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>adv-router &lt;ip-address&gt;</td>
<td>Filters per advertise router</td>
</tr>
<tr>
<td>area-id</td>
<td>Filters the command per OSPF Area ID. Range is 0-4294967295.</td>
</tr>
<tr>
<td>link-state-id</td>
<td>The link state ID</td>
</tr>
<tr>
<td>self-originated</td>
<td>Self Originate</td>
</tr>
<tr>
<td>summary</td>
<td>Summarizes the output of the OSPF database.</td>
</tr>
<tr>
<td>process-id</td>
<td>Displays OSPF database on specific instance ID</td>
</tr>
<tr>
<td>vrf</td>
<td>Displays OSPF database on specific VRF</td>
</tr>
</tbody>
</table>

Default
Process ID: 1
VRF: Active VRF routing-context

Configuration Mode
Any Command Mode

History
3.3.3500
3.6.1002 Added VRF and process ID parameters and updated Example

Role
admin

Example
switch (config)# show ip ospf database 2 vrf myvrf

OSPF Router with ID (2.2.2.2) (Process ID 2 VRF myvrf)

Router Link States (Area 0.0.0.0)

<table>
<thead>
<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>

Network Link States (Area 0.0.0.0)

<table>
<thead>
<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>
<tr>
<td>Related Commands</td>
<td>N/A</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>------------------</td>
<td>-----</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Note**
### show ip ospf interface

**show ip ospf interface [<process-id>] [vlan <vlan-id>] [brief]**

Displays the OSPF related interface configuration.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>brief</th>
<th>Gives a brief summary of the output</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>process-id</td>
<td>Displays OSPF interface configuration on specific instance ID</td>
</tr>
<tr>
<td></td>
<td>vlan &lt;vlan-id&gt;</td>
<td>Displays OSPF interface configuration and status per VLAN interface</td>
</tr>
<tr>
<td></td>
<td>vrf</td>
<td>Displays OSPF interface configuration on specific VRF</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Default</th>
<th>Process ID: 1</th>
<th>VRF: Active VRF routing-context</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Configuration Mode</th>
<th>Any Command Mode</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>History</th>
<th>3.3.3500</th>
</tr>
</thead>
</table>

3.6.1002 Added VRF and process ID parameters and updated Example

<table>
<thead>
<tr>
<th>Role</th>
<th>admin</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>switch (config) # show ip ospf interface 2 vrf myvrf</td>
</tr>
<tr>
<td>Interface Vlan is 21 Enabled, line protocol is Up</td>
</tr>
<tr>
<td>IP address 21.21.21.2, Mask 255.255.255.0</td>
</tr>
<tr>
<td>Process ID 2 VRF myvrf, Area 0.0.0.0</td>
</tr>
<tr>
<td>OSPF Interface Admin State is enabled</td>
</tr>
<tr>
<td>State DESIGNATED ROUTER, Network Type BROADCAST, Cost 10</td>
</tr>
<tr>
<td>Transmit delay 1 sec, Router Priority 1</td>
</tr>
<tr>
<td>DR is 2.2.2.2</td>
</tr>
<tr>
<td>Backup Designated Router is 1.1.1.1</td>
</tr>
<tr>
<td>Timer intervals (secs): Hello 10, Dead 40, Wait 40, Retransmit 5</td>
</tr>
<tr>
<td>No authentication</td>
</tr>
<tr>
<td>Number of opaque link LSAs: 0, checksum sum 0</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>switch (config) # show ip ospf interface 2 vrf myvrf brief</th>
</tr>
</thead>
<tbody>
<tr>
<td>OSPF Process ID 2 VRF myvrf</td>
</tr>
<tr>
<td>Total number of interface: 2</td>
</tr>
<tr>
<td>Interface Id</td>
</tr>
<tr>
<td>Vlan21</td>
</tr>
<tr>
<td>Ethernet1/22</td>
</tr>
<tr>
<td>Related Commands</td>
</tr>
<tr>
<td>------------------</td>
</tr>
<tr>
<td>Note</td>
</tr>
</tbody>
</table>
show ip ospf neighbors

show ip ospf neighbors [vlan <vlan-id>] [<neighbor-id>] [vrf <vrf-name>]

Displays the OSPF related interface neighbor configuration.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan &lt;vlan-id&gt;</td>
<td>Displays OSPF interface configuration and status per VLAN interface</td>
</tr>
<tr>
<td>neighbor-id</td>
<td>Filters the output per a specific OSPF neighbor</td>
</tr>
<tr>
<td>vrf</td>
<td>Displays OSPF interface neighbor configuration on specific VRF</td>
</tr>
</tbody>
</table>

Default: VRF: Active VRF routing-context

Configuration Mode: Any Command Mode

History:
- 3.3.3500
- 3.6.1002 Added VRF parameter and updated Example

Role: admin

Example:

```
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
```
<table>
<thead>
<tr>
<th>Related Commands</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Note</td>
<td></td>
</tr>
</tbody>
</table>
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.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>neighbor-id</th>
<th>Filters the output per a specific OSPF neighbor.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>vlan-id</td>
<td>Filters the output per a specific VLAN ID.</td>
</tr>
<tr>
<td></td>
<td>vrf &lt;vrf-name&gt;</td>
<td>Displays OSPF request-list on specific VRF</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Default</th>
<th>vrf: active VRF routing-context</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuration Mode</td>
<td>Any Command Mode</td>
</tr>
<tr>
<td>History</td>
<td>3.6.3504</td>
</tr>
<tr>
<td></td>
<td>3.3.3500</td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
</tr>
<tr>
<td>Example</td>
<td>switch (config) # show ip ospf request-list 4.4.4.4 vlan 7</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Type</th>
<th>ID-ID</th>
<th>ADV-RTR</th>
<th>Seq No</th>
<th>Age</th>
<th>Checksum</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>10.10.10.23</td>
<td>10.10.10.23</td>
<td>0x8000012f</td>
<td>37</td>
<td>0xa7b9</td>
</tr>
<tr>
<td>1</td>
<td>10.10.10.24</td>
<td>10.10.10.24</td>
<td>0x8000012f</td>
<td>38</td>
<td>0xbad61</td>
</tr>
</tbody>
</table>

| Related Commands | N/A |
| Note             |     |
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.

**Syntax Description**

- **neighbor-id**: Filters the output per a specific OSPF neighbor.
- **vrf <vrf-name>**: Displays OSPF retransmission-list on specific VRF.
- **vlan-id**: Filters the output per a specific VLAN ID.

**Default**

- vrf: Active VRF routing-context

**Configuration Mode**

- Any Command Mode

**History**

- 3.6.3504
- 3.3.3500

**Role**

- admin

**Example**

```bash
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

<table>
<thead>
<tr>
<th>Type</th>
<th>LS-ID</th>
<th>ADV-RTR</th>
<th>Seq No</th>
<th>Age</th>
<th>Checksum</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>22.22.22</td>
<td>7.7.7.1</td>
<td>0x80000045</td>
<td>0</td>
<td>0xaaf4</td>
</tr>
<tr>
<td>3</td>
<td>192.168.23.2</td>
<td>7.7.7.1</td>
<td>0x80000001</td>
<td>353</td>
<td>0x6752</td>
</tr>
</tbody>
</table>
```

**Related Commands**

- N/A

**Note**
**show ip ospf summary-address**

**Syntax**

```
show ip ospf summary-address [vrf <vrf-name>]
```

Displays a list of all summary address redistribution information configured on the OSPF.

**Syntax Description**

- **vrf <vrf-name>**
  
  Display summary address and area range information on specific VRF.

**Default**

- **vrf**: Active VRF routing-context

**Configuration Mode**

- Any Command Mode

**History**

- 3.6.3504
- 3.3.3500

**Role**

- **admin**

**Example**

```
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   
```

**Related Commands**

- N/A

**Note**
6.3 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.

6.3.1 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.

6.3.2 Configuring BGP

Figure 35: Basic BGP Configuration

![Basic BGP Configuration](image)
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
```
6.3.3 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)#
```

- 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.
### 6.3.4 Commands

#### 6.3.4.1 Config

**protocol bgp**

```plaintext
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.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>Disabled</td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Config</td>
</tr>
<tr>
<td>History</td>
<td>3.3.5006</td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
</tr>
</tbody>
</table>
| Example            | switch (config)# protocol bgp
                     | switch (config)# |
| Related Commands   | ip routing |
| Note               |     |
**clear ip bgp**

clear ip bgp [{<ip-address> | all} [soft] [in]]

Clears BGP learned routes from the BGP table and resets the connection to the neighbor.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip-address</td>
<td>A BGP peer IP address. Only the specified neighbor is reset.</td>
</tr>
<tr>
<td>all</td>
<td>All BGP peers. All BGP neighbors are reset.</td>
</tr>
<tr>
<td>soft</td>
<td>Clears BGP learned routes from the BGP table without resetting the connection to the neighbor</td>
</tr>
<tr>
<td>in</td>
<td>Inbound routes are reset</td>
</tr>
</tbody>
</table>

| Default          | N/A |
| Configuration Mode | Config |
| History          | 3.3.5006  First release  
                  | 3.3.5200  Updated description  
                  | 3.6.3004  Removed “out” parameter |
| Role             | admin |

**Example**

```
switch (config)# clear ip bgp all
switch (config)#
```

**Related Commands**

N/A

**Note**

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.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>as-number</th>
<th>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.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>N/A</td>
<td></td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Config</td>
<td></td>
</tr>
<tr>
<td>History</td>
<td>3.3.5006</td>
<td>First version</td>
</tr>
<tr>
<td></td>
<td>3.3.5200</td>
<td>Updated syntax description</td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
<td></td>
</tr>
</tbody>
</table>
| Example                   | switch (config)# router bgp 100  
switch (config router bgp 100)# |                                                                                                                                                                                             |
| Related Commands          | ip routing |                                                                                                                                                                                             |
| Note                      |           |                                                                                                                                                                                             |
### shutdown

**shutdown**

**no shutdown**

Gracefully disables BGP protocol without removing existing configuration. The no form of the command enables BGP.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>Enabled</td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Config Router BGP</td>
</tr>
<tr>
<td>History</td>
<td>3.3.5006</td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
</tr>
<tr>
<td>Example</td>
<td>switch (config router bgp 100)# no shutdown</td>
</tr>
<tr>
<td>Related Commands</td>
<td></td>
</tr>
<tr>
<td>Note</td>
<td></td>
</tr>
</tbody>
</table>
aggregate-address

aggregate-address <prefix> [summary-only] [as-set] [attribute-map]
no aggregate-address <prefix> [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.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>prefix</td>
<td>Destination to aggregate</td>
</tr>
<tr>
<td>summary-only</td>
<td>Contributor routes are not advertised.</td>
</tr>
<tr>
<td>as-set</td>
<td>Includes AS_PATH information from contributor routes as AS_SET attributes</td>
</tr>
<tr>
<td>attribute-map</td>
<td>Assigns attribute values in set commands of the map’s permit clauses. Deny clauses and match commands in permit clauses are ignored.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Default</th>
<th>Disabled</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuration Mode</td>
<td>Config Router BGP</td>
</tr>
<tr>
<td>History</td>
<td>3.4.0000</td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
</tr>
<tr>
<td>Example</td>
<td>switch-e07c04 [standalone: master] (config router bgp 4) # aggregate-address 3.5.3.7 /32</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Related Commands</th>
</tr>
</thead>
<tbody>
<tr>
<td>Note</td>
</tr>
<tr>
<td>- Aggregate routes combine the characteristics of multiple routes into a single route that the switch advertises</td>
</tr>
<tr>
<td>- Aggregation can reduce the amount of information that a BGP speaker is required to store and transmit when advertising routes to other BGP speakers</td>
</tr>
<tr>
<td>- Aggregate routes are advertised only after they are redistributed</td>
</tr>
</tbody>
</table>
**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.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>force</th>
<th>Applies configuration while BGP is admin-up</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Default</strong></td>
<td>Disabled</td>
<td></td>
</tr>
<tr>
<td><strong>Configuration Mode</strong></td>
<td>Config Router BGP</td>
<td></td>
</tr>
<tr>
<td><strong>History</strong></td>
<td>3.3.5006</td>
<td></td>
</tr>
<tr>
<td></td>
<td>3.3.5200</td>
<td>Updated description and notes</td>
</tr>
<tr>
<td></td>
<td>3.6.3004</td>
<td>Added “force” parameter</td>
</tr>
<tr>
<td><strong>Role</strong></td>
<td>admin</td>
<td></td>
</tr>
<tr>
<td><strong>Example</strong></td>
<td><code>switch (config router bgp 100)# bestpath as-path multipath-relax</code></td>
<td></td>
</tr>
<tr>
<td><strong>Related Commands</strong></td>
<td>maximum-paths</td>
<td></td>
</tr>
</tbody>
</table>

**Note**
- With this option disabled, only routes with exactly the same AS path as the best route to a destination are considered for ECMP
- With this option enabled, all routes with similar length AS path as the best route are considered for ECMP
### bgp fast-external-fallover

**Syntax:**

```
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.

<table>
<thead>
<tr>
<th><strong>Syntax Description</strong></th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Default</strong></td>
<td>no bgp fast-external-fallover</td>
</tr>
<tr>
<td><strong>Configuration Mode</strong></td>
<td>Config Router BGP</td>
</tr>
<tr>
<td><strong>History</strong></td>
<td>3.4.0000</td>
</tr>
<tr>
<td><strong>Role</strong></td>
<td>admin</td>
</tr>
<tr>
<td><strong>Example</strong></td>
<td><code>switch (config router bgp 100)# bgp fast-external-fallover</code></td>
</tr>
<tr>
<td><strong>Related Commands</strong></td>
<td><code>maximum-paths</code></td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>Although this feature improves BGP conversion time, it may cause instability in your BGP table due to a flapping interface.</td>
</tr>
</tbody>
</table>
**bgp listen limit**

```plaintext
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.

### Syntax Description

<table>
<thead>
<tr>
<th></th>
<th>maximum</th>
<th>The maximum number of dynamic BGP peers to be allowed on the switch. Range: 1-128.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Default</strong></td>
<td>100</td>
<td></td>
</tr>
<tr>
<td><strong>Configuration Mode</strong></td>
<td>Config Router BGP</td>
<td></td>
</tr>
<tr>
<td><strong>History</strong></td>
<td>3.4.0000</td>
<td></td>
</tr>
<tr>
<td><strong>Role</strong></td>
<td>admin</td>
<td></td>
</tr>
<tr>
<td><strong>Example</strong></td>
<td>switch (config router bgp 100)# bgp listen limit 101</td>
<td></td>
</tr>
</tbody>
</table>

### Related Commands

None.

### Note

None.
bgp listen range peer-group

`bgp listen range <ip-prefix> <length> peer-group <peer-group-name> remote-as <as-number>
no bgp listen range <ip-prefix> <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.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip-prefix</td>
<td>IP address</td>
</tr>
<tr>
<td>length</td>
<td>Mask length (e.g. /24 or 255.255.255.254)</td>
</tr>
<tr>
<td>peer-group-name</td>
<td>Peer group name</td>
</tr>
<tr>
<td>remote-as &lt;as-number&gt;</td>
<td>Remote peer’s number</td>
</tr>
</tbody>
</table>

Default: 100

Configuration Mode: Config Router BGP

History:
- 3.4.0000
- 3.6.3004 Added note

Role: admin

Example:
```
switch (config router bgp 100)# bgp listen range 10.10.10.10 /24 peer-group my-group remote-as 13
```

Related Commands

Note:
- To create a static peer group, use the command `neighbor peer-group`
- Neighbors in a dynamic peer group are configured as a group and cannot be configured individually
- 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.
- If dynamic peer range is defined with an overlap to another defined range, the longest remote address prefix take affect
**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.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip-address</td>
<td>The route reflector cluster ID</td>
</tr>
<tr>
<td></td>
<td>• 0.0.0.1 to 255.255.255.255 Valid cluster ID number</td>
</tr>
<tr>
<td></td>
<td>• 0.0.0.0 removes the cluster-ID from the switch (similar to “no cluster-id”)</td>
</tr>
<tr>
<td>force</td>
<td>Applies configuration while BGP is admin-up</td>
</tr>
</tbody>
</table>

| Default             | Cluster ID is the same as Router ID |
| Configuration Mode  | Config Router BGP |

<table>
<thead>
<tr>
<th>History</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.2.1000</td>
<td>First version</td>
</tr>
<tr>
<td>3.4.0000</td>
<td>Updated syntax description</td>
</tr>
<tr>
<td>3.6.3004</td>
<td>Added “force” parameter</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Role</th>
<th>admin</th>
</tr>
</thead>
</table>

**Example**

```
switch (config router bgp 100)# cluster-id 10.10.10.10
```

**Related Commands**

N/A

**Note**
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

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>client-to-client reflection is enabled</td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Config Router BGP</td>
</tr>
<tr>
<td>History</td>
<td>3.2.1000</td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
</tr>
<tr>
<td>Example</td>
<td>switch (config router bgp 100)# client-to-client reflection</td>
</tr>
<tr>
<td>Related Commands</td>
<td>N/A</td>
</tr>
<tr>
<td>Note</td>
<td>N/A</td>
</tr>
</tbody>
</table>
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.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>external</th>
<th>Administrative distance for external BGP routes. Range: 1-255.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>internal</td>
<td>Administrative distance for internal BGP routes. Range: 1-255.</td>
</tr>
<tr>
<td></td>
<td>local</td>
<td>Administrative distance for local BGP routes. Range: 1-255.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Default</th>
<th>external: 200</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>internal: 200</td>
</tr>
<tr>
<td></td>
<td>local: 200</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Configuration Mode</th>
<th>Config Router BGP</th>
</tr>
</thead>
<tbody>
<tr>
<td>History</td>
<td>3.3.5006</td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
</tr>
</tbody>
</table>

Example

switch (config router bgp 100)# distance 10 20 30

Related Commands

N/A

Note

- Routers use administrative distances to decide on a route when two protocols provide routing information to the same destination.
- Lower distance values correspond to higher reliability.
- Routes are external when learned from an external autonomous system.
- Routes are internal when learned from a peer in the local autonomous system.
- 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.
- BGP routing tables do not include routes with a distance of 255.
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.

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>300 seconds</td>
<td></td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Config Router BGP</td>
<td></td>
</tr>
<tr>
<td>History</td>
<td>3.4.0000</td>
<td></td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
<td></td>
</tr>
<tr>
<td>Example</td>
<td><code>switch (config router bgp 100)# graceful-restart stalepath-time 350</code></td>
<td></td>
</tr>
<tr>
<td>Related Commands</td>
<td>N/A</td>
<td></td>
</tr>
<tr>
<td>Note</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
## graceful-restart helper

```
graceful-restart helper
no graceful-restart helper
```

Enables BGP graceful restart helper mode on the switch for all BGP neighbors.
The no form of the command disables BGP graceful restart helper mode on the switch for all BGP neighbors.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>Graceful restart is enabled</td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Config Router BGP</td>
</tr>
<tr>
<td>History</td>
<td>3.4.0000</td>
</tr>
<tr>
<td></td>
<td>3.6.3004 Updated Note section</td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
</tr>
<tr>
<td>Example</td>
<td>switch (config router bgp 100) gracefull-restart helper</td>
</tr>
<tr>
<td>Related Commands</td>
<td>N/A</td>
</tr>
<tr>
<td>Note</td>
<td>When graceful restart helper mode is enabled, the switch retains routes from neighbors capable of graceful restart while those neighbors are restarting BGP</td>
</tr>
<tr>
<td></td>
<td>Individual neighbor configuration takes precedence over the global configuration</td>
</tr>
<tr>
<td></td>
<td>This parameter can only be configured when BGP is admin-down state</td>
</tr>
</tbody>
</table>
**maximum-paths**

`maximum-paths [ibgp] <maximum-path>`

Configures the maximum number of parallel eBGP/iBGP routes that the switch installs in the routing table.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>ibgp</th>
<th>Sets the configuration on the internal BGP.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>maximum-path</td>
<td>The number of routes to install to the routing table.</td>
</tr>
</tbody>
</table>

**Default**

1

**Configuration Mode**

Config Router BGP

**History**

3.3.5006

3.3.5200 Updated description and notes

**Role**

admin

**Example**

switch (config router bgp 100)# maximum-paths ibgp 10
switch (config router bgp 100)#

**Related Commands**

N/A

**Note**

- 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.
- The action is effective after BGP restart.
- 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.
**neighbor advertisement-interval**

```
 neighbor {<ip-address> | <peer-group-name>} advertisement-interval <delay>
 no neighbor {<ip-address> | <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.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip-address</td>
<td>A BGP peer IP address</td>
</tr>
<tr>
<td>peer-group-name</td>
<td>Peer group name</td>
</tr>
<tr>
<td>delay</td>
<td>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</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Default</th>
<th>30 seconds</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuration Mode</td>
<td>Config Router BGP</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>History</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.4.0000</td>
<td>First version</td>
</tr>
<tr>
<td>3.6.3004</td>
<td>Updated description of “delay” parameter</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Role</th>
<th>admin</th>
</tr>
</thead>
</table>

| Example | switch (config router bgp 100)# neighbor 10.10.10.10 advertisement-interval 90 |

<table>
<thead>
<tr>
<th>Related Commands</th>
<th></th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Note</th>
<th></th>
</tr>
</thead>
</table>
**neighbor allowas-in**

```
neighbor {<ip-address> | <peer-group-name>} allowas-in [number]
no neighbor {<ip-address> | <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.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip-address</td>
<td>A BGP peer IP address</td>
</tr>
<tr>
<td>peer-group-name</td>
<td>Peer group name</td>
</tr>
<tr>
<td>number</td>
<td>Number of switch’s (ASN) allowed in path</td>
</tr>
<tr>
<td></td>
<td>Range: 0-10 where “0” disables this function and</td>
</tr>
<tr>
<td></td>
<td>prevents the system from inheriting this param-</td>
</tr>
<tr>
<td></td>
<td>ter’s group configuration</td>
</tr>
</tbody>
</table>

**Default**

N/A

**Configuration Mode**

Config Router BGP

**History**

3.4.0000 First version

3.6.3004 Updated description of “number” parameter

**Role**

admin

**Example**

```
switch (config router bgp 100)# neighbor 10.10.10.10 allowas-in 2
```

**Related Commands**

- ip routing
- router bgp <as-number>

**Note**

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 {<ip-address> | <peer-group-name>} description <string>
no neighbor {<ip-address> | <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.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip-address</td>
<td>IP address of the neighbor</td>
</tr>
<tr>
<td>peer-group-name</td>
<td>Peer group name</td>
</tr>
<tr>
<td>string</td>
<td>Free string, up to 80 characters in length</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Default</th>
<th>No description</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Configuration Mode</th>
<th>Config Router BGP</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>History</th>
<th>First version</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.3.5006</td>
<td></td>
</tr>
<tr>
<td>3.3.5200</td>
<td>Updated example</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Role</th>
<th>admin</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Example</th>
<th><code>switch (config router bgp 100)# neighbor 10.10.10.10 description The next door neighbor</code></th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Related Commands</th>
<th>N/A</th>
</tr>
</thead>
</table>

| Note                | The peer description only appears in the show commands.                             |
neighbor ebgp-multihop

neighbor {<ip-address> | <peer-group-name>} ebgp-multihop [<ttl>]
no neighbor {<ip-address> | <peer-group-name>} ebgp-multihop

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.

**Syntax Description**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip-address</td>
<td>IP address of the BGP-speaking neighbor</td>
</tr>
<tr>
<td>peer-group-name</td>
<td>Peer group name</td>
</tr>
<tr>
<td>ttl</td>
<td>Time-to-live 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</td>
</tr>
</tbody>
</table>

**Default**
ttl: 1

**Configuration Mode**
Config Router BGP

**History**
- 3.3.5006 First version
- 3.3.5200 Updated default
- 3.6.3004 Updated description of “ttl” parameter

**Role**
admin

**Example**
switch (config router bgp 100)# neighbor 10.10.10.10 ebgp-multihop 5

**Related Commands**
ip routing
neighbor <ip-address> remote-as <as-number>

**Note**
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 {<ip-address> | <peer-group-name>} export-localpref <value>
no neighbor {<ip-address> | <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.

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip-address</td>
<td>IP address of the BGP-speaking neighbor</td>
</tr>
<tr>
<td>peer-group-name</td>
<td>Peer group name</td>
</tr>
<tr>
<td>value</td>
<td>Preference value</td>
</tr>
</tbody>
</table>

**Range:** 0-2147483647 where “100” configures the default, and prevents the system from inheriting this parameter’s group configuration

**Default**

100

**Configuration Mode**

Config Router BGP

**History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.4.0000</td>
<td>First version</td>
</tr>
<tr>
<td>3.6.3004</td>
<td>Updated description of “value” parameter</td>
</tr>
</tbody>
</table>

**Role**

admin

**Example**

```
switch (config router bgp 100)# neighbor 10.10.10.10 export-localpref 100
```

**Related Commands**

**Note**
**neighbor import-localpref**

```
neighbor {<ip-address> | <peer-group-name>} import-localpref <value>
no neighbor {<ip-address> | <peer-group-name>} import-localpref
```

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.

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip-address</td>
<td>IP address of the BGP-speaking neighbor</td>
</tr>
<tr>
<td>peer-group-name</td>
<td>Peer group name</td>
</tr>
<tr>
<td>value</td>
<td>Preference value</td>
</tr>
</tbody>
</table>

Range: 0-2147483647 where “100” configures the default, and prevents the system from inheriting this parameter’s group configuration

**Default**

100

**Configuration Mode**

Config Router BGP

**History**

- 3.4.0000: First version
- 3.6.3004: Updated description of “value” parameter

**Role**

admin

**Example**

```
switch (config router bgp 100)# neighbor 10.10.10.10 import-localpref 100
```

**Related Commands**

**Note**
**neighbor local-as**

```
neighbor {<ip-address> | <peer-group-name>} local-as <as-id> [no-prepend | replace-as]
no neighbor {<ip-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.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>ip-address</th>
<th>IP address of the BGP-speaking neighbor</th>
</tr>
</thead>
<tbody>
<tr>
<td>peer-group-name</td>
<td></td>
<td>Peer group name</td>
</tr>
<tr>
<td>as-id</td>
<td></td>
<td>Range: 0-4294967295 where “12000” configures the default, and prevents the system from inheriting this parameter’s group configuration</td>
</tr>
<tr>
<td>no-prepend</td>
<td></td>
<td>local-as number is not pre-pended to the routes received from external neighbors</td>
</tr>
<tr>
<td>replace-as</td>
<td></td>
<td>Prepends only the local autonomous system number (as configured with the IP address argument) to the AS path attribute</td>
</tr>
</tbody>
</table>

**Default**

12000

**Configuration Mode**

Config Router BGP

**History**

3.4.0000 First version
3.6.3004 Updated description of “as-id” parameter

**Role**

admin

**Example**

```
switch-e07c04 [standalone: master] (config router bgp 4) # neighbor 100.100.100.100 local-as 123
```

**Related Commands**

- `ip routing`
- `neighbor <ip-address> remote-as <as-number>`

**Note**

- This function allows the switch to appear as a member of a different autonomous system (AS) to external peers.
- To disable peering with the neighbor run the command `clear ip bgp`
neighbor maximum-prefix

neighbor {<ip-address> | <peer-group-name>} maximum-prefix <maximum> [warning-only]
no neighbor {<ip-address> | <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.

Syntax Description

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip-address</td>
<td>IP address of the BGP-speaking neighbor</td>
</tr>
<tr>
<td>peer-group-name</td>
<td>Peer group name</td>
</tr>
<tr>
<td>maximum</td>
<td>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</td>
</tr>
<tr>
<td>warning-only</td>
<td>Only generates a warning rather than disconnecting the neighbor</td>
</tr>
</tbody>
</table>

Default

12000

Configuration Mode

Config Router BGP

History

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.4.0000</td>
<td>First version</td>
</tr>
<tr>
<td>3.6.3004</td>
<td>Updated description of “maximum” parameter</td>
</tr>
</tbody>
</table>

Role

admin

Example

switch (config router bgp 100)# neighbor 10.10.10.10 maximum-prefix 12000 warning-only

Related Commands

ip routing
neighbor <ip-address> remote-as <as-number>

Note
**neighbor next-hop-peer**

```
neighbor {<ip-address> | <peer-group-name>} next-hop-peer [disable]
no neighbor {<ip-address> | <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.

### Syntax Description

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip-address</td>
<td>IP address of the neighbor</td>
</tr>
<tr>
<td>peer-group-name</td>
<td>Peer group name</td>
</tr>
<tr>
<td>disable</td>
<td>Disables this function and prevents the system from inheriting this parameter’s group configuration</td>
</tr>
</tbody>
</table>

### Default

```
no next-hop-peer
```

### Configuration Mode

Config Router BGP

### History

- **3.3.5006**
  - Added “disable” parameter

### Role

admin

### Example

```
switch (config router bgp 100)# neighbor 10.10.10.10 next-hop-peer
```

### Related Commands

- This command overrides the next hop for all routes received from this neighbor or peer group

### Note

This command overrides the next hop for all routes received from this neighbor or peer group.
neighbor next-hop-self

neighbor {<ip-address> | <peer-group-name>} next-hop-self [disable]
no neighbor {<ip-address> | <peer-group-name>} next-hop-self

Configures the IP address of the router as the next hop address in routes advertised to the specific neighbor.
The no form of the command resets this parameter to its default.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>ip-address</th>
<th>IP address of the neighbor</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>peer-group-name</td>
<td>Peer group name</td>
</tr>
<tr>
<td></td>
<td>disable</td>
<td>Enables this function and prevents the system from inheriting this parameter’s group configuration</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Default</th>
<th>no next-hop-self</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Configuration Mode</th>
<th>Config Router BGP</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>History</th>
<th>3.3.5006</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Role</th>
<th>admin</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Example</th>
<th>switch (config router bgp 100)# neighbor 10.10.10.10 next-hop-self</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Related Commands</th>
<th>neighbor &lt;ip-address&gt; remote-as &lt;as-number&gt;</th>
</tr>
</thead>
</table>

| Note | • This function is used in networks where BGP neighbors do not directly access all other neighbors on the same subnet.  
• In the default state, the next hop is generated based on the IP address and the present next hop in the route information. |
neighbor password

neighbor {<ip-address> | <peer-group-name>} password [<encryption>] <string>
no neighbor {<ip-address> | <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.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>ip-address</th>
<th>IP address of the neighbor</th>
</tr>
</thead>
<tbody>
<tr>
<td>peer-group-name</td>
<td>Peer group name</td>
<td></td>
</tr>
<tr>
<td>encryption</td>
<td>Possible values:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• no parameter – clear text</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• 0 – clear text</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• 7 – obfuscated</td>
<td></td>
</tr>
<tr>
<td>string</td>
<td>Up to 8 bytes in length</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Default</th>
<th>no neighbor password</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuration Mode</td>
<td>Config Router BGP</td>
</tr>
<tr>
<td>History</td>
<td>3.4.0000 First version</td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
</tr>
<tr>
<td>Example</td>
<td><code>switch (config router bgp 100)# neighbor 10.10.10.10 password 7 admin123</code></td>
</tr>
<tr>
<td>Related Commands</td>
<td></td>
</tr>
</tbody>
</table>

Note

- Peers must use the same password to ensure communication.
- `neighbor <ip-address> password 7 <password>'` can only accept data that was created using 'show config'.
- 'show config' will never show the clear-test password, it will always be obfuscated (and thus displayed using the 'password 7' syntax).
- Router BGP neighbor password cannot be set when enabling secure mode.
- Router BGP peer-group password cannot be set when enabling with secure mode.
neighbor no-password

neighbor {<ip-address> | <peer-group-name>} no-password

Disables authentication for peer without inheritance.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
<th>Default</th>
<th>Configuration Mode</th>
<th>History</th>
<th>Role</th>
<th>Example</th>
<th>Related Commands</th>
<th>Note</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip-address</td>
<td>IP address of the neighbor</td>
<td>N/A</td>
<td>Config Router BGP</td>
<td>3.6.3004</td>
<td>admin</td>
<td>switch (config router bgp 100)# neighbor 10.10.10.10 no-password</td>
<td>neighbor password</td>
<td></td>
</tr>
</tbody>
</table>
### neighbor peer-group

1. `neighbor {<ip-address>} peer-group <peer-group-name>`
2. `neighbor {<peer-group-name>} peer-group`
3. `no neighbor {<ip-address>} 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

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>ip-address</th>
<th>IP address of the neighbor</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>peer-group-name</td>
<td>Peer group name</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Default</th>
<th>N/A</th>
</tr>
</thead>
</table>

**Configuration Mode**: Config Router BGP

**History**

- 3.4.0000 | First version
- 3.6.3004 | Added notes

**Role**: admin

**Example**

```plaintext
switch (config router bgp 100)# neighbor groupA peer-group
switch (config router bgp 100)# neighbor 1.2.3.4 peer-group groupA
```
Related Commands

Note

- 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.
- Settings applied to an individual neighbor in the peer group override group settings.
- 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.
- When a neighbor is removed from a peer group, the neighbor retains the configuration inherited from the peer group.
- Router BGP peer-group password cannot be set when enabling with secure mode.
- 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).
- A group must already exist before a node is configured to use it.
- Any configuration change on a group affects each of the peers inheriting this specific parameter from the group only after undergoing admin state toggle.
neighbor remote-as

neighbor {<ip-address>} remote-as <as-number>
no neighbor {<ip-address>} 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.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>ip-address</th>
<th>A BGP peer IP address</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>peer-group-name</td>
<td>Peer group name</td>
</tr>
<tr>
<td></td>
<td>as-number</td>
<td>The BGP peer as-number. Range: 1-65535.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Default</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuration Mode</td>
<td>Config Router BGP</td>
</tr>
<tr>
<td>History</td>
<td>3.3.5006</td>
</tr>
<tr>
<td></td>
<td>3.3.5200</td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
</tr>
<tr>
<td>Example</td>
<td>switch (config router bgp 100)# neighbor 10.10.10.10 remote-as 200</td>
</tr>
<tr>
<td></td>
<td>switch (config router bgp 100)#</td>
</tr>
<tr>
<td>Related Commands</td>
<td>ip routing</td>
</tr>
<tr>
<td></td>
<td>router bgp &lt;as-number&gt;</td>
</tr>
<tr>
<td>Note</td>
<td>Neighbors from the same AS as the router are considered as iBGP peers, and neighbors from other ASs are considered eBGP peers.</td>
</tr>
</tbody>
</table>
**neighbor remove-private-as**

`neighbor {<ip-address> | <peer-group-name>} remove-private-as [disable]`

no neighbor {<ip-address> | <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.

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip-address</td>
<td>A BGP peer IP address</td>
</tr>
<tr>
<td>peer-group-name</td>
<td>Peer group name</td>
</tr>
<tr>
<td>disable</td>
<td>Preserves private AS numbers for the specified peer and prevents the system from inheriting this parameter’s group configuration</td>
</tr>
</tbody>
</table>

**Default**

N/A

**Configuration Mode**

Config Router BGP

**History**

3.4.0000 First version

**Role**

admin

**Example**

```
switch (config router bgp 100)# neighbor 10.10.10.10 remove-private-as
switch (config router bgp 100)#
```

**Related Commands**

- ip routing
- router bgp <as-number>

**Note**

- This can only be used with external BGP (eBGP) peers.
- If the update has only private AS numbers in the AS path, BGP removes these numbers.
- 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.
- If the AS path contains the AS number of the eBGP neighbor, BGP does not remove the private AS number.
- If the AS path contains confederations, BGP removes the private AS numbers only if they come after the confederation portion of the AS path.
**neighbor route-map**

```
neighbor {<ip-address> | <peer-group-name>} route-map <route-map-name> [in | out]
no neighbor {<ip-address> | <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.

**Syntax Description**

- **ip-address**: 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

**Default**

N/A

**Configuration Mode**

Config Router BGP

**History**

- 3.3.5006: First version
- 3.3.5200: Updated notes and default
- 3.4.1100: Added “out” parameter
- 3.6.3004: Added note

**Role**

admin

**Example**

```
switch (config router bgp 100)# neighbor 10.10.10.10 route-map MyRouteMap in
```

**Related Commands**

- `neighbor <ip-address> remote-as <as-number>`
- `route-map <map-name> [deny | permit] [sequence-number]`
- `clear ip bgp {<ip-address> | all}`

**Note**

- Only one inbound route-map can be applied to a given neighbor
- If a new route-map is applied to a neighbor, it replaces the previous route map
- Changing a route-map only takes effect on routes received or sent after the change
- A route-map must already exist before a node is configured to use it
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.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>ip-address</th>
<th>IP address of the neighbor</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>peer-group-name</td>
<td>Peer group name</td>
</tr>
</tbody>
</table>

**Default**

N/A

**Configuration Mode**

Config Router BGP

**History**

3.6.3004

**Role**

admin

**Example**

```
switch (config router bgp 100)# neighbor 10.10.10.10 no-route-map
```

**Related Commands**

- `neighbor <ip-address> remote-as <as-number>`
- `route-map <map-name> [deny | permit] [sequence-number]`

**Note**

**neighbor route-reflector-client**

```
neighbor {<ip-address> | <peer-group-name>} route-reflector-client [disable]
no neighbor {<ip-address> | <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.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>ip-address</th>
<th>IP address of the neighbor.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>peer-group-name</td>
<td>Peer group name</td>
</tr>
<tr>
<td></td>
<td>disable</td>
<td>Unsets neighbor as route reflector client and prevents the system from inheriting this parameter’s group configuration</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Default</th>
<th>N/A</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Configuration Mode</th>
<th>Config Router BGP</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>History</th>
<th>3.3.5006</th>
<th>First version</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>3.3.5200</td>
<td>Updated notes and default</td>
</tr>
<tr>
<td></td>
<td>3.6.3004</td>
<td>Added “disable” parameter</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Role</th>
<th>admin</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Example</th>
<th>switch (config router bgp 100)# neighbor 10.10.10.10 route-reflector-client</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Related Commands</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Note</th>
<th></th>
</tr>
</thead>
</table>
neighbor send-community

neighbor {<ip-address> | <peer-group-name>} send-community [extended] [disable]
no neighbor {<ip-address> | <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.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip-address</td>
<td>IP address of the neighbor</td>
</tr>
<tr>
<td>peer-group-name</td>
<td>Peer group name</td>
</tr>
<tr>
<td>extended</td>
<td>Sends extended community attributes to neighbor</td>
</tr>
<tr>
<td>disable</td>
<td>Disables sending community attributes for the specified peer and prevents the system from inheriting this parameter’s group configuration</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Default</th>
<th>Enabled</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuration Mode</td>
<td>Config Router BGP</td>
</tr>
<tr>
<td>History</td>
<td>3.4.0000 First version</td>
</tr>
<tr>
<td></td>
<td>3.6.3004 Added “disable” parameter</td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
</tr>
<tr>
<td>Example</td>
<td>switch (config router bgp 100)# neighbor 10.10.10.10 send-community</td>
</tr>
<tr>
<td>Related Commands</td>
<td>N/A</td>
</tr>
<tr>
<td>Note</td>
<td></td>
</tr>
</tbody>
</table>
neighbor shutdown

neighbor {<ip-address> | <peer-group-name>} shutdown [disable]
no neighbor {<ip-address> | <peer-group-name>} shutdown

Disables BGP neighbor gracefully.
The no form of the command enables BGP neighbor.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip-address</td>
<td>IP address of the neighbor</td>
</tr>
<tr>
<td>peer-group-name</td>
<td>Peer group name</td>
</tr>
<tr>
<td>disable</td>
<td>Enables BGP neighbor and prevents the system from inheriting this parameter’s group configuration</td>
</tr>
</tbody>
</table>

Default: Enabled

Configuration Mode: Config Router BGP

History:
3.3.5006 First version
3.3.5200 Updated note

Role: admin

Example:
switch (config router bgp 100)# neighbor 10.10.10.10 shutdown

Related Commands: N/A

Note:
- Disabling a neighbor terminates all its active sessions and removes associated routing information
- A group’s shutdown immediately impacts every peer in this group, making them inherit this parameter
neighbor timers

neighbor {<ip-address> | <peer-group-name>} timers <keep-alive> <hold-time>
no neighbor {<ip-address> | <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.

Syntax Description

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip-address</td>
<td>IP address of the neighbor.</td>
</tr>
<tr>
<td>peer-group-name</td>
<td>Peer group name</td>
</tr>
<tr>
<td>keep-alive</td>
<td>The period between the transmission of consecutive keep-alive messages</td>
</tr>
<tr>
<td></td>
<td>• Range: 1-3600 seconds</td>
</tr>
<tr>
<td></td>
<td>• “0” means that keepalive is not sent and the connection does not expire</td>
</tr>
<tr>
<td></td>
<td>• Explicitly configuring the default, “60”, prevents the system from inheriting this parameter’s group configuration</td>
</tr>
<tr>
<td>hold-time</td>
<td>The period the switch waits for a keepalive or update message before it disables peering</td>
</tr>
<tr>
<td></td>
<td>• Range: 3-7200 seconds</td>
</tr>
<tr>
<td></td>
<td>• “0” means that keepalive is not sent and the connection does not expire</td>
</tr>
<tr>
<td></td>
<td>• Explicitly configuring the default, “180”, prevents the system from inheriting this parameter’s group configuration</td>
</tr>
</tbody>
</table>

Default

keep-alive: 60 seconds
hold-time: 180 seconds

Configuration Mode

Config Router BGP

History

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.3.5006</td>
<td>First version</td>
</tr>
<tr>
<td>3.3.5200</td>
<td>Updated description</td>
</tr>
<tr>
<td>3.6.3004</td>
<td>Updated “hold-time” and “keep-alive” parameter’s syntax description</td>
</tr>
</tbody>
</table>

Role

admin

Example

switch (config router bgp 100)# neighbor 10.10.10.10 timers 65 195

Related Commands

neighbor <ip-address> remote-as <as-number>

Note

Hold time must be at least 3 seconds and should be three times longer than the keep-alive setting.
**neighbor transport connection-mode passive**

```bash
neighbor {<ip-address> | <peer-group-name>} transport connection-mode passive [disable]
no neighbor {<ip-address> | <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.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>ip-address</th>
<th>IP address of the neighbor</th>
</tr>
</thead>
<tbody>
<tr>
<td>peer-group-name</td>
<td>Peer group name</td>
<td></td>
</tr>
<tr>
<td>disable</td>
<td>Sets the specified BGP neighbor or peer group to active connection mode and prevents the system from inheriting this parameter’s group configuration</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Default</th>
<th>TCP sessions initiated</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuration Mode</td>
<td>Config Router BGP</td>
</tr>
<tr>
<td>History</td>
<td>3.4.0000</td>
</tr>
<tr>
<td></td>
<td>First version</td>
</tr>
<tr>
<td></td>
<td>3.6.3004</td>
</tr>
<tr>
<td></td>
<td>Added “disable” parameter</td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
</tr>
</tbody>
</table>

**Example**

```bash
switch (config router bgp 100)# neighbor 10.10.10.10 transport connection-mode passive
```

**Related Commands**

- When the peer’s transport connection mode is set to passive, it accepts TCP connections for BGP, but does not initiate them
- BGP peers in active mode can both accept and initiate TCP connections for BGP

**Note**
neighbor update-source

neighbor <ip-address> update-source {ethernet <slot/port> | loopback <number> | port-channel <number> | vlan <vlan-id>}
no neighbor <ip-address> 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.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip-address</td>
<td>IP address of the neighbor.</td>
</tr>
<tr>
<td>ethernet &lt;slot/port&gt;</td>
<td>Ethernet interface.</td>
</tr>
<tr>
<td>loopback &lt;number&gt;</td>
<td>Loopback interface number.</td>
</tr>
<tr>
<td>port-channel &lt;number&gt;</td>
<td>LAG interface. Range is 1-4094.</td>
</tr>
</tbody>
</table>

| Default | BGP uses best local address |
| Configuration Mode | Config Router BGP |
| History | 3.3.5006 First version |
| | 3.3.5200 Updated example |
| Role | admin |
| Example | switch (config router bgp 100)# neighbor 10.10.10.2 update-source vlan 10 |
| Related Commands | N/A |
| Note | |

Rev 4.60 Mellanox Technologies Confidential 1099
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.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>BGP uses best local address</td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Config Router BGP</td>
</tr>
<tr>
<td>History</td>
<td>3.6.3004 First version</td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
</tr>
<tr>
<td>Example</td>
<td>switch (config router bgp 100)# neighbor 10.10.10.2 no-update-source</td>
</tr>
<tr>
<td>Related Commands</td>
<td>N/A</td>
</tr>
<tr>
<td>Note</td>
<td></td>
</tr>
</tbody>
</table>
**neighbor weight**

```
neighbor {<ip-address> | <peer-group-name>} weight <value>
no neighbor {<ip-address> | <peer-group-name>} weight
```

Assigns a weight attribute to paths from the specified neighbor.
The no form of the command resets to default values.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>ip-address</th>
<th>IP address of the neighbor</th>
</tr>
</thead>
<tbody>
<tr>
<td>peer-group-name</td>
<td>peer group name</td>
<td></td>
</tr>
<tr>
<td>value</td>
<td>Weight value</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Range: 1-65535</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Explicitly configuring a default value prevents the system from inheriting this parameter’s group configuration</td>
<td></td>
</tr>
</tbody>
</table>

**Default**
Value is 32768 for router-originated paths and 0 for routes received through BGP

**Configuration Mode**
Config Router BGP

**History**
3.4.0000 First version

**Role**
admin

**Example**
```
switch (config router bgp 100)# neighbor 10.10.10.10 weight 100
```

**Related Commands**
N/A

**Note**
- Weight values set through route map commands have precedence over neighbor weight command values.
- Other attributes are used only when all paths to the prefix have the same weight.
- A path’s BGP weight is also configurable through route maps.
- When multiple paths to a destination prefix exist, the best-path selection algorithm prefers the path with the highest weight.
- Weight is the first parameter that the BGP best-path selection algorithm considers.
### network

**Syntax**

```
network <ip-prefix> <length> [route-map-name]
no network <ip-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.

#### Syntax Description

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip-prefix</td>
<td>A string that specific route map is assigned to the network.</td>
</tr>
<tr>
<td>length</td>
<td>/24 or 255.255.255.0 format.</td>
</tr>
<tr>
<td>route-map-name</td>
<td>The name of a route-map which is used to set the route’s attributes when it is advertised.</td>
</tr>
</tbody>
</table>

#### Default

N/A

#### Configuration Mode

Config Router BGP

#### History

- 3.3.5006: First version
- 3.3.5200: Updated description, syntax description and notes

#### Role

admin

#### Example

```
switch (config router bgp 100)# network 10.10.0 /24 routemap
```

#### Related Commands

- `network` command

#### Note

- The parameters “ip-prefix” and “length” specify the route destination
- 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)
- This command cannot be used with route-maps
**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.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>connected</th>
<th>Redistributes the direct routes</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>static</td>
<td>Redistributes the user-defined (static) route</td>
</tr>
<tr>
<td></td>
<td>ospf</td>
<td>Redistributes all routes learned by OSPF protocol</td>
</tr>
<tr>
<td></td>
<td>ospf-internal</td>
<td>Redistributes all OSPF-learned routes which are marked as internal</td>
</tr>
<tr>
<td></td>
<td>ospf-external</td>
<td>Redistributes all OSPF-learned routes which are marked as external</td>
</tr>
</tbody>
</table>

**Default**
No redistribution

**Configuration Mode**
Config Router BGP

**History**
3.2.1000

**Role**
admin

**Example**
```
switch (config router bgp 100)# redistribute ospf
```

**Related Commands**
N/A

**Note**
- Multiple redistribution options can be applied
- This command cannot be used with route-maps
**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.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip-address</td>
<td>IP Address identified the router ID</td>
</tr>
<tr>
<td>force</td>
<td>Applies configuration while BGP is admin-up</td>
</tr>
</tbody>
</table>

**Default**

The Router ID is dynamically elected (no router-id).
- If a loopback interface is configured, the router ID is set to the IP address of the loopback interface.
- If multiple loopback interfaces are configured, the router ID is set to the IP address of the loopback interface with the highest IP address.
- If no loopback interface is configured, the router ID is set to the highest IP address on a physical interface.

**Configuration Mode**

Config Router BGP

**History**

- 3.3.5006
- 3.6.3004 Added “force” parameter

**Role**

admin

**Example**

```
switch (config router bgp 100)# router-id 10.10.10.10
```

**Related Commands**

**Note**

The IP address configured identifies the BGP speaker. The command triggers an automatic notification and session reset for the BGP neighbors.
### show ip bgp

`show ip bgp [<ip-address> <mask> [detail | longer-prefixes [detail]]]`

Displays information about the BGP routes table (RIB).

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip-address</td>
<td>IP address (e.g. 172.3.12.4).</td>
</tr>
<tr>
<td>mask</td>
<td>Netmask (e.g. /24 or 255.255.255.0).</td>
</tr>
<tr>
<td>detail</td>
<td>Displays detailed information about a subset of the bgp learned routes.</td>
</tr>
<tr>
<td>longer-prefixes</td>
<td>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.</td>
</tr>
</tbody>
</table>

| Default             | N/A |
| Configuration Mode  | Any Command Mode |
| History             | 3.3.5200 |
| Role                | admin |

#### Example

```
switch (config) # show ip bgp
BGP table version is 100, local router ID is 16.0.1.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
              r RIB-failure, S Stale, m multipath, b backup-path, x best-external
Origin codes: i - IGP, e - EGP, ? - incomplete
              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

   Network      Next Hop    Metric LocPrf Weight Path
              20.20.20.0/24 2.2.2.2    0 2 20  e
              40.40.40.0/24 4.4.4.4    0 4 40  i
              100.100.90.32/28 2.2.2.2 0 2 100  i
              100.100.100.0/24 4.4.4.4 0 4 50  i
```

#### Related Commands

N/A

#### Note

N/A
### show ip bgp community

**show ip bgp community <comm1> <comm2> ... <commn> [exact] [detail]**

Displays information about the BGP routes (RIB) filtered according to communities.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>N/A</td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Any Command Mode</td>
</tr>
<tr>
<td>History</td>
<td>3.4.0000</td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
</tr>
</tbody>
</table>

**Example**

```
switch (config) # show ip bgp community 100:1
BGP table version is 8, local router ID is 3.5.7.4
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
    r RIB-failure, S Stale, m multipath, b backup-path, x best-external
Origin codes: i - IGP, e - EGP, ? - incomplete

<table>
<thead>
<tr>
<th>Network</th>
<th>Next Hop</th>
<th>Metric</th>
<th>LocPrf</th>
<th>Weight</th>
</tr>
</thead>
<tbody>
<tr>
<td>*&gt; 3.4.3.11/32</td>
<td>0.0.0.0</td>
<td>0</td>
<td>0</td>
<td>32768</td>
</tr>
<tr>
<td>*&gt; 3.5.7.88/32</td>
<td>0.0.0.0</td>
<td>0</td>
<td>0</td>
<td>32768</td>
</tr>
<tr>
<td>*&gt; 3.5.7.99/32</td>
<td>0.0.0.0</td>
<td>0</td>
<td>0</td>
<td>32768</td>
</tr>
</tbody>
</table>
```

```
switch (config) # show ip bgp community 100:1 exact
BGP table version is 8, local router ID is 3.5.7.4
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
    r RIB-failure, S Stale, m multipath, b backup-path, x best-external
Origin codes: i - IGP, e - EGP, ? - incomplete

<table>
<thead>
<tr>
<th>Network</th>
<th>Next Hop</th>
<th>Metric</th>
<th>LocPrf</th>
<th>Weight</th>
</tr>
</thead>
<tbody>
<tr>
<td>*&gt; 3.4.3.11/32</td>
<td>0.0.0.0</td>
<td>0</td>
<td>0</td>
<td>32768</td>
</tr>
<tr>
<td>*&gt; 3.5.7.99/32</td>
<td>0.0.0.0</td>
<td>0</td>
<td>0</td>
<td>32768</td>
</tr>
</tbody>
</table>
```

**Related Commands**

| N/A |

**Note**
show ip bgp neighbors

show ip bgp neighbors

Displays summaries information about all BGP neighbors.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>N/A</td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Any Command Mode</td>
</tr>
<tr>
<td>History</td>
<td>3.3.5200</td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
</tr>
</tbody>
</table>

Example

```
switch (config) # show ip bgp neighbors 3.5.7.5 received
BGP table version is 66, local router ID is 3.5.7.4
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
    r RIB-failure, S Stale, m multipath, b backup-path, x best-external
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
   *>  3.5.7.128/32       3.5.7.5                  7        100          0 5 i
   *>  100.0.30.0/24      3.5.7.5                  0        100          0 5 i
   *>  10.20.30.0/24      3.5.7.5                  0        100          0 5 12 i
```

Related Commands

N/A

Note

N/A
**show ip bgp neighbors <ip>**

**show ip bgp neighbors <ip-address>**

Displays BGP summary information.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>ip-address</th>
<th>Neighbor IP address.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>N/A</td>
<td></td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Any Command Mode</td>
<td></td>
</tr>
<tr>
<td>History</td>
<td>3.3.5200</td>
<td></td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
<td></td>
</tr>
</tbody>
</table>

**Example**

```
switch (config) # show ip bgp neighbors 3.5.7.5 received
BGP table version is 66, local router ID is 3.5.7.4
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
    r RIB-failure, S Stale, m multipath, b backup-path, x best-external
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 1
*>  3.5.7.128/32       3.5.7.5                  7        100          0 5 1
*>  100.0.30.0/24      3.5.7.5                  0        100          0 5 1
*>  10.20.30.0/24      3.5.7.5                  0        100          0 5 12 1
```

**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.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>ip-address</th>
<th>Neighbor IP address</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>longer-prefixes</td>
<td>Displays the routes to the specified destination and any routes to a more specific destination. (Only available if both IP and mask are specified.)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Default</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuration Mode</td>
<td>Any Command Mode</td>
</tr>
<tr>
<td>History</td>
<td>3.3.5200</td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
</tr>
<tr>
<td>Example</td>
<td></td>
</tr>
<tr>
<td>Related Commands</td>
<td>N/A</td>
</tr>
<tr>
<td>Note</td>
<td></td>
</tr>
</tbody>
</table>

Related Commands

Note
**show ip bgp paths**

**Syntax Description**

Displays summary of all AS paths.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>N/A</td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Any Command Mode</td>
</tr>
<tr>
<td>History</td>
<td>3.3.5200</td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
</tr>
</tbody>
</table>

**Example**

```
switch (config) # show ip bgp paths
Refcount  Metric  Path
1         0        4 50 100
1         0        2 50 100
1         0        4 40
1         0        12 50 100
1         0        2
1         0        2 20
switch (config) #
```

**Related Commands**

N/A

**Note**
show ip bgp peer-group

show ip bgp peer-group [<peer-group-name>]

Displays information about peer groups.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>peer-group-name</th>
<th>Displays information about a specific peer-group.</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Default</th>
<th>N/A</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Configuration Mode</th>
<th>Any Command Mode</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>History</th>
<th>3.4.0000</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Role</th>
<th>admin</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Example</th>
</tr>
</thead>
</table>
| switch (config) # show ip bgp peer-group
BGP Peer-group [grpA]:
  Hold time: 1, Keep-alive: 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, Keep-alive: 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, Keep-alive: 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) # |
<table>
<thead>
<tr>
<th>Related Commands</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Note</td>
<td></td>
</tr>
</tbody>
</table>
show ip bgp summary

Displays BGP summary information.

**Syntax Description**  
N/A

**Default**  
N/A

**Configuration Mode**  
Any Command Mode

**History**  
3.3.5200

**Role**  
admin

**Example**

```
switch (config) # show ip bgp summary
BGP router identifier 3.5.7.4, local AS number 4
BGP table version is 70, main routing table version 70
8 network entries using 2176 bytes of memory
4 path entries using 1088 bytes of memory
4 BGP path attribute entries using 256 bytes of memory
0 multipath network entries and 0 multipath paths
4 BGP community entries using 64 bytes of memory
0 received paths for inbound soft reconfiguration
BGP using 26308 total bytes of memory
Dampening disabled. 0 history paths, 0 dampened paths
BGP activity 37/8 prefixes, 37/4 paths
Neighbor     V  AS MsgRcvd MsgSent  TblVer  InQ OutQ Up/Down State/PfxRcd
3.4.3.7       4  7    3     9     70     0     0 0:00:00:48 ESTABLISHED
3.5.7.5       0  5    0     0     0       0     0 0:00:01:54 CONNECT
100.100.100.100 0 100    0     0     0     0     0 0 Never
```

**Related Commands**  
N/A

**Note**  
N/A
6.3.5  IP AS-Path Access-List

6.3.5.1  Commands

**ip as-path access-list**

```plaintext
ip as-path access-list <list-name> {permit | deny} <reg-exp> [any | egp | igp | 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.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>list-name</td>
<td>The name for the access 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>
<tr>
<td>reg-exp</td>
<td>Regular expression that is used to specify a pattern to match against an input string.</td>
</tr>
<tr>
<td>any</td>
<td>Any route type</td>
</tr>
<tr>
<td>egp</td>
<td>External BGP routes</td>
</tr>
<tr>
<td>igp</td>
<td>Internal BGP routes</td>
</tr>
<tr>
<td>incomplete</td>
<td>Routes marked as “Incomplete”</td>
</tr>
</tbody>
</table>

Default: N/A

Configuration Mode: Config

History: 3.4.0000

Role: admin

Example:
```
switch (config)# ip as-path access-list mylist permit
switch (config)#
```

Related Commands: N/A

Note: 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

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>list-name</th>
<th>Displays a specific prefix-list.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>N/A</td>
<td></td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Config</td>
<td></td>
</tr>
<tr>
<td>History</td>
<td>3.4.0000</td>
<td></td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
<td></td>
</tr>
</tbody>
</table>

**Example**

```
switch (config)# show ip as-path access-list mylist
```

**Related Commands**

N/A

**Note**
6.3.6 IP Community-List

6.3.6.1 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.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<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>
<tr>
<td>list-of-communities</td>
<td>List of standard communities:</td>
</tr>
<tr>
<td></td>
<td>• <a href="">aa:nn</a></td>
</tr>
<tr>
<td></td>
<td>• &lt;number&gt;</td>
</tr>
<tr>
<td></td>
<td>• internet</td>
</tr>
<tr>
<td></td>
<td>• local-AS</td>
</tr>
<tr>
<td></td>
<td>• no-advertise</td>
</tr>
<tr>
<td></td>
<td>• no-export</td>
</tr>
</tbody>
</table>

| Default          | N/A          |
| Configuration Mode | Config      |
| History          | 3.4.0000     |
| Role             | admin        |
| Example          | `switch (config)# ip community-list standard mycommunity permit 1:2 3:4` |
| Related Commands | N/A          |
| Note             | 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>
o 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.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>list-name</th>
<th>Configures a named standard community list.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>permit</td>
<td>Permits access for a matching condition.</td>
</tr>
<tr>
<td></td>
<td>deny</td>
<td>Denies access for a matching condition.</td>
</tr>
<tr>
<td></td>
<td>reg-exp</td>
<td>Regular expression that is used to specify a pattern to match against an input string.</td>
</tr>
</tbody>
</table>

Default: N/A
Configuration Mode: Config
History: 3.4.0000
Role: admin

Example:
switch (config)# ip community-list expanded mycommunity permit 1:[0-9]+  

Related Commands: N/A

Note: 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

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>community-list-name</th>
<th>An optional parameter to display only the specified list</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>N/A</td>
<td></td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Config</td>
<td></td>
</tr>
<tr>
<td>History</td>
<td>3.4.0000</td>
<td></td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
<td></td>
</tr>
<tr>
<td>Example</td>
<td>switch (config)# show ip community-list mycommunity</td>
<td></td>
</tr>
<tr>
<td>Related Commands</td>
<td>N/A</td>
<td></td>
</tr>
<tr>
<td>Note</td>
<td>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.</td>
<td></td>
</tr>
</tbody>
</table>
6.4 Policy Rules

6.4.1 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 1102 or “redistribute” on page 1103.
### 6.4.1.1 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.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>name</td>
<td>Name of the route-map</td>
</tr>
<tr>
<td>deny</td>
<td>permit</td>
</tr>
<tr>
<td>sequence-number</td>
<td>Sequence number for a route-map specific record</td>
</tr>
</tbody>
</table>

**Default**

N/A

**Configuration Mode**

Config

**History**

3.3.5006

3.3.5200 Updated notes

**Role**

admin

**Example**

```
switch (config) # route-map mymap permit 1200
switch (config route-map mymap permit 1200)#
```

**Related Commands**

N/A

**Note**

- All changes in a the route map configuration mode become pending until the end of the route-map session.
- If not configured, deny | permit is configured as permit.
- If not configured, sequence-number default value is 10.
**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.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>sequence-number</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>N/A</td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Config Route Map</td>
</tr>
<tr>
<td>History</td>
<td>3.3.5006</td>
</tr>
<tr>
<td></td>
<td>First version</td>
</tr>
<tr>
<td></td>
<td>3.3.5200</td>
</tr>
<tr>
<td></td>
<td>Updated example</td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
</tr>
</tbody>
</table>

**Example**

```
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)#
```
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**

**Syntax Description**

N/A

**Default**

N/A

**Configuration Mode**

Config Route Map

**History**

3.3.5006 First version

3.3.5200 Updated example

**Role**

admin

**Example**

```
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)#
```

**Related Commands**

N/A

**Note**
exit

exit

Saves pending route map clause changes to running-config and returns to global configuration mode.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>N/A</td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Config Route Map</td>
</tr>
<tr>
<td>History</td>
<td>3.3.5006</td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
</tr>
</tbody>
</table>

**Example**

```
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
```

**Related Commands**

N/A

**Note**
### 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.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>number</th>
<th>Autonomous system number to check.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>N/A</td>
<td></td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Config Route Map</td>
<td></td>
</tr>
<tr>
<td>History</td>
<td>3.3.5006</td>
<td></td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
<td></td>
</tr>
</tbody>
</table>
| Example            | switch (config route-map mymap permit 10)# match as-number 40  
switch (config route-map mymap permit 10)# |       |
| Related Commands   | N/A    |                                     |
| Note               | • 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.  
• 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.  
• If all clauses fail to permit or deny the route, the route is denied. |                   |
**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.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>number</th>
<th>Autonomous system number to check.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>N/A</td>
<td></td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Config Route Map</td>
<td></td>
</tr>
<tr>
<td>History</td>
<td>3.3.5006</td>
<td></td>
</tr>
<tr>
<td></td>
<td>3.6.3004</td>
<td>Added note</td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
<td></td>
</tr>
<tr>
<td>Example</td>
<td>switch (config route-map mymap permit 10)# match as-path my-list</td>
<td></td>
</tr>
<tr>
<td>Related Commands</td>
<td>N/A</td>
<td></td>
</tr>
</tbody>
</table>
| Note               | • 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  
• 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  
• If all clauses fail to permit or deny the route, the route is denied  
• An as-path-list must already exist before a node is configured to use it |
**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.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>list of communities</th>
<th>List of standard communities:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>• <a href="">aa:nn</a></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• &lt;number&gt;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• internet</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• local-AS</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• no-advertise</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• no-export</td>
</tr>
</tbody>
</table>

| exact-match | Creates a route map clause entry that matches the route’s communities exactly. |

<table>
<thead>
<tr>
<th>Default</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuration Mode</td>
<td>Config Route Map</td>
</tr>
<tr>
<td>History</td>
<td>3.3.5006</td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
</tr>
<tr>
<td>Example</td>
<td><code>switch (config route-map mymap permit 10)# match community 1:100 3:52</code></td>
</tr>
<tr>
<td>Related Commands</td>
<td>N/A</td>
</tr>
</tbody>
</table>

**Note**

- 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.
- 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.
- If all clauses fail to permit or deny the route, the route is denied.
- Route-map’s match on a list of communities is performed with the command “match community-list” and not this command.
### match community-list

Syntax:

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>communities-list-name</th>
<th>A name of an IP community list</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>N/A</td>
<td></td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Config Route Map</td>
<td></td>
</tr>
<tr>
<td>History</td>
<td>3.3.5006</td>
<td></td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
<td></td>
</tr>
</tbody>
</table>

Example:

```
switch (config route-map mymap permit 10)# match community-list COM_LIST exact-match
```

Related Commands: N/A

Note:
- 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.
- 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.
- If all clauses fail to permit or deny the route, the route is denied.
## 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.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>prefix-list-name</th>
<th>Prefix-list name.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>N/A</td>
<td></td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Config Route Map</td>
<td></td>
</tr>
<tr>
<td>History</td>
<td>3.3.5006</td>
<td></td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
<td></td>
</tr>
<tr>
<td>Example</td>
<td>switch (config route-map mymap permit 10)# match interface ethernet 1/1</td>
<td></td>
</tr>
<tr>
<td>Related Commands</td>
<td>N/A</td>
<td></td>
</tr>
</tbody>
</table>
| Note                     | • 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.
• 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.
• If all clauses fail to permit or deny the route, the route is denied. |
### 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.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>prefix-list-name</th>
<th>Prefix-list name.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>N/A</td>
<td></td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Config Route Map</td>
<td></td>
</tr>
<tr>
<td>History</td>
<td>3.3.5006</td>
<td></td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
<td></td>
</tr>
<tr>
<td>Example</td>
<td><code>switch (config route-map mymap permit 10)# match ip address listSmallRoutes</code></td>
<td></td>
</tr>
<tr>
<td>Related Commands</td>
<td>N/A</td>
<td></td>
</tr>
<tr>
<td>Note</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- 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.
- 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.
- If all clauses fail to permit or deny the route, the route is denied.
- 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.
**match ip next-hop**

```
mach ip next-hop <value>
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.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>value</th>
<th>Next hop IP address: A.B.C.D (e.g. 10.0.13.86).</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Default</strong></td>
<td>N/A</td>
<td></td>
</tr>
<tr>
<td><strong>Configuration Mode</strong></td>
<td>Config Route Map</td>
<td></td>
</tr>
<tr>
<td><strong>History</strong></td>
<td>3.3.5200</td>
<td></td>
</tr>
<tr>
<td><strong>Role</strong></td>
<td>admin</td>
<td></td>
</tr>
<tr>
<td><strong>Example</strong></td>
<td><code>switch (config route-map mymap permit 10)# match ip next-hop 10.10.10.10</code></td>
<td></td>
</tr>
<tr>
<td><strong>Related Commands</strong></td>
<td>N/A</td>
<td></td>
</tr>
</tbody>
</table>
| **Note**           | • 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.  
• 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.  
• If all clauses fail to permit or deny the route, the route is denied. |
**match local-preference**

```plaintext
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.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>value</th>
<th>Range: 1-2147483647.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>N/A</td>
<td></td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Config Route Map</td>
<td></td>
</tr>
<tr>
<td>History</td>
<td>3.3.5200</td>
<td>First version</td>
</tr>
<tr>
<td></td>
<td>3.4.0000</td>
<td>Updated value range</td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
<td></td>
</tr>
<tr>
<td>Example</td>
<td>switch (config route-map mymap permit 10)# match local-preference 10</td>
<td></td>
</tr>
<tr>
<td>Related Commands</td>
<td>N/A</td>
<td></td>
</tr>
</tbody>
</table>
| Note                | • 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.  
  • 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.  
  • If all clauses fail to permit or deny the route, the route is denied. |
**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.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>value</th>
<th>Range: 1-2147483647.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>N/A</td>
<td></td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Config Route Map</td>
<td></td>
</tr>
<tr>
<td>History</td>
<td>3.3.5200</td>
<td>First version</td>
</tr>
<tr>
<td></td>
<td>3.4.0000</td>
<td>Updated value range</td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
<td></td>
</tr>
<tr>
<td>Example</td>
<td>switch (config route-map mymap permit 10)# match metric 10</td>
<td></td>
</tr>
<tr>
<td>Related Commands</td>
<td>N/A</td>
<td></td>
</tr>
</tbody>
</table>
| Note               | • 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.  
• 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.  
• If all clauses fail to permit or deny the route, the route is denied. |
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.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>value</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>BGP AS number that is prepended to as-path. Range: 1-4294967295.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Default</th>
<th>N/A</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Configuration Mode</th>
<th>Config Route Map</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>History</th>
<th>3.4.0000</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Role</th>
<th>admin</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Example</th>
<th>switch (config route-map mymap permit 10)# set as-path prepend 5 10</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Related Commands</th>
<th>N/A</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Note</th>
<th>N/A</th>
</tr>
</thead>
</table>
**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.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>value</th>
<th>Range: 1-2147483648.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>N/A</td>
<td></td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Config Route Map</td>
<td></td>
</tr>
<tr>
<td>History</td>
<td>3.3.5200</td>
<td></td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
<td></td>
</tr>
<tr>
<td>Example</td>
<td>switch (config route-map mymap permit 10)# set as-path tag 1</td>
<td></td>
</tr>
<tr>
<td>Related Commands</td>
<td>N/A</td>
<td></td>
</tr>
<tr>
<td>Note</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
**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.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>list of communities</th>
<th>List of standard communities:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>• <a href="">aa:nn</a></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• &lt;number&gt;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• internet</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• local-AS</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• no-advertise</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• no-export</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Default</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuration Mode</td>
<td>Config Route Map</td>
</tr>
<tr>
<td>History</td>
<td>3.3.5200</td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
</tr>
</tbody>
</table>

**Example**

```
switch (config route-map mymap permit 10)# set community 1:2 3:4
```

**Related Commands**

N/A

**Note**
### 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.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>list-of-communities</th>
<th>List of standard communities:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>• <a href="">aa:nn</a></td>
</tr>
<tr>
<td></td>
<td></td>
<td>•  &lt;number&gt;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• internet</td>
</tr>
<tr>
<td></td>
<td></td>
<td>•  local-AS</td>
</tr>
<tr>
<td></td>
<td></td>
<td>•  no-advertise</td>
</tr>
<tr>
<td></td>
<td></td>
<td>•  no-export</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Default</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuration Mode</td>
<td>Config Route Map</td>
</tr>
<tr>
<td>History</td>
<td>3.3.5200</td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
</tr>
<tr>
<td>Example</td>
<td><code>switch (config route-map mymap permit 10)# set community none</code></td>
</tr>
<tr>
<td>Related Commands</td>
<td>N/A</td>
</tr>
<tr>
<td>Note</td>
<td></td>
</tr>
</tbody>
</table>
### 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.

<table>
<thead>
<tr>
<th>Default</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuration Mode</td>
<td>Config Route Map</td>
</tr>
<tr>
<td>History</td>
<td>3.3.5200</td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
</tr>
<tr>
<td>Example</td>
<td><code>switch (config route-map mymap permit 10)# set community none</code></td>
</tr>
<tr>
<td>Related Commands</td>
<td>N/A</td>
</tr>
<tr>
<td>Note</td>
<td></td>
</tr>
</tbody>
</table>
**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.

| Syntax Description | list of communities | List of standard communities:
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>• <code>&lt;aa:nn&gt;</code></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <code>&lt;number&gt;</code></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <code>internet</code></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <code>local-AS</code></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <code>no-advertise</code></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <code>no-export</code></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Default</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuration Mode</td>
<td>Config Route Map</td>
</tr>
<tr>
<td>History</td>
<td>3.3.5200</td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
</tr>
</tbody>
</table>

**Example**

```
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
```

**Related Commands**

N/A

**Note**

N/A
**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.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;community-list-name&gt;</code></td>
<td>Name of community list</td>
</tr>
</tbody>
</table>

**Default**

N/A

**Configuration Mode**

Config Route Map

**History**

3.3.5200

3.6.3004 Added note

**Role**

admin

**Example**

switch (config route-map mymap permit 10)# set community internet 1:3 additive

**Related Commands**

N/A

**Note**

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.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>&lt;community-list-name&gt;</th>
<th>Name of community list</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>N/A</td>
<td></td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Config Route Map</td>
<td></td>
</tr>
<tr>
<td>History</td>
<td>3.3.5200</td>
<td></td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
<td></td>
</tr>
<tr>
<td>Example</td>
<td>switch (config route-map mymap permit 10)# set community-list mycommunity additive</td>
<td></td>
</tr>
<tr>
<td>Related Commands</td>
<td>N/A</td>
<td></td>
</tr>
<tr>
<td>Note</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
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.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>community-list-name</th>
<th>Name of community list</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>N/A</td>
<td></td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Config Route Map</td>
<td></td>
</tr>
<tr>
<td>History</td>
<td>3.3.5200</td>
<td></td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
<td></td>
</tr>
<tr>
<td>Example</td>
<td>switch (config route-map mymap permit 10)# set community-list mycommunity delete</td>
<td></td>
</tr>
<tr>
<td>Related Commands</td>
<td>N/A</td>
<td></td>
</tr>
<tr>
<td>Note</td>
<td>N/A</td>
<td></td>
</tr>
</tbody>
</table>
**set ip next-hop**

```
set ip next-hop <value>
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.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>value</td>
<td>Route next-hop IP: A.B.C.D (e.g. 10.0.13.86).</td>
</tr>
</tbody>
</table>

| Default             | N/A                                |
| Configuration Mode  | Config Route Map                   |
| History             | 3.3.5200                           |
| Role                | admin                              |
| Example             | `switch (config route-map mymap permit 10)# set ip next-hop 10.10.10` |
| Related Commands    | N/A                                |
**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.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>value</th>
<th>Route local-pref: 1-2147483648.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>N/A</td>
<td></td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Config Route Map</td>
<td></td>
</tr>
<tr>
<td>History</td>
<td>3.3.5200</td>
<td></td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
<td></td>
</tr>
<tr>
<td>Example</td>
<td>switch (config route-map mymap permit 10)# set local-preference 10</td>
<td></td>
</tr>
<tr>
<td>Related Commands</td>
<td>N/A</td>
<td></td>
</tr>
<tr>
<td>Note</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
**set metric**

```plaintext
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.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
<th>Default</th>
<th>Configuration Mode</th>
<th>Configuration Mode</th>
<th>History</th>
<th>Role</th>
<th>Example</th>
<th>Related Commands</th>
</tr>
</thead>
<tbody>
<tr>
<td>value</td>
<td>Route metric: 1-2147483647.</td>
<td>N/A</td>
<td>Config Route Map</td>
<td>admin</td>
<td>3.3.5200</td>
<td>admin</td>
<td><code>switch (config route-map mymap permit 10)# set metric 10</code></td>
<td>N/A</td>
</tr>
</tbody>
</table>

**Note**

N/A
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.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>egp</th>
<th>Set a route’s entry origin parameter to external.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>igp</td>
<td>Set a route’s entry origin parameter to internal.</td>
</tr>
<tr>
<td></td>
<td>incomplete</td>
<td>Set a route’s entry origin parameter to incomplete.</td>
</tr>
</tbody>
</table>

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: N/A
### 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.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>value</th>
<th>Range: 1-2147483647.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>N/A</td>
<td></td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Config Route Map</td>
<td></td>
</tr>
<tr>
<td>History</td>
<td>3.3.5200</td>
<td></td>
</tr>
<tr>
<td></td>
<td>3.4.0000</td>
<td>Updated parameter range</td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
<td></td>
</tr>
<tr>
<td>Example</td>
<td><code>switch (config route-map mymap permit 10)# set tag 10</code></td>
<td></td>
</tr>
<tr>
<td>Related Commands</td>
<td>N/A</td>
<td></td>
</tr>
<tr>
<td>Note</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
## 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.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>number</th>
<th>Value of the weight to set. Range: 1-65535.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>N/A</td>
<td></td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Config Route Map</td>
<td></td>
</tr>
<tr>
<td>History</td>
<td>3.3.5006</td>
<td>First version</td>
</tr>
<tr>
<td></td>
<td>3.4.0000</td>
<td>Updated parameter range</td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
<td></td>
</tr>
<tr>
<td>Example</td>
<td>switch (config route-map mymap permit 10)# set weight 7</td>
<td></td>
</tr>
<tr>
<td>Related Commands</td>
<td>route-map &lt;map-name&gt; [deny</td>
<td>permit] [sequence-number]</td>
</tr>
</tbody>
</table>

**Note**
### show route-map

**show route-map [<name>]**

Displays route map configuration.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>N/A</td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Any Command Mode</td>
</tr>
<tr>
<td>History</td>
<td>3.3.5006</td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
</tr>
</tbody>
</table>

**Example**

```plaintext
switch (config)# show route-map mymap
route-map mymap, permit, sequence 1200
  Set clauses:
    continue 1800
switch (config)#
```

**Related Commands**

N/A

**Note**

N/A
6.4.2 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.
6.4.2.1 Commands

**ip prefix-list**

```
ip prefix-list <list-name> [seq <number>] {permit | deny} <ip> [eq <length> | <prefix> [eq <length> | le <length> | ge <length> [le <length>]]]
no ip prefix-list <list-name> [seq <number>]
```

Creates or updates a prefix-list. The no form of the command deletes a prefix-list or a prefix-list entry.

### Syntax Description

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>list-name</td>
<td>String</td>
</tr>
<tr>
<td>seq &lt;number&gt;</td>
<td>Sequence number assigned to entry. Range: 0-65535.</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>
<tr>
<td>ip</td>
<td>IP address</td>
</tr>
</tbody>
</table>
| eq | ge | le <mask> | **Equal to a specified prefix length**  
**ge**: Greater than or equal to a specified prefix length  
**le**: Less than or equal to a specified prefix length |

### Default

Sequence value = 10

### Configuration Mode

Config

### History

3.3.5200

### Role

admin

### Example

```
switch (config)# ip prefix-list a-list permit 10.20.0.0 /16 eq 24
switch (config)#
```

### Related Commands

N/A

### Note

N/A
**show ip prefix-list**

*show ip prefix-list [<name>]*

Displays prefix-lists.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>name</th>
<th>Displays a specific prefix-list.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>N/A</td>
<td></td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Any Command Mode</td>
<td></td>
</tr>
<tr>
<td>History</td>
<td>3.3.5200</td>
<td></td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
<td></td>
</tr>
</tbody>
</table>

**Example**

```
switch (config)# show ip prefix-list
prefix-list: a-list
  count: 1, range entries: 1, sequences: 10 - 10
  seq 10 permit 10.20.0.0 /16 ge 24 (hit count: 0, refcount: 0)
prefix-list: b-list
  count: 2, range entries: 2, sequences: 10 - 20
  seq 10 deny 10.10.0.0 /16 le 24 (hit count: 0, refcount: 0)
  seq 20 deny 10.20.0.0 /16 le 24 (hit count: 0, refcount: 0)
switch (config)#
```

**Related Commands**

N/A

**Note**
6.5 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), PIM sparse mode (PIM-SM, which is not supported on Mellanox platforms), Bidirectional PIM (PIM-BIDIR) and Bootstrap router (BSR) protocol.

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.

6.5.1 Bidirectional PIM

Bidirectional PIM (PIM-BIDIR) is a variant of PIM-SM that builds bidirectional distribution trees that connect multicast senders and receivers. It differs from PIM-SM by eliminating a need to tunnel multicast packets to RP and to keep a state for each (S,G) pair. It also eliminates a need in data driven protocol events. PIM-BIDIR achieves it by defining a new role, Designated Forwarder (DF), and by defining new forwarding rules and keeping all other PIM-SM mechanisms intact.

DF is a PIM enabled router that is the closest router to RP among all PIM routers residing on specific L2 network. It is dynamically elected by all PIM routers on that network. DF is required on each L2 multicast capable network for each RP. DF serves all multicast groups that share the same RP and has following duties:

- It is an only router that is responsible to receive and forward upstream multicast packets on that L2 segment
- It is a router that should collect all Join requests from the routers on that L2 segment
- It is an only router that will distribute downstream multicast packets on that segment.

Once Designated forwarders are elected and forwarding rules are established, PIM routers can start to issue (*,G) Join messages and build shared distribution trees. When shared tree is created, multicast sources can start to exchange data with receivers and it doesn't require any additional maintenance of the multicast states.

Compared to PIM-SM, in bidirectional PIM:

- Each router will keep only (*,G) state and not (*,G) and (S,G) like in PIM-SM
- Multicast traffic from the beginning is forwarded naturally - no need to tunnel data to RP
- Resulting multicast tree is not shortest path optimal and converges around selected Rendezvous point, but is shared among all participants in that multicast group

In BIDIR-PIM, the packet forwarding rules have been improved over PIM-SM, allowing traffic to be passed up the shared tree toward the RP. To avoid multicast packet looping, bidir-PIM introduces a new mechanism called designated forwarder (DF) election, which establishes a loop-free SPT rooted at the RP.
6.5.2 PIM Load-Sharing

PIM load-sharing improves network efficiency in IP multicast applications especially in cases when we have multiple equal-cost paths to the same destination. There are two methods which enhance IP multicast bandwidth capacity consumption: rendezvous point load sharing and next-hop load sharing.

Routers should be connected via router port interfaces and not VLAN interfaces. Connecting two routers via VLAN interface with PIM load-sharing causes loops in the network.

6.5.2.1 Rendezvous Point Load-Sharing

IP multicast routing is facilitated by use of rendezvous points (RPs) which are anchors in IP multicast distribution trees, and, in case of PIM-BIDIR, are central points that perform IP multicast packet forwarding. Therefore, they can get heavily loaded.

When multiple RPs serve the same multicast IP addresses and are located at an equal distance from a traffic source or receiver, data streams can be shared between those RPs. This enhances switching performance, improves network bandwidth consumption and increases reliability. Data packets based on the packet flow parameters are equally shared between all RPs located at an equal-distance.

6.5.2.2 Next Hop Load-Sharing

Another way to improve network capacity consumption and increase the amount of IP multicast data carried by the network, is to utilize multiple equal-cost paths from RPs to IP multicast receivers. A network usually selects a single path to carry specific multicast group data packets from a source to a specific multicast destination. But when enabling next hop load-sharing, multiple paths between RP and multicast group receivers may be utilized, and based on traffic flow parameters, the data stream may be split to multiple flows that go through several equal-cost paths to the same destination.

6.5.3 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. Bootstrap 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.

### 6.5.4 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
```

### 6.5.4.1 Configuring IGMP

IGMP is enabled when IP multicast is enabled and static multicast or PIM is enabled on the interface.

### 6.5.4.2 Verifying IGMP

**Step 1.** Display a brief IGMP interface status. Run:

```
switch (config)# show ip igmp interface brief
```

<table>
<thead>
<tr>
<th>Interface</th>
<th>IP Address</th>
<th>IGMP Querier</th>
<th>Membership</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLAN10</td>
<td>10.10.10.1</td>
<td>10.10.10.1</td>
<td>5</td>
<td>v2</td>
</tr>
</tbody>
</table>
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 immediate leave: Disabled
  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
```

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

<table>
<thead>
<tr>
<th>Group Address</th>
<th>Type</th>
<th>Interface</th>
<th>Uptime</th>
<th>Expires</th>
<th>Last Reporter</th>
</tr>
</thead>
<tbody>
<tr>
<td>226.0.1.0</td>
<td>D</td>
<td>vlan10</td>
<td>[0d 00:00:07.46]</td>
<td>[0d 00:04:05.08]</td>
<td>10.10.10.2</td>
</tr>
<tr>
<td>226.0.1.1</td>
<td>D</td>
<td>vlan10</td>
<td>[0d 00:00:07.47]</td>
<td>[0d 00:04:05.08]</td>
<td>10.10.10.2</td>
</tr>
</tbody>
</table>

switch (config)#
```

6.5.4.3 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
```
6.5.5 Commands

6.5.5.1 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.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>Disabled</td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Config</td>
</tr>
<tr>
<td>History</td>
<td>3.3.5006</td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
</tr>
<tr>
<td>Example</td>
<td>switch (config) # protocol pim</td>
</tr>
<tr>
<td>Related Commands</td>
<td>N/A</td>
</tr>
<tr>
<td>Note</td>
<td></td>
</tr>
</tbody>
</table>
### 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.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>Disabled</td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Config</td>
</tr>
<tr>
<td>History</td>
<td>3.3.5006</td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
</tr>
<tr>
<td>Example</td>
<td>switch (config) # no ip pim bidir shutdown</td>
</tr>
<tr>
<td>Related Commands</td>
<td>N/A</td>
</tr>
<tr>
<td>Note</td>
<td></td>
</tr>
</tbody>
</table>
**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.

### Syntax Description

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>rp-address</td>
<td>The static IP address of rendezvous point.</td>
</tr>
<tr>
<td>ip-address</td>
<td>IP address of the group-range (coupled with the prefix parameter).</td>
</tr>
<tr>
<td>prefix</td>
<td>Network prefix (in the format of /24, or 255.255.255.0 for example) of group range.</td>
</tr>
<tr>
<td>override</td>
<td>Specifies that this configuration overrides dynamic configuration learned by BSR.</td>
</tr>
<tr>
<td>bidir</td>
<td>Specifies that the group range uses a bidirectional PIM.</td>
</tr>
</tbody>
</table>

### Default
N/A

### Configuration Mode
Config

### History
3.3.5006

### Role
admin

### Example
```
switch (config) # ip pim rp-address 10.10.10.10 bidir
```

### Related Commands
N/A

### Note

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.

**Syntax Description**

- `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.

**Default**

- The interface is not BSR candidate by default.
- priority: 64
- interval: 60
- hash-len: 30

**Configuration Mode**

- 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

**History**

- 3.3.5006

**Role**

- admin

**Example**

```
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**

```plaintext
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.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>period</td>
<td>In seconds. Range: 12-1073741823 (1.073 billion).</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Default</th>
<th>period = 2*(BSR candidate interval) + 10</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuration Mode</td>
<td>Config</td>
</tr>
<tr>
<td>History</td>
<td>3.3.5006</td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
</tr>
</tbody>
</table>

**Example**

```
switch (config) # ip pim bsr-holdtime 30
```

**Related Commands**

```
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.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ethernet &lt;slot/port&gt;</td>
<td>Ethernet interface.</td>
</tr>
<tr>
<td>port-channel &lt;number&gt;</td>
<td>LAG interface.</td>
</tr>
<tr>
<td>vlan &lt;vlan-id&gt;</td>
<td>VLAN ID. Range: 1-4094.</td>
</tr>
<tr>
<td>loopback &lt;number&gt;</td>
<td>Loopback interface number.</td>
</tr>
<tr>
<td>ip-address</td>
<td>The group IP address.</td>
</tr>
<tr>
<td>prefix</td>
<td>Network prefix (for example /24, or 255.255.255.0).</td>
</tr>
<tr>
<td>priority</td>
<td>RP priority rating. Range: 0-255, where smaller numbers mean higher priority.</td>
</tr>
</tbody>
</table>

**Default**
The RP priority is 192. The BSR message interval is 60 seconds.

**Configuration Mode**
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

**History**
3.3.5006

**Role**
admin

**Example**
switch (config) # ip pim rp-candidate vlan 19 group-list 225.6.5.0 /25 priority 20 interval 30 bidir
### Related Commands
N/A

### Note
- 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.
- Running-config supports multiple multicast groups through multiple `ip pim rp-candidate` statements:
  - 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.
  - 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.
  - 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.
  - When setting a priority, all previous rp-candidates within all interfaces and groups are configured to this priority.
### ip pim sparse-mode

**Syntax**

```
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.

**Syntax Description**

N/A

**Default**

Disabled

**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 pim sparse-mode  
```

**Related Commands**

N/A

**Note**

N/A
**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.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>priority</th>
<th>The designated router priority of the PIM Hello messages. Range is 1-4294967295.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Config Interface VLAN Config Interface Ethernet configured as a router port interface Config Interface Port Channel configured as a router port interface</td>
<td></td>
</tr>
<tr>
<td>History</td>
<td>3.3.5006</td>
<td></td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
<td></td>
</tr>
<tr>
<td>Example</td>
<td>switch (config interface vlan 10) # ip pim dr-priority 5</td>
<td></td>
</tr>
<tr>
<td>Related Commands</td>
<td>ip pim sparse-mode</td>
<td></td>
</tr>
<tr>
<td>Note</td>
<td>The command “ip pim sparse-mode” must be run prior to using this command.</td>
<td></td>
</tr>
</tbody>
</table>
### 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.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>interval</th>
<th>PIM Hello interval in milliseconds. Range: 1000-65535000.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td></td>
<td>30,000 milliseconds</td>
</tr>
</tbody>
</table>
| 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 pim hello-interval 70000 |
| Related Commands         |          | ip pim sparse-mode                                        |
| Note                     |          | 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.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>period</th>
<th>Range: 1-1000000 seconds.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>60 seconds</td>
<td></td>
</tr>
</tbody>
</table>
| 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            | 3.3.5200 |
| Role               | admin |
| Example            | switch (config interface vlan 10) # ip pim join-prune-interval 60 |
| Related Commands   | |
| Note               | |
**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.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>Disabled</td>
</tr>
</tbody>
</table>
| 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 pim border` |
| Related Commands   |     |
| Note               | 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.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>no pim bsr-border</td>
</tr>
</tbody>
</table>
| 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             | 3.3.5200          |
| Role                | admin             |
| Example             | switch (config interface vlan 10) # ip pim bsr-border |
| Related Commands    |                   |

**Note**
### 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.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>Disabled</td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Config</td>
</tr>
<tr>
<td>History</td>
<td>3.4.2008</td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
</tr>
<tr>
<td>Example</td>
<td>switch (config) # ip pim multipath rp</td>
</tr>
<tr>
<td>Related Commands</td>
<td>N/A</td>
</tr>
<tr>
<td>Note</td>
<td></td>
</tr>
</tbody>
</table>
**debug ethernet ip pim**

```plaintext
d debug ethernet ip pim {all | control-plane | data-path | fail-all | init-shut | management | memory | packet-dump | resources}
no debug ethernet ip pim {all | control-plane | data-path | fail-all | init-shut | management | memory | packet-dump | resources}
```

Configures the trace level for PIM. The no form of the command removes the trace level for PIM.

### Syntax Description

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Usage</th>
</tr>
</thead>
<tbody>
<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>
</tbody>
</table>

### Default

N/A

### Configuration Mode

Config

### History

3.3.5200

### Role

admin

### Example

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

### Related Commands

Note
show ip pim protocol

Displays PIM protocol information (counters).

**Syntax Description**
N/A

**Default**
N/A

**Configuration Mode**
Any Command Mode

**History**
3.3.5200

**Role**
admin

**Example**
```
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
```

**Related Commands**

**Note**
show ip pim bsr

**Syntax Description**
- Displays PIM BSR information.

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Syntax Description</td>
<td>N/A</td>
</tr>
<tr>
<td>Default</td>
<td>N/A</td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Any Command Mode</td>
</tr>
<tr>
<td>History</td>
<td>3.3.5006</td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
</tr>
</tbody>
</table>

**Example**
```bash
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
```

**Related Commands**

**Note**
### show ip pim neighbor

**show ip pim neighbor [vlan <vlan-id> | <other interfaces> | <ip-addr>]**

Displays information about IPv4 PIM neighbors.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan &lt;vlan-id&gt;</td>
<td>Filters the output per specific VLAN ID.</td>
</tr>
<tr>
<td>neighbor-addr</td>
<td>Filters the output per specific neighbor IP address.</td>
</tr>
</tbody>
</table>

**Default**

N/A

**Configuration Mode**

Any Command Mode

**History**

3.3.5006

**Role**

admin

**Example**

```
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
```

**Related Commands**

**Note**
show ip pim rp

show ip pim rp <rp-address>

Displays information about the rendezvous points (RPs) for PIM.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>rp-address</td>
<td>A rendezvous points address.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Default</th>
<th>N/A</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Configuration Mode</th>
<th>Any Command Mode</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>History</th>
<th>3.3.5006</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Role</th>
<th>admin</th>
</tr>
</thead>
</table>

| Example            | 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)# |

<table>
<thead>
<tr>
<th>Related Commands</th>
<th></th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Note</th>
<th></th>
</tr>
</thead>
</table>
show ip pim rp-hash

    show ip pim rp-hash <group>

Displays the hashed value of the group (RP address according the group address).

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>group</th>
<th>Filters the output per a specific IP Multicast group address.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>N/A</td>
<td></td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Any Command Mode</td>
<td></td>
</tr>
<tr>
<td>History</td>
<td>3.3.5006</td>
<td></td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
<td></td>
</tr>
</tbody>
</table>

**Example**

```
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)#
```

**Related Commands**

- show ip pim rp-hash

**Note**
show ip pim rp-candidate

Syntax Description
Displays information about RP candidate status.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>N/A</td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Any Command Mode</td>
</tr>
<tr>
<td>History</td>
<td>3.3.5006</td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
</tr>
</tbody>
</table>

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
```

Related Commands

Note

---

show ip pim rp-candidate

Displays information about RP candidate status.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>N/A</td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Any Command Mode</td>
</tr>
<tr>
<td>History</td>
<td>3.3.5006</td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
</tr>
</tbody>
</table>

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
```

Related Commands

Note
show ip pim interface

show ip pim interface {v[lan <vlan id>] | ethernet <port> | df | brief}

Displays information about the enabled interfaces for PIM.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan &lt;vlan-id&gt;</td>
<td>Filters the output for specific interface.</td>
</tr>
<tr>
<td>ethernet &lt;port&gt;</td>
<td>Ethernet interface.</td>
</tr>
<tr>
<td>df</td>
<td>Displays information about elected designated forwarders.</td>
</tr>
<tr>
<td>brief</td>
<td>Displays a summary of information for all interfaces.</td>
</tr>
</tbody>
</table>

Default: N/A

Configuration Mode: Any Command Mode

History: 3.3.5006

Role: admin

Example:

```
# 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
```
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

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>N/A</td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Any Command Mode</td>
</tr>
<tr>
<td>History</td>
<td>3.3.5006</td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
</tr>
</tbody>
</table>

**Example**

```
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) #
```

**Related Commands**

**Note**

Should contain the following information: neighbor address, interface address, group range, Joins, Prunes.
### 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.

<table>
<thead>
<tr>
<th><strong>Syntax Description</strong></th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Default</strong></td>
<td>Disabled</td>
</tr>
<tr>
<td><strong>Configuration Mode</strong></td>
<td>Config</td>
</tr>
<tr>
<td><strong>History</strong></td>
<td>3.3.5006</td>
</tr>
<tr>
<td><strong>Role</strong></td>
<td>admin</td>
</tr>
<tr>
<td><strong>Example</strong></td>
<td><code>switch (config)# ip multicast-routing</code></td>
</tr>
<tr>
<td><strong>Related Commands</strong></td>
<td>N/A</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td></td>
</tr>
</tbody>
</table>
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**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip-addr</td>
<td>Unicast IP address.</td>
</tr>
<tr>
<td>ip-mask</td>
<td>Network mask in a dotted format (e.g. 255.255.255.0) or /24 format.</td>
</tr>
<tr>
<td>next-hop</td>
<td>Next hop IP address.</td>
</tr>
<tr>
<td>preference</td>
<td>Route preference. Range: 1-255.</td>
</tr>
</tbody>
</table>

**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.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ttl-value</td>
<td>Range: 0-225.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Default</th>
<th>0 – all packets are forwarded</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuration Mode</td>
<td>Config Interface VLAN</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Config Interface Ethernet</td>
<td></td>
</tr>
<tr>
<td></td>
<td>configured as a router port</td>
<td></td>
</tr>
<tr>
<td></td>
<td>interface</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Config Interface Port Channel</td>
<td></td>
</tr>
<tr>
<td></td>
<td>configured as a router port</td>
<td></td>
</tr>
<tr>
<td></td>
<td>interface</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>History</th>
<th>3.3.5006</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Role</td>
<td>admin</td>
<td></td>
</tr>
</tbody>
</table>

Example

```
switch (config interface vlan 10)# ip multicast ttl-threshold 10
```

<table>
<thead>
<tr>
<th>Related Commands</th>
<th>N/A</th>
<th></th>
</tr>
</thead>
</table>

Note
**show ip mroute**

`show ip mroute [summary | <group> [<prefix> [<source>]]]`

Displays information about IPv4 multicast routes.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>source</th>
<th>Source IP address.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>group</td>
<td>IP address of multicast group.</td>
</tr>
<tr>
<td></td>
<td>prefix</td>
<td>Network prefix of multicast group (in the format of /24, or 255.255.255.0 for example).</td>
</tr>
<tr>
<td></td>
<td>summary</td>
<td>Displays a summary of the multicast routes.</td>
</tr>
</tbody>
</table>

| Default          | N/A               |
| Configuration Mode | Any Command Mode |
| History          | 3.2.1000          |
|                  | 3.5.1000          |
| Role             | admin             |
| Example          | 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  

| Related Commands | N/A |
| Note             | N/A |
### ip igmp immediate-leave

**ip igmp immediate-leave**  
**no ip igmp immediate-leave**

Enables the device to remove the group entry from the multicast routing table immediately upon receiving a leave message for the group. The no form of the command disables immediate-leave.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>Disabled</td>
</tr>
<tr>
<td><strong>Configuration Mode</strong></td>
<td></td>
</tr>
<tr>
<td>Config Interface VLAN</td>
<td></td>
</tr>
<tr>
<td>Config Interface Ethernet configured as a router port interface</td>
<td></td>
</tr>
<tr>
<td>Config Interface Port Channel configured as a router port interface</td>
<td></td>
</tr>
<tr>
<td><strong>History</strong></td>
<td>3.3.5006</td>
</tr>
<tr>
<td><strong>Role</strong></td>
<td>admin</td>
</tr>
<tr>
<td><strong>Example</strong></td>
<td></td>
</tr>
<tr>
<td>switch (config interface vlan 10)# ip igmp immediate-leave</td>
<td></td>
</tr>
<tr>
<td><strong>Related Commands</strong></td>
<td>N/A</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td></td>
</tr>
</tbody>
</table>
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.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Count</th>
<th>Range: 1-7.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Config Interface VLAN Config Interface Ethernet configured as a router port interface Config Interface Port Channel configured as a router port interface</td>
<td></td>
</tr>
<tr>
<td>History</td>
<td>3.3.5006</td>
<td></td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
<td></td>
</tr>
<tr>
<td>Example</td>
<td>switch (config interface vlan 10) # ip igmp last-member-query-count 7</td>
<td></td>
</tr>
<tr>
<td>Related Commands</td>
<td>N/A</td>
<td></td>
</tr>
<tr>
<td>Note</td>
<td>This parameter reflects expected packet loss on a congested network.</td>
<td></td>
</tr>
</tbody>
</table>
**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.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>interval</th>
<th>IGMP last member query response time. Range: 1-25 seconds.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>1</td>
<td></td>
</tr>
</tbody>
</table>
| 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 last-member-query-response-time 10 |
| Related Commands   | N/A       |                                                          |
| Note               |           |                                                          |
**ip igmp startup-query-count**

```
ip igmp startup-query-count <count>
nop 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.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>count</th>
<th>Range: 1-65535.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Config Interface VLAN</td>
<td>Config Interface Ethernet configured as a router port interface</td>
</tr>
<tr>
<td>History</td>
<td>3.3.5006</td>
<td></td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
<td></td>
</tr>
<tr>
<td>Example</td>
<td>switch (config interface vlan 10)# ip igmp startup-query-count 10</td>
<td>N/A</td>
</tr>
<tr>
<td>Related Commands</td>
<td>N/A</td>
<td></td>
</tr>
<tr>
<td>Note</td>
<td>N/A</td>
<td></td>
</tr>
</tbody>
</table>
### ip igmp startup-query-interval

**Syntax**

```
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.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>interval</td>
<td>Range: 1-1800 seconds.</td>
</tr>
</tbody>
</table>

| Default | 30 |

<table>
<thead>
<tr>
<th>Configuration Mode</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Config Interface VLAN</td>
<td></td>
</tr>
<tr>
<td>Config Interface Ethernet configured as a router port interface</td>
<td></td>
</tr>
<tr>
<td>Config Interface Port Channel configured as a router port interface</td>
<td></td>
</tr>
</tbody>
</table>

| History | 3.3.5006 |

| Role | admin |

| Example | switch (config interface vlan 10)# ip igmp startup-query-interval 10 |

| Related Commands | N/A |

| Note | |

**Example**

```
switch (config interface vlan 10)# ip igmp startup-query-interval 10
```
### 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.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>interval</th>
<th>The IGMP query interval. Range: 1-1800 seconds.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>125</td>
<td></td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Config Interface VLAN</td>
<td></td>
</tr>
<tr>
<td>History</td>
<td>3.3.5006</td>
<td></td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
<td></td>
</tr>
<tr>
<td>Example</td>
<td>switch (config interface vlan 10)# ip igmp query-interval 60</td>
<td></td>
</tr>
<tr>
<td>Related Commands</td>
<td>N/A</td>
<td></td>
</tr>
<tr>
<td>Note</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
**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.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>time</th>
<th>The IGMP max response time. Range: 1-25 seconds.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>10</td>
<td></td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Config Interface VLAN</td>
<td></td>
</tr>
<tr>
<td>History</td>
<td>3.3.5006</td>
<td></td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
<td></td>
</tr>
<tr>
<td>Example</td>
<td>switch (config interface vlan 10)# ip igmp query-max-response-time 20</td>
<td></td>
</tr>
<tr>
<td>Related Commands</td>
<td>N/A</td>
<td></td>
</tr>
<tr>
<td>Note</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
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.

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>2</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Configuration Mode</th>
<th>Config Interface VLAN</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Config Interface Ethernet configured as a router port interface</td>
</tr>
<tr>
<td></td>
<td>Config Interface Port Channel configured as a router port interface</td>
</tr>
</tbody>
</table>

| History | 3.3.5006 |

| Role | admin |

| Example | switch (config interface vlan 10)# ip igmp robustness-variable 4 |

| Related Commands | N/A |

| Note | • The robustness variable can be increased to increase the number of times that packets are resent.  
• This parameter reflects expected packet loss on a congested network. |
**ip igmp static-oif**

```bash
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.

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>group</strong></td>
<td>Multicast IP address.</td>
</tr>
</tbody>
</table>

**Default**

no ip igmp static-oif

**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**

```bash
switch (config interface vlan 10)# ip igmp static-oif 10.10.10.5
```

**Related Commands**

N/A

**Note**

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.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>all</th>
<th>Clears all IGMP groups.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>group-address</td>
<td>Clears a specific group.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Default</th>
<th>no ip igmp static-oif</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuration Mode</td>
<td>Config</td>
</tr>
<tr>
<td>History</td>
<td>3.3.5200</td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
</tr>
</tbody>
</table>
| Example             | `switch (config)# clear ip igmp groups all
switch (config)#` |

| Related Commands    | N/A |

| Note                |     |
debug ethernet ip igmp-l3

d 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.

### Syntax Description

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>all</th>
<th>Enable track traces.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>control-plane</td>
<td>Control plane traces.</td>
</tr>
<tr>
<td></td>
<td>data-path</td>
<td>IP packet dump trace.</td>
</tr>
<tr>
<td></td>
<td>fail-all</td>
<td>All failures including Packet Validation Trace.</td>
</tr>
<tr>
<td></td>
<td>init-shut</td>
<td>Init and shutdown messages.</td>
</tr>
<tr>
<td></td>
<td>management</td>
<td>Management messages.</td>
</tr>
<tr>
<td></td>
<td>memory</td>
<td>Memory related messages.</td>
</tr>
<tr>
<td></td>
<td>packet-dump</td>
<td>Packet dump messages.</td>
</tr>
<tr>
<td></td>
<td>resources</td>
<td>OS Resource trace.</td>
</tr>
</tbody>
</table>

### Default

N/A

### Configuration Mode

Config

### History

3.3.5200

### Role

admin

### Example

```
switch (config)# debug ethernet ip igmp-l3 all
```

### Related Commands

Note
show ip igmp groups

show ip igmp groups [<group>] [vlan <vlan-id>]

Displays information about IGMP-attached group membership.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>group</td>
<td>Filters the output to a specific IP multicast group address.</td>
</tr>
<tr>
<td>vlan &lt;vlan-id&gt;</td>
<td>Filters the output to a specific VLAN ID.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Default</th>
<th>N/A</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Configuration Mode</th>
<th>Any Command Mode</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>History</th>
<th>admin</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Role</th>
<th>admin</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Example</th>
</tr>
</thead>
</table>
| 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 | |

<table>
<thead>
<tr>
<th>Related Commands</th>
<th>N/A</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Note</th>
<th></th>
</tr>
</thead>
</table>
show ip igmp interface

show ip igmp interface [vlan <vlan-id> | brief]

Displays IGMP brief configuration and status.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>brief</th>
<th>Displays brief output information.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>vlan &lt;vlan-id&gt;</td>
<td>Filters the output to a specific VLAN ID.</td>
</tr>
</tbody>
</table>

Default: N/A

Configuration Mode: Any Command Mode

Role: admin
Example

```plaintext
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 immediate leave: Disabled
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
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 immediate leave: Disabled
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
6.6 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.

6.6.1 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.
6.6.2 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:

```bash
switch (config interface vlan 20)# ip address 20.20.20.30 /24
```

**Step 6.** Enable the interface. Run:

```bash
switch (config interface vlan 20)# no shutdown
```

**Configure VRRP:**

This is the same configuration on both switches

**Step 1.** Enable VRRP protocol globally. Run:

```bash
switch (config)# protocol vrrp
```

**Step 2.** Create a virtual router group for an IP interface. Up to 255 VRRP IDs are supported. Run:

```bash
switch (config interface vlan 20)# vrrp 100
```

**Step 3.** Set the VIP address. Run:

```bash
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:

```bash
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:

```bash
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:

```bash
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:

```bash
switch (config interface vlan 20 vrrp 100)# preempt
```

**Step 8.** Disable VRRP. Run:

```bash
switch (config interface vlan 20 vrrp 100)# shutdown
```

The configuration will not be deleted, only the VRRP state machine will be stopped.
6.6.3 Verifying VRRP

Step 1. Display VRRP brief status. Run:

```bash
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:

```bash
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:

```bash
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)#
```
### 6.6.4 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.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>no feature vrrp</td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Config</td>
</tr>
<tr>
<td>History</td>
<td>3.3.4500</td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
</tr>
<tr>
<td>Example</td>
<td>switch (config)# protocol vrrp</td>
</tr>
<tr>
<td>Related Commands</td>
<td></td>
</tr>
<tr>
<td>Note</td>
<td></td>
</tr>
</tbody>
</table>
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.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>number</th>
<th>A VRRP instance number. Range is 1-255.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>N/A</td>
<td></td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Config Interface VLAN</td>
<td></td>
</tr>
<tr>
<td>History</td>
<td>3.3.4500</td>
<td></td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
<td></td>
</tr>
<tr>
<td>Example</td>
<td>switch (config interface vlan 10)#</td>
<td></td>
</tr>
<tr>
<td></td>
<td>switch (config interface vlan 10 vrrp 10)#</td>
<td></td>
</tr>
</tbody>
</table>

Related Commands

Note: A maximum total of 255 VRRP instances are supported per switch system.
### address

```plaintext
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.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip-address</td>
<td>The virtual IP address.</td>
</tr>
<tr>
<td>secondary</td>
<td>A secondary IP address for the virtual router.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Default</th>
<th>N/A</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Configuration Mode</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Config VRRP Interface</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>History</th>
<th>3.3.4500</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Role</th>
<th>admin</th>
</tr>
</thead>
</table>

| Example | 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 |

<table>
<thead>
<tr>
<th>Related Commands</th>
<th></th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Note</th>
<th></th>
</tr>
</thead>
</table>
| • This command is the enabler of the protocol. Therefore, set all the protocol parameters initially and only then set the ip-address.  
| • There are up to 10 IP addresses associated with the VRRP instance. One primary and up to 10 secondary ip-addresses.  
| • If the configured IP address is the same as the interface IP address, this switch automatically owns the IP address (priority 255).  |
**shutdown**

`shutdown`

`no shutdown`

Disables the virtual router. The no form of the command enables the virtual router (stops the VRRP state machine).

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>Enabled (no shutdown)</td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Config VRRP Interface</td>
</tr>
<tr>
<td>History</td>
<td>3.3.4500</td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
</tr>
<tr>
<td>Example</td>
<td>switch (config vrrp 100)# shutdown</td>
</tr>
</tbody>
</table>

**Related Commands**

**Note**
# priority

```plaintext
priority <level>
no priority
```

Sets the priority of the virtual router.
The no form of the command resets the priority to its default.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>level</th>
<th>The virtual router priority level. Range is 1-254.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>100</td>
<td></td>
</tr>
</tbody>
</table>

**Configuration Mode**

Config VRRP Interface

**History**

3.3.4500

**Role**

admin

**Example**

```plaintext
switch (config vrrp 100)# priority 200
```

**Related Commands**

**Note**

- The higher IP address will be selected as master, in case the priority of the routers in the VR are the same.
- To influence the election of the master in the VR cluster make sure that the priority of the desired master is the higher.
**preempt**

```
preempt
no preempt
```

Sets virtual router preemption mode.
The no form of the command disables the virtual router preemption.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>Enabled (preempt)</td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Config VRRP Interface</td>
</tr>
<tr>
<td>History</td>
<td>3.3.4500</td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
</tr>
<tr>
<td>Example</td>
<td><code>switch (config vrrp 100)# preempt</code></td>
</tr>
<tr>
<td>Related Commands</td>
<td></td>
</tr>
<tr>
<td>Note</td>
<td>To set this router as backup for the current virtual router master, preempt must be enabled.</td>
</tr>
</tbody>
</table>
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.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>password</td>
<td>The virtual router authentication password. The password string must be up to 8 alphanumeric characters.</td>
</tr>
</tbody>
</table>

**Default** Disabled

**Configuration Mode** Config VRRP Interface

**History** 3.3.4500

**Role** admin

**Example**

```bash
switch (config vrrp 100)# authentication text mypassword
```

**Related Commands**

**Note**
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.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>seconds</th>
<th>The virtual router advertisement-interval in seconds. Range: 1-255.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Config VRRP Interface</td>
<td></td>
</tr>
<tr>
<td>History</td>
<td>3.3.4500</td>
<td></td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
<td></td>
</tr>
<tr>
<td>Example</td>
<td>switch (config vrrp 100)# advertisement-interval 10</td>
<td></td>
</tr>
<tr>
<td>Related Commands</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Note</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### show vrrp

```
show vrrp [interface <type> <number>] [vr <id>]
```

Displays VRRP brief configuration and status.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>interface &lt;type&gt; &lt;number&gt;</td>
<td>Filters the output to a specific interface type and number.</td>
</tr>
<tr>
<td>vr &lt;id&gt;</td>
<td>Filters the output to a specific virtual router. Range: 1-10.</td>
</tr>
</tbody>
</table>

- **Default**: N/A
- **Configuration Mode**: Any Command Mode
- **History**: 3.3.4500
- **Role**: admin

#### Example

```
switch(config)# show vrrp
Interface  VR Pri Time   Pre  State VR  IP addr
-----------------------------------------------
Eth1/5     1  200  2s  Y Init  192.0.1.10
```

#### Related Commands

- Note
**show vrrp detail**

`show vrrp detail [interface <type> <number>] [vr <id>]`

Displays detailed VRRP configuration and status.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>interface &lt;type&gt; &lt;number&gt;</td>
<td>Filters the output to a specific interface type and number.</td>
</tr>
<tr>
<td>vr &lt;id&gt;</td>
<td>Filters the output to a specific virtual router. Range: 1-255.</td>
</tr>
</tbody>
</table>

| Default | N/A |
| Configuration Mode | Any Command Mode |
| History | 3.3.4500 |
| Role | admin |

**Example**

```
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)#
```

**Related Commands**

<table>
<thead>
<tr>
<th>Related Commands</th>
<th></th>
</tr>
</thead>
</table>

**Note**
**show vrrp statistics**

```
show vrrp statistics [interface <type <number>>] [vr <id>]
```

Displays VRRP counters.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>interface &lt;type&gt; &lt;number&gt;</td>
<td>Filters the output to a specific interface type and number.</td>
</tr>
<tr>
<td>vr &lt;id&gt;</td>
<td>Filters the output to a specific virtual router. Range: 1-255.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Default</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuration Mode</td>
<td>Any Command Mode</td>
</tr>
<tr>
<td>History</td>
<td>3.3.4500</td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
</tr>
</tbody>
</table>

**Example**

```plaintext
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)#
```

**Related Commands**

**Note**
6.7 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.

Warning: 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.

6.7.1 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
```
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
  MAGP state: Master
  MAGP virtual IP: 11.11.11.254
switch (config)#
```

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](https://community.mellanox.com/docs/DOC-1476).
6.7.2 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.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>Disabled</td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Config</td>
</tr>
<tr>
<td>History</td>
<td>3.3.4500</td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
</tr>
</tbody>
</table>
| Example            | switch (config)# protocol magp  
                    | switch (config)#          |
| Related Commands   |            |
| Note               | IP routing must be enabled to enable MAGP. |
**magp**

```bash
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.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>instance</td>
<td>MAGP instance number. Range: 1-255.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disabled</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Configuration Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>Config Interface VLAN</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>History</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.3.4500</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>admin</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>switch (config interface vlan 20)# magp 100</td>
</tr>
<tr>
<td>switch (config interface vlan 20 magp 100)#</td>
</tr>
</tbody>
</table>

| Related Commands |

<table>
<thead>
<tr>
<th>Note</th>
</tr>
</thead>
<tbody>
<tr>
<td>Only one MAGP instance can be created on an interface</td>
</tr>
<tr>
<td>Different interfaces cannot share an MAGP instance</td>
</tr>
<tr>
<td>MAGP and VRRP are mutually exclusive</td>
</tr>
</tbody>
</table>
**shutdown**

```
shutdown
no shutdown
```

Enables MAGP instance.
The no form of the command disables the MAGP instance.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>Disabled</td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Config Interface VLAN MAGP</td>
</tr>
<tr>
<td>History</td>
<td>3.3.4500</td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
</tr>
<tr>
<td>Example</td>
<td><code>switch (config interface vlan 10 magp 1)# shutdown</code></td>
</tr>
</tbody>
</table>

**Related Commands**

**Note**
### ip virtual-router address

**Syntax**

```
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.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip-address</td>
<td>The virtual router IP address.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Default</th>
<th>N/A</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Configuration Mode</th>
<th>Config Interface VLAN MAGP</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>History</th>
<th>3.3.4500</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Role</th>
<th>admin</th>
</tr>
</thead>
</table>

| Example | switch (config interface vlan 10 magp 1)# ip virtual-router address 10.10.10.10
switch (config interface vlan 10 magp 1)# |
|---------|----------------------------------------|

**Related Commands**

**Note**
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.

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>00:00:5E:00:01-&lt;magp instance&gt;</td>
<td></td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Config Interface VLAN MAGP</td>
<td></td>
</tr>
<tr>
<td>History</td>
<td>3.3.4500</td>
<td></td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
<td></td>
</tr>
<tr>
<td>Example</td>
<td>switch (config interface vlan 10 magp 1)# ip virtual-router mac-address AA:BB:CC:DD:EE:FF</td>
<td></td>
</tr>
<tr>
<td></td>
<td>switch (config interface vlan 10 magp 1)#</td>
<td></td>
</tr>
</tbody>
</table>

Related Commands

Note
**show magp**

`show magp [instance <instance> | interface vlan <id>]`

Displays the configuration of a specific MAGP instance.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>instance</th>
<th>MAGP instance number. Range: 1-255.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>N/A</td>
<td></td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Any Command Mode</td>
<td></td>
</tr>
<tr>
<td>History</td>
<td>3.3.4500</td>
<td></td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
<td></td>
</tr>
<tr>
<td>Example</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>switch (config)# show magp 3</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Magp instance id: 3</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Interface : vlan 10</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Magp state: Active</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Magp virtual ip :192.168.1.1</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Magp virtual MAC : 00:11:22:22:44:55</td>
<td></td>
</tr>
<tr>
<td></td>
<td>switch (config)#</td>
<td></td>
</tr>
</tbody>
</table>

**Related Commands**

**Note**
6.8 DHCP Relay

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.

6.8.1 DHCP-R 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 1231 for more information.
### 6.8.2 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.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>instance-id</th>
<th>Range: 1-8</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>N/A</td>
<td></td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Config</td>
<td></td>
</tr>
<tr>
<td>History</td>
<td>3.6.3004</td>
<td></td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
<td></td>
</tr>
</tbody>
</table>
| Example            | switch (config)# ip dhcp relay instance 1
                   | switch (config ip dhcp relay instance 1)# |
| Related Commands   | N/A         |            |
| Note               | 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.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip-address</td>
<td>Valid IP unicast address of DHCP server.</td>
</tr>
</tbody>
</table>

| Default | N/A |

<table>
<thead>
<tr>
<th>Configuration Mode</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Config IP DHCP Relay</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>History</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.3.4150</td>
<td></td>
</tr>
<tr>
<td>3.6.1002</td>
<td>Added VRF parameter</td>
</tr>
<tr>
<td>3.6.3004</td>
<td>Enhanced command for DHCP-R multi-instance</td>
</tr>
</tbody>
</table>

| Role | admin |

<table>
<thead>
<tr>
<th>Example</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>switch (config ip dhcp relay instance 1)# address 1.2.3.4</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Related Commands</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip dhcp relay</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Note</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• Up to 16 IP addresses may be configured</td>
</tr>
<tr>
<td></td>
<td>• 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”</td>
</tr>
<tr>
<td></td>
<td>• 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).</td>
</tr>
</tbody>
</table>
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.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>vrf</th>
<th>VRF name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>Disabled</td>
<td></td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Config IP DHCP Relay</td>
<td></td>
</tr>
<tr>
<td>History</td>
<td>3.3.4150</td>
<td></td>
</tr>
<tr>
<td></td>
<td>3.6.1002 Added VRF parameter</td>
<td></td>
</tr>
<tr>
<td></td>
<td>3.6.3004 Enhanced command for DHCP-R multi-instance</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Role</th>
<th>admin</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Example</th>
<th>switch (config ip dhcp relay instance 1)# always-on</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Related Commands</th>
<th>ip dhcp relay</th>
</tr>
</thead>
</table>

| Note | | Broadcasts DHCP requests to all interfaces with the DHCP relay agent for given VRF |
|------|--------------------------|
|      | 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 |
|      | When DHCP servers are configured, requests are forwarded only to configured servers |
|      | 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). |
**information option**

```markdown
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.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>Disabled</td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Config IP DHCP Relay</td>
</tr>
<tr>
<td>History</td>
<td>3.3.4150</td>
</tr>
<tr>
<td></td>
<td>3.6.3004 Enhanced command for DHCP-R multi-instance</td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
</tr>
<tr>
<td>Example</td>
<td>switch (config ip dhcp relay instance 1)# information option</td>
</tr>
<tr>
<td>Related Commands</td>
<td>ip dhcp relay</td>
</tr>
<tr>
<td>Note</td>
<td>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).</td>
</tr>
</tbody>
</table>
**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.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>N/A</td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Config IP DHCP Relay</td>
</tr>
<tr>
<td>History</td>
<td>3.6.3004</td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
</tr>
<tr>
<td>Example</td>
<td>switch (config ip dhcp relay instance 1)# vrf 2</td>
</tr>
<tr>
<td>Related Commands</td>
<td>N/A</td>
</tr>
</tbody>
</table>
| Note               | • If no VRF is specified, then the DHCP-R instance is created in the active VRF  
                     • If the VRF is changed, then the configuration of the DHCP-R instance is automatically deleted  
                     • The following option for running this command is also possible: ip dhcp relay instance 1 vrf `<vrf-name>`. However, if an instance is not specified then instance 1 is used (if nonexistent, then it is created). |
### 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.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>udp-port</th>
<th>UDP port Range: 1-65534</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>67</td>
<td></td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Config IP DHCP Relay</td>
<td></td>
</tr>
<tr>
<td>History</td>
<td>3.6.3004</td>
<td></td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
<td></td>
</tr>
<tr>
<td>Example</td>
<td>switch (config ip dhcp relay instance 1)# port 65534</td>
<td></td>
</tr>
<tr>
<td>Related Commands</td>
<td>N/A</td>
<td></td>
</tr>
</tbody>
</table>
| Note               | - The system allocated 2 ports: One is the server port (udp-port), and another is client port (udp-port+1).
- The following option for running this command is also possible: ip dhcp relay instance 1 port <udp-port>. However, if an instance is not specified then instance 1 is used (if nonexistent, then it is created). |
**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

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>N/A</td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Config IP DHCP Relay</td>
</tr>
<tr>
<td>History</td>
<td>3.6.3004</td>
</tr>
<tr>
<td>Role</td>
<td>admin</td>
</tr>
<tr>
<td>Example</td>
<td>switch (config ip dhcp relay instance 1)# vrf-auto-helper</td>
</tr>
<tr>
<td>Related Commands</td>
<td>N/A</td>
</tr>
</tbody>
</table>
| Note               | • 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  
• 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). |
### 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.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>instance-id</th>
<th>DHCP instance ID</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Range: 1-8</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Default</th>
<th>N/A</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Configuration Mode</th>
<th>Config Interface VLAN</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Config Interface Port Channel</td>
</tr>
<tr>
<td></td>
<td>Config Interface Ethernet set as router port interface</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>History</th>
<th>3.6.3004</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Role</th>
<th>admin</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Example</th>
<th>switch (config interface vlan 10)# ip dhcp relay instance 7</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Related Commands</th>
<th>N/A</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Note</th>
</tr>
</thead>
<tbody>
<tr>
<td>• 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”</td>
</tr>
<tr>
<td>• When DHCP servers are configured, requests are forwarded only to configured servers</td>
</tr>
<tr>
<td>• Only an existent DHCP-R may be specified</td>
</tr>
</tbody>
</table>
clear ip dhcp relay counters

```
clear ip dhcp relay counters [vrf <vrf-name> | instance <instance-id>]
```

Clears all DHCP relay counters (all interfaces) in a given VRF or instance.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>vrf-name</th>
<th>VRF name</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>instance-id</td>
<td>DHCP instance ID</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Range: 1-8</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Default</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuration Mode</td>
<td>Config</td>
</tr>
<tr>
<td>History</td>
<td>3.3.4150</td>
</tr>
<tr>
<td></td>
<td>3.6.1002</td>
</tr>
<tr>
<td></td>
<td>3.6.3004</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Role</th>
<th>admin</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Example</th>
<th>switch (config)# clear ip dhcp relay counters</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Related Commands</th>
<th>N/A</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Note</th>
</tr>
</thead>
<tbody>
<tr>
<td>• If no DHCP-R instance is specified, then the counters of all DHCP-R instances are cleared</td>
</tr>
<tr>
<td>• If a VRF is specified, then the counters of all instances on that VRF are cleared</td>
</tr>
<tr>
<td>• The command “clear counters all” may also be used to clear all DHCP-R counters</td>
</tr>
</tbody>
</table>
### ip dhcp relay information option circuit-id

**Syntax**

```plaintext
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.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>label</th>
<th>Specifies the label attached to packets. The string may be up to 15 characters.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>The label is taken from the IP interface name (e.g. “vlan1”).</td>
<td></td>
</tr>
</tbody>
</table>
| Configuration Mode | Config Interface VLAN
  Config Interface Ethernet set as router port interface
  Config Interface Port Channel set as router port interface |
| History            | 3.3.4150 |
|                    | 3.6.1002 | Added VRF parameter |
| Role               | admin |
| Example            | switch (config interface vlan 10)# ip dhcp relay information options circuit-id my-label |
| Related Commands   | N/A |
| Note               | The circuit ID sub-option is an IP interface attribute which is shared across all DHCP-R instances. |
### show ip dhcp relay

**show ip dhcp relay [instance <instance-id>]**

Displays general DHCP configuration.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>instance-id</td>
<td>If instance ID is specified, then a particular instance configuration is displayed</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Default</th>
<th>N/A</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Configuration Mode</th>
<th>Any Command Mode</th>
</tr>
</thead>
</table>

**History**

- 3.3.4150
- 3.6.1002 Added VRF and all parameters
- 3.6.3004 Updated output and parameters

<table>
<thead>
<tr>
<th>Role</th>
<th>admin</th>
</tr>
</thead>
</table>

**Example**

```
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

<table>
<thead>
<tr>
<th>Interface</th>
<th>Label</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan40</td>
<td>N/A</td>
</tr>
<tr>
<td>vlan50</td>
<td>my-instance</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Related Commands</th>
<th>N/A</th>
</tr>
</thead>
</table>

**Note**

If no DHCP-R instance is given, then all DHCP-R instances are displayed

### show ip dhcp relay counters

**show ip dhcp relay counters [vrf <vrf-name> | all]**

Displays the DHCP relay counters in a given VRF.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vrf</td>
<td>VRF name</td>
</tr>
<tr>
<td>all</td>
<td>All VRF instances</td>
</tr>
</tbody>
</table>

**Related Commands**

N/A
Default: N/A
Configuration Mode: Any Command Mode
History: 3.3.4150
3.6.1002 Added VRF and all parameters
Role: admin
Example:
```
switch (config) # VRF Name: user

<table>
<thead>
<tr>
<th>Interface</th>
<th>Received</th>
<th>Forwarded</th>
<th>Dropped</th>
</tr>
</thead>
<tbody>
<tr>
<td>All Req</td>
<td>2</td>
<td>2</td>
<td>0</td>
</tr>
<tr>
<td>All Resp</td>
<td>2</td>
<td>2</td>
<td>0</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Interface</th>
<th>Received</th>
<th>Forwarded</th>
<th>Dropped</th>
<th>Last Cleared</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vlan10</td>
<td>2</td>
<td>2</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>Vlan20</td>
<td>2</td>
<td>2</td>
<td>0</td>
<td></td>
</tr>
</tbody>
</table>
```

VRF Name: default
```

<table>
<thead>
<tr>
<th>Interface</th>
<th>Received</th>
<th>Forwarded</th>
<th>Dropped</th>
</tr>
</thead>
<tbody>
<tr>
<td>All Req</td>
<td>3</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>All Resp</td>
<td>3</td>
<td>3</td>
<td>0</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Interface</th>
<th>Received</th>
<th>Forwarded</th>
<th>Dropped</th>
<th>Last Cleared</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vlan30</td>
<td>3</td>
<td>2</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>Vlan40</td>
<td>3</td>
<td>3</td>
<td>0</td>
<td></td>
</tr>
</tbody>
</table>
```

Related Commands: N/A
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

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

➤ To configure a default certificate:

Step 1. Create a new sha256 certificate. Run:

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

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

Step 2. Show crypto certificate detail. Run:

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

Search for “signature algorithm” in the output.

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

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

➤ To configure default parameters and create a new certificate:

Step 1. Define the default hash algorithm. Run:

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

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

```
switch (config) # crypto certificate name <cert name> generate self-signed
```
When no options are selected, the generated certificate uses the default values for each field.

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

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

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

Make sure not to confuse “signature algorithm” with “Thumbprint algorithm”.

### A.3 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.

### HTTPS

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

- RSA_WITH_AES_128_CBC_SHA256
- RSA_WITH_AES_256_CBC_SHA256
- DHE_RSA_WITH_AES_128_CBC_SHA256
- DHE_RSA_WITH_AES_256_CBC_SHA256
- TLS_RSA_WITH_AES_128_GCM_SHA256
- TLS_RSA_WITH_AES_256_GCM_SHA384
- TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
To enable all encryption methods, run:

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

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

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

To enable HTTPS strict mode, run:

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

To verify which encryption methods are used, run:

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

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

Web file transfer proxy:
  Proxy enabled: no

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

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

To disable HTTP, run:

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

### A.6 LDAP

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

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

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

```bash
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: Mellanox NEO™ on Switch

Mellanox NEO is a powerful platform for data center network orchestration and management. Mellanox NEO enables data center operators to efficiently provision, monitor and operate the modern data center fabric.

Mellanox NEO serves as interface to the fabric, thereby extending existing tools’ capabilities into monitoring and provisioning the data center network. Mellanox NEO uses an extensive set of REST APIs to allow access to fabric-related data and provisioning activities.

Mellanox NEO eliminates the complexity of fabric management. It automates the configuration of devices, provides deep visibility into traffic and health, and provides early detection of errors and failures.

For more information on Mellanox NEO, please refer to the NEO product brief at: [http://www.mellanox.com/related-docs/prod_management_software/PB_Mellanox_NEO.pdf](http://www.mellanox.com/related-docs/prod_management_software/PB_Mellanox_NEO.pdf).

Starting with MLNX-OS® version 3.6.2000 and NEO version 1.7, Mellanox NEO is supported on switch systems with x86 CPU architecture. Mellanox NEO is able to operate as a virtual machine directly on your switch system. Running NEO on the switch is an ideal solution for small-to-medium sized fabrics, with up to 10 Mellanox switches. Simply allocate one (or more for high-availability) of your Mellanox switches to host the Mellanox NEO virtual machine. Then follow the installation instructions in Section B.1.

After its deployment, NEO will automatically discover your Mellanox switches over the management interface allowing you to provision and monitor all of your Mellanox Ethernet switches from a single pain-of-glass using Mellanox NEO software.

B.1 Deploying Mellanox NEO™ on a MLNX-OS® Switch

**Step 1.** Obtain the NEO image and Mellanox-supplied installation script and load it on a USB drive.

**Step 2.** Insert the USB drive into your switch system’s USB port.

**Step 3.** Log into the switch and enter config mode. Run:

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

**Step 4.** Enable virtual machine (VM) on the switch. Run:

```plaintext
switch (config) # virtual-machine enable
```

**Step 5.** Create a VM. Run:

```plaintext
switch (config)# virtual-machine host my_NEO
switch (config virtual-machine host my_NEO)#
```

**Step 6.** Install the NEO image from the USB drive.

**Step a.** To obtain an IP address from the DHCP server, run:

```plaintext
switch (config virtual-machine host my_NEO)# install-from-usb
100.0%
[###################################################]
VM host my_NEO MAC is: aa:bb:cc:dd:ee:ff
switch (config virtual-machine host my_NEO)#
```
Step b. Alternatively, to configure your own MAC address, run:

```
switch (config virtual-machine host my_NEO)# install-from-usb mac aa:bb:cc:dd:ee:ff
100.0%
[######################
#########################################################
] VM host my_NEO MAC is: aa:bb:cc:dd:ee:ff
switch (config virtual-machine host my_NEO)#
```

For more information on the command, please refer to “switch (config virtual-machine host my_NEO)# install-from-usb” on page 1243.

Step 7. Save the VM configuration. Run:

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

Step 8. Obtain the VM’s IP address from the DHCP server by using the provided MAC address.

Step 9. Connect to NEO’s GUI by entering this IP address into your web browser.

## B.2 Getting Familiar with Mellanox NEO GUI

The screen captions used in this section are relevant for NEO 1.7 only. For more up-to-date information, please refer to the Mellanox NEO User Manual.

The Mellanox NEO software has several main GUI views. Before exploring the different options, it is recommended to perform the following steps:

The steps below can be performed by administrators only.

1. Click the “Settings” tab:
   a. Select the “Users” view to add new Mellanox NEO users, and define users’ roles and credentials.
   b. Select the “Email” view to add recipient lists. Upon user’s definition, these lists could be used to distribute specific event alerts to a group of recipients.
2. Click the “Events” tab to activate and deactivate events, and define the severity, condition-value, description and notification parameters for each event.

### B.2.1 Account Password, General Information, User Manual and Log-out Menu

By clicking on the small profile icon at the top right corner of the interface’s frame, a drop down menu appears. Users can change their account password, read about the Mellanox NEO version used, access the User Manual, and log-out of the system.
**Figure 37: NEO GUI**

**B.2.2 Network Notifications Icon**

Clicking on the small envelope icon on the top right corner of the interface’s frame, will lead to the “Notifications” tab. The number next to the icon indicates the quantity of unread network notifications.

**B.2.3 Main Tabs/Categories/Navigator Buttons**

The following table describes the main Mellanox NEO™ windows and categories:

*Table 58 - Navigator Tabs*

<table>
<thead>
<tr>
<th>Icon</th>
<th>Function</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>🌐</td>
<td>Dashboard</td>
<td>Provides single view highlighting information and network status.</td>
</tr>
<tr>
<td>🏛️</td>
<td>Managed Elements</td>
<td>Provides a list of devices, inventory, ports and groups.</td>
</tr>
<tr>
<td>💼</td>
<td>Network Map</td>
<td>Provides a visual view of the physical connectivity between managed devices.</td>
</tr>
<tr>
<td>🔧</td>
<td>Services</td>
<td>Provides automation tools for complex networking configurations.</td>
</tr>
<tr>
<td>📊</td>
<td>Reports</td>
<td>Presents several reports of information collected by the management system, and allows to save and load them.</td>
</tr>
<tr>
<td>🖼️</td>
<td>Tasks</td>
<td>Displays future scheduled Jobs.</td>
</tr>
<tr>
<td>🕵️</td>
<td>Jobs</td>
<td>Displays all the running and completed jobs in the system.</td>
</tr>
<tr>
<td>⚠️</td>
<td>Events</td>
<td>Provides notification events or critical device faults of the switch and server data events. The “Events Policy” view allows the user to activate and deactivate events, and define the severity, condition-value, description and notification parameters for each event.</td>
</tr>
</tbody>
</table>
Table 58 - Navigator Tabs

<table>
<thead>
<tr>
<th>Icon</th>
<th>Function</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Notifications</td>
<td>Available for administrators only. Displays all network notifications.</td>
</tr>
<tr>
<td></td>
<td>Logs</td>
<td>Available for administrators only. Displays detailed logs and alarms that are filtered and sorted by category.</td>
</tr>
<tr>
<td></td>
<td>System Health</td>
<td>Available for administrators only. Provides information on Mellanox NEO building blocks.</td>
</tr>
</tbody>
</table>

B.2.3.1 Dashboard Window

The Mellanox NEO dashboard enables an efficient network view from a single screen, and serves as a starting point for event or metric exploration. The central dashboard provides single view highlighting information and network status in the following smaller dashboard windows:

- Last 24 Hours Events
- Devices Heatmap
- Fabric Utilization (pie chart which also appears in the daily report)
- Top Alerted Devices
- Recent Activity

B.2.3.2 Network Map Window

The Network Map window shows the fabric, its topology, elements and properties. NEO performs automatic fabric discovery and displays the fabric elements and the connectivity between the elements. In the Network Map window you can see how the fabric and its elements are organized (e.g., switches and servers).

B.2.3.3 Services Window

The Tools panel provides automation tools for complex networking configurations. The tools available in this panel are: Virtual Modular Switch, Lossless Fabric, MLAG, and MTU.

B.2.3.4 Reports Window

The Reports panel presents several reports of information collected by the management system. Mellanox NEO™ offers several options of reports: per ports or per devices.

B.2.3.5 Tasks Window

The Tasks panel presents user’s defined tasks (future scheduled Jobs). The following tasks are supported:

- Selecting a single or multiple devices and setting an action such as software upgrade or provisioning (CLI-command) and the action setting data
- Selecting specific action on device / devices and create a task from this action and its setting data
• Adding or deleting a task
• Dynamically selecting devices using filters (wildcards) tasks

B.2.3.6 Jobs Window

The Jobs panel displays all of Mellanox NEO’s running Jobs. A Job is a running task defined by a user and applied on one or more of the devices (provisioning, software upgraded, switch reboot etc.)

Mellanox NEO users can monitor the progress of a running job, as well as the time it was created, its last update description and its status. The status value can be “Running”, during operation, “Pending”, in case another job is already running, “Completed with Errors”, in case an error has occurred, and “Completed”. To cancel a pending job, right-click on the relevant job, and then choose “Abort”.

Table 59 - Job States

<table>
<thead>
<tr>
<th>Job State</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Created</td>
<td>Job was created and will shortly start running.</td>
</tr>
<tr>
<td>Pending</td>
<td>Job is pending by Mellanox NEO. This state appears in case another job that contains at least one common device is already running.</td>
</tr>
<tr>
<td>Running</td>
<td>The pending job was released and is now running.</td>
</tr>
<tr>
<td>Completed</td>
<td>All sub-jobs were completed successfully</td>
</tr>
<tr>
<td>Completed with Errors</td>
<td>All sub-jobs were completed, but on some of them, errors occurred.</td>
</tr>
<tr>
<td>Aborted</td>
<td>A pending job was canceled by the user.</td>
</tr>
</tbody>
</table>

Figure 38: NEO Jobs

Jobs can also be tasks scheduled by the system. In such cases, the users can monitor the progress of these jobs but cannot control them.
B.2.3.7 Events Window

Mellanox NEO™ includes an advanced granular monitoring engine that provides real time access to switch and server data events. Network events can either be notification events or critical device faults. The events information includes severity, time.

B.2.3.8 Notifications Window

This panel is visible to administrators only.

The “Notifications” tab is Mellanox NEO’s incoming messages box, providing the administrators network notifications.

B.2.3.9 Logs Window

This panel is visible to administrators only.

The Logging panel presents detailed logs and alarms that are filtered and sorted by category, providing visibility into traffic and device events as well as into Mellanox NEO server activity history.

B.2.3.10 System Health Window

This panel is visible to administrators only.

The System Health panel is composed of two windows:

- Providers

  Providers are the building blocks of Mellanox NEO. Each provider runs a specific service such as Managing Device Access, Device Provisioning, and IP Discovery. Providers are controlled by a controller. They can either run together with the controller on the same machine or separately on a different device or VM (or container in the future).

- High Availability

  This window enables configures NEO high availability and is meant to grant more stability to the system.
B.3 Fabric Dashboard for On-Screen Status Monitoring

The screen captions used in this section are relevant for NEO 1.7 only. For more up-to-date information, please refer to the Mellanox NEO User Manual.

The Dashboard contains a snapshot of the network view and day to day required information such as Notifications, Events and Jobs.

**Figure 39: Fabric Dashboard**

Network activities are displayed in the following manner.

**B.3.1 Last 24 Hours Events**

Last 24 Hours Events displays the events that occurred over the last 24 hours in an axis view where each column displays the level of severity per hour. The severity levels are grouped into one column.

**Figure 40: 24-Hour View**
6.8.3 Devices Heatmap

Devices Heatmap displays all the devices in different colors according to the severity of their health state. Once clicked on a certain device, you will be directed to the Devices tab under Managed Elements where you can access all information about that device.

The colors imply the following health states:

- Green – OK
- Grey – Unknown
- Orange – Degraded
- Red – Major
- Dark Red – Critical

Through the Devices Heatmap panel, you can apply filters by clicking the icon (Figure 41).

![Figure 41: Device Heatmap](image)

The following filter dialog will be displayed.

![Figure 42: Device Heatmap Dialog](image)

After customizing a certain filter for the devices, you can choose either the red or the green color to denote the devices that match your filter.

**Example:**

If you wish to filter for the devices that their CPU load is greater than 5, you need to select the “CPU Load” as the Attribute, the “>” icon as the Operator, and “5” as the Threshold. If you wish to view the devices you filtered in green, choose the green color as the Matching Color (Figure 43).
Once clicked on “Submit”, the customized filter will be added to the bottom of the Devices Heatmap panel in the Dashboard (see below). The filters will be stored in the browser’s local storage so on any user login or page reload, the heatmap panel will remain saved with all applied filters.

On the right side of the panel, you can find:

- Brief text that describes the filtered criterion, and a square icon colored with the Matching Color (in this example, CPU Load > 5, green). If you click on the description, you will be able to edit your current customized filter.

- Recycle bin icon ( ☞ ) that enables you to delete the filtered heatmap.

- Help icon (“?”) that displays your devices’ criteria according to the defined colors.
6.8.4 Fabric Utilization

Fabric Utilization displays information on groups of switches in a pie chart view where each switch belongs to a group according to its utilization status.

**Figure 46: NEO Fabric Utilization Display**

Utilization of all devices which are part of a specific category can be seen by clicking on any of the colors in the pie chart.

**Figure 47: Fabric Utilization of Device per Category**

![Pie chart with utilization levels]

6.8.5 Top Alerted Devices

Top Alerted Devices displays the total amount of critical events for the selected switches.
Figure 48: Top Alerted Devices

6.8.6 Recent Activity

Recent Activity provides direct access to the most recent 20 events, jobs and notifications in a date descending order.

Once clicked on the Event icon on the left side of each activity, you will be directed to the Events tab where you can access all information about that event.

Table 60 - Recent Activity Icon Description

<table>
<thead>
<tr>
<th>Icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>🔄</td>
<td>Jobs</td>
</tr>
<tr>
<td>📣</td>
<td>Events</td>
</tr>
<tr>
<td>💌</td>
<td>Notifications</td>
</tr>
</tbody>
</table>

Figure 49: Recent Activity Examples
Appendix C: Show Commands Supported by JSON API

Table 61 lists the “show” commands which currently support JSON API.

The character “*” indicates a wildcard.

Table 61 - JSON API Show Commands

<table>
<thead>
<tr>
<th>Ethernet Commands</th>
</tr>
</thead>
<tbody>
<tr>
<td>show interfaces ethernet transceiver</td>
</tr>
<tr>
<td>show interfaces ethernet * transceiver</td>
</tr>
<tr>
<td>show interface ethernet * status</td>
</tr>
<tr>
<td>show interface ethernet status</td>
</tr>
<tr>
<td>show interfaces ethernet * counters</td>
</tr>
<tr>
<td>show interfaces port-channel * counters</td>
</tr>
<tr>
<td>show interfaces mlag-port-channel * counters</td>
</tr>
<tr>
<td>show interfaces ethernet capabilities</td>
</tr>
<tr>
<td>show ip interface brief</td>
</tr>
<tr>
<td>show ip load-sharing</td>
</tr>
<tr>
<td>show lldp interfaces port-channel * system-identifier</td>
</tr>
<tr>
<td>show lldp timers</td>
</tr>
<tr>
<td>show lldp statistics global</td>
</tr>
<tr>
<td>show qos interface port-channel *</td>
</tr>
<tr>
<td>show vrf</td>
</tr>
<tr>
<td>show vrf *</td>
</tr>
<tr>
<td>show routing-context vrf</td>
</tr>
<tr>
<td>show interfaces ethernet * description</td>
</tr>
<tr>
<td>show interfaces ethernet description</td>
</tr>
<tr>
<td>show interfaces ethernet * transceiver diagnostics</td>
</tr>
<tr>
<td>show interfaces ethernet</td>
</tr>
<tr>
<td>show interfaces ethernet *</td>
</tr>
<tr>
<td>show dot1x interfaces ethernet</td>
</tr>
<tr>
<td>show dot1x interfaces ethernet *</td>
</tr>
<tr>
<td>show ip igmp snooping interfaces</td>
</tr>
<tr>
<td>show ip igmp snooping querier vlan *</td>
</tr>
</tbody>
</table>
### Table 61 - JSON API Show Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show ip igmp snooping querier counters</td>
<td>Show IGMP Snooping Querier Counters</td>
</tr>
<tr>
<td>show ip igmp snooping querier counters vlan *</td>
<td>Show IGMP Snooping Querier Counters for VLANs</td>
</tr>
<tr>
<td>show ip igmp snooping querier counters vlan * group *</td>
<td>Show IGMP Snooping Querier Counters for VLANs and Groups</td>
</tr>
<tr>
<td>show ip igmp snooping vlan *</td>
<td>Show IGMP Snooping Counters for VLANs</td>
</tr>
<tr>
<td>show ip igmp snooping statistics</td>
<td>Show IGMP Snooping Statistics</td>
</tr>
<tr>
<td>show ip igmp snooping mrouter</td>
<td>Show IGMP Snooping MRouters</td>
</tr>
<tr>
<td>show interfaces vlan</td>
<td>Show VLAN Interfaces</td>
</tr>
<tr>
<td>show interfaces vlan *</td>
<td>Show VLAN Interfaces for Multiple VLANs</td>
</tr>
<tr>
<td>show interfaces vlan status</td>
<td>Show VLAN Interface Status</td>
</tr>
<tr>
<td>show ip arp count</td>
<td>Show IP ARP Count</td>
</tr>
<tr>
<td>show ip interface vlan *</td>
<td>Show IP Interface for VLANs</td>
</tr>
<tr>
<td>show interfaces port-channel</td>
<td>Show Port-Channel Interfaces</td>
</tr>
<tr>
<td>show interfaces port-channel *</td>
<td>Show Port-Channel Interfaces for Multiple Port-Channels</td>
</tr>
<tr>
<td>show interfaces port-channel load-balance</td>
<td>Show Port-Channel Load-Balance</td>
</tr>
<tr>
<td>show interfaces mlag-port-channel</td>
<td>Show MLAG Port-Channel Interfaces</td>
</tr>
<tr>
<td>show interfaces mlag-port-channel *</td>
<td>Show MLAG Port-Channel Interfaces for Multiple Port-Channels</td>
</tr>
<tr>
<td>show openflow tables</td>
<td>Show OpenFlow Tables</td>
</tr>
<tr>
<td>show isolation-group</td>
<td>Show Isolation-Group</td>
</tr>
<tr>
<td>show isolation-group *</td>
<td>Show Multiple Isolation-Groups</td>
</tr>
<tr>
<td>show interfaces proxy-arp</td>
<td>Show Proxy-ARP Interfaces</td>
</tr>
<tr>
<td>show interfaces proxy-arp *</td>
<td>Show Multiple Proxy-ARP Interfaces</td>
</tr>
<tr>
<td>show qos interface ethernet *</td>
<td>Show QoS for Ethernet Interfaces</td>
</tr>
<tr>
<td>show qos interface mlag-port-channel *</td>
<td>Show QoS for MLAG Port-Channel Interfaces</td>
</tr>
<tr>
<td>show mac-address-table aging-time</td>
<td>Show MAC Address Table Aging-Time</td>
</tr>
<tr>
<td>show mac-address-table summary</td>
<td>Show MAC Address Table Summary</td>
</tr>
<tr>
<td>show vrrp</td>
<td>Show VRRP Settings</td>
</tr>
<tr>
<td>show vrrp vr *</td>
<td>Show VRRP Configuration for Multiple VRs</td>
</tr>
<tr>
<td>show vrrp interface vlan *</td>
<td>Show VRRP Interfaces for Multiple VLANs</td>
</tr>
<tr>
<td>show vrrp interface vlan * vr</td>
<td>Show VRRP Interfaces for Multiple VR and VLANs</td>
</tr>
<tr>
<td>show vrrp statistics</td>
<td>Show VRRP Statistics</td>
</tr>
<tr>
<td>show vrrp statistics vr *</td>
<td>Show VRRP Statistics for Multiple VRs</td>
</tr>
<tr>
<td>show vrrp statistics interface vlan *</td>
<td>Show VRRP Statistics for Multiple VR and VLANs</td>
</tr>
</tbody>
</table>
### Table 61 - JSON API Show Commands

<table>
<thead>
<tr>
<th>Chassis Management Commands</th>
</tr>
</thead>
<tbody>
<tr>
<td>show leds</td>
</tr>
<tr>
<td>show leds *</td>
</tr>
<tr>
<td>show battery-backup-unit * detail</td>
</tr>
<tr>
<td>show asic-version</td>
</tr>
<tr>
<td>show bios</td>
</tr>
<tr>
<td>show inventory</td>
</tr>
<tr>
<td>show fan</td>
</tr>
<tr>
<td>show module</td>
</tr>
<tr>
<td>show system capabilities</td>
</tr>
<tr>
<td>show system profile</td>
</tr>
<tr>
<td>show version</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>General Commands</th>
</tr>
</thead>
<tbody>
<tr>
<td>show ha dns</td>
</tr>
<tr>
<td>show files system</td>
</tr>
<tr>
<td>show stats sample</td>
</tr>
<tr>
<td>show stats sample *</td>
</tr>
<tr>
<td>show stats chd</td>
</tr>
<tr>
<td>show stats chd *</td>
</tr>
<tr>
<td>show stats cpu</td>
</tr>
<tr>
<td>show whoami</td>
</tr>
<tr>
<td>show users</td>
</tr>
<tr>
<td>show usernames</td>
</tr>
<tr>
<td>show xml-gw</td>
</tr>
<tr>
<td>show services small-servers</td>
</tr>
<tr>
<td>show ftp-server</td>
</tr>
<tr>
<td>show telnet-server</td>
</tr>
<tr>
<td>show memory</td>
</tr>
<tr>
<td>show configuration</td>
</tr>
<tr>
<td>show configuration expanded</td>
</tr>
<tr>
<td>show configuration running</td>
</tr>
<tr>
<td>show running-config</td>
</tr>
<tr>
<td>show running-config expanded</td>
</tr>
<tr>
<td>show running-config protocol</td>
</tr>
</tbody>
</table>