

IBM Flex System Fabric EN4093 and EN4093R 10Gb Scalable Switch



ISCLI—Industry Standard CLI Command Reference

for IBM Networking OS 7.7

Note: Before using this information and the product it supports, read the general information in the *Safety information and Environmental Notices and User Guide* documents on the *IBM Documentation* CD and the *Warranty Information* document that comes with the product.

First Edition (August 2013)

IBM Flex System Fabric EN4093 and EN4093R 10Gb Scalable Switch ISCLI Command Reference

US Government Users Restricted Rights – Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

Contents

| | |
|---|-------------|
| Preface | xiii |
| Who Should Use This Book | xiv |
| How This Book Is Organized | xv |
| Typographic Conventions | xvi |
| | |
| Chapter 1. ISCLI Basics | .1 |
| Accessing the ISCLI | .2 |
| ISCLI Command Modes | .3 |
| Global Commands | .7 |
| Command Line Interface Shortcuts | .9 |
| CLI List and Range Inputs | .9 |
| Command Abbreviation | .9 |
| Tab Completion | .9 |
| User Access Levels | 10 |
| Idle Timeout | 12 |
| | |
| Chapter 2. Information Commands | 13 |
| System Information | 14 |
| CLI Display Information | 15 |
| Error Disable and Recovery Information | 16 |
| SNMPv3 System Information | 17 |
| SNMPv3 USM User Table Information | 18 |
| SNMPv3 View Table Information | 19 |
| SNMPv3 Access Table Information | 20 |
| SNMPv3 Group Table Information | 20 |
| SNMPv3 Community Table Information | 21 |
| SNMPv3 Target Address Table Information | 21 |
| SNMPv3 Target Parameters Table Information | 23 |
| SNMPv3 Notify Table Information | 23 |
| SNMPv3 Dump Information | 24 |
| General System Information | 25 |
| Show Software Version Brief Information | 26 |
| Show Specific System Information | 26 |
| Show Recent Syslog Messages | 27 |
| User Status | 28 |
| Stacking Information | 29 |
| Stacking Switch Information | 30 |
| Attached Switches Information | 31 |
| Stack Name Information | 32 |
| Stack Backup Switch Information | 32 |
| Stack Version Information | 32 |
| Stack Packet Path Information | 33 |
| Stack Push Status Information | 33 |
| Layer 2 Information | 35 |
| FDB Information | 37 |
| Show All FDB Information | 38 |
| Show FDB Multicast Address Information | 39 |
| Clearing Entries from the Forwarding Database | 39 |
| Link Aggregation Control Protocol Information | 40 |
| Link Aggregation Control Protocol | 40 |
| Layer 2 Failover Information Commands | 41 |

| | |
|--|----|
| Layer 2 Failover Information | 41 |
| Hot Links Information | 42 |
| Edge Control Protocol Information | 42 |
| LLDP Information | 43 |
| LLDP Remote Device Information | 44 |
| Unidirectional Link Detection Information | 45 |
| UDLD Port Information | 45 |
| OAM Discovery Information | 46 |
| OAM Port Information | 46 |
| vLAG Information | 47 |
| vLAG Trunk Information | 47 |
| 802.1X Information | 48 |
| Spanning Tree Information | 50 |
| RSTP/MSTP/PVRST Information | 52 |
| Common Internal Spanning Tree Information | 54 |
| Trunk Group Information | 56 |
| VLAN Information | 57 |
| Layer 3 Information | 59 |
| IP Routing Information. | 62 |
| Show All IP Route Information | 63 |
| ARP Information | 64 |
| Show All ARP Entry Information | 65 |
| ARP Address List Information | 65 |
| BGP Information | 66 |
| BGP Peer information | 67 |
| BGP Summary Information | 67 |
| BGP Peer Routes Information | 67 |
| Dump BGP Information. | 67 |
| OSPF Information | 68 |
| OSPF General Information | 69 |
| OSPF Interface Loopback Information | 70 |
| OSPF Interface Information | 70 |
| OSPF Database Information. | 71 |
| OSPF Information Route Codes | 72 |
| OSPFv3 Information | 73 |
| OSPFv3 Information Dump | 74 |
| OSPFv3 Interface Information | 75 |
| OSPFv3 Database Information. | 75 |
| OSPFv3 Route Codes Information | 76 |
| Routing Information Protocol | 77 |
| RIP Routes Information. | 77 |
| RIP Interface Information | 77 |
| IPv6 Routing Information. | 78 |
| IPv6 Routing Table | 78 |
| IPv6 Neighbor Discovery Cache Information | 79 |
| IPv6 Neighbor Discovery Cache Information | 79 |
| IPv6 Neighbor Discovery Prefix Information | 80 |
| ECMP Static Route Information | 80 |
| ECMP Hashing Result. | 81 |
| IGMP Multicast Group Information | 81 |
| IGMP Querier Information. | 82 |
| IGMP Group Information | 83 |
| IGMP Multicast Router Information | 84 |

| | |
|---|-----|
| IPMC Group Information | 84 |
| MLD information | 85 |
| VRRP Information | 87 |
| Interface Information | 87 |
| IPv6 Interface Information | 88 |
| IPv6 Path MTU Information | 88 |
| IP Information | 89 |
| DHCP Snooping Binding Table Information | 90 |
| IKEv2 Information | 91 |
| IKEv2 Information Dump | 92 |
| IPsec Information | 93 |
| IPsec Manual Policy Information | 94 |
| PIM Information | 94 |
| PIM Component Information | 96 |
| PIM Interface Information | 96 |
| PIM Neighbor Information | 97 |
| PIM Multicast Route Information Commands | 97 |
| PIM Multicast Route Information | 98 |
| Quality of Service Information | 99 |
| 802.1p Information | 99 |
| WRED and ECN Information | 100 |
| Access Control List Information Commands | 101 |
| Access Control List Information | 102 |
| OpenFlow Information | 103 |
| OpenFlow Global Configuration Information | 104 |
| OpenFlow Flow Allocation Information | 104 |
| OpenFlow Configuration Information | 105 |
| OpenFlow Table Information | 106 |
| RMON Information Commands | 108 |
| RMON History Information | 109 |
| RMON Alarm Information | 110 |
| RMON Event Information | 111 |
| Link Status Information | 112 |
| Port Information | 114 |
| Port Transceiver Status | 116 |
| Virtual Machines Information | 118 |
| VM Information | 118 |
| VM Check Information | 119 |
| VMware Information | 119 |
| VMware Host Information | 119 |
| EVB Information | 121 |
| vNIC Information | 122 |
| Virtual NIC (vNIC) Information | 122 |
| vNIC Group Information | 123 |
| SLP Information | 124 |
| UFP Information | 124 |
| Port Information | 125 |
| CDCP Information | 126 |
| QoS Information | 126 |
| TLV Status Information | 127 |
| Virtual Port Information | 128 |
| VLAN Information | 128 |
| TLV Information | 129 |

| | |
|---|------------|
| Converged Enhanced Ethernet Information | 130 |
| DCBX Information | 130 |
| DCBX Control Information | 131 |
| DCBX Feature Information | 132 |
| DCBX ETS Information | 132 |
| DCBX PFC Information | 134 |
| DCBX Application Protocol Information | 135 |
| ETS Information | 137 |
| PFC Information | 138 |
| FCoE Information | 139 |
| FIP Snooping Information | 139 |
| Information Dump | 141 |
| Chapter 3. Statistics Commands | 143 |
| Port Statistics | 144 |
| 802.1X Authenticator Statistics | 146 |
| 802.1X Authenticator Diagnostics | 147 |
| Bridging Statistics | 150 |
| Ethernet Statistics | 151 |
| Interface Statistics | 154 |
| Interface Protocol Statistics | 157 |
| Link Statistics | 157 |
| RMON Statistics | 158 |
| QoS Queue Rate-Based Statistics | 160 |
| Trunk Group Statistics | 162 |
| Layer 2 Statistics | 163 |
| LACP Statistics | 164 |
| Hotlinks Statistics | 165 |
| LLDP Port Statistics | 166 |
| OAM Statistics | 167 |
| vLAG Statistics | 167 |
| vLAG ISL Statistics | 168 |
| vLAG Statistics | 168 |
| Layer 3 Statistics | 170 |
| IPv4 Statistics | 173 |
| IPv6 Statistics | 176 |
| IPv4 Route Statistics | 181 |
| IPv6 Route Statistics | 182 |
| ARP statistics | 182 |
| DNS Statistics | 183 |
| ICMP Statistics | 184 |
| TCP Statistics | 186 |
| UDP Statistics | 187 |
| IGMP Statistics | 188 |
| MLD Statistics | 190 |
| MLD Global Statistics | 191 |
| OSPF Statistics | 193 |
| OSPF Global Statistics | 194 |
| OSPFv3 Statistics | 197 |
| OSPFv3 Global Statistics | 198 |
| VRRP Statistics | 201 |
| PIM Statistics | 202 |
| Routing Information Protocol Statistics | 203 |

| | |
|---|------------|
| OpenFlow Statistics | 204 |
| Management Processor Statistics | 212 |
| Packet Statistics | 213 |
| MP Packet Statistics. | 213 |
| Packet Statistics Log | 219 |
| Packet Log example | 219 |
| Packet Statistics Last Packet | 220 |
| Packet Statistics Dump | 220 |
| Logged Packet Statistics | 221 |
| TCP Statistics | 225 |
| UDP Statistics | 226 |
| CPU Statistics | 226 |
| CPU Statistics History | 229 |
| Access Control List Statistics | 230 |
| ACL Statistics | 231 |
| VMAP Statistics | 231 |
| Fibre Channel over Ethernet Statistics | 232 |
| ACL Meter Statistics | 233 |
| SNMP Statistics | 234 |
| NTP Statistics | 238 |
| PTP Statistics | 239 |
| SLP Statistics | 240 |
| Statistics Dump | 242 |
| | |
| Chapter 4. Configuration Commands | 243 |
| Viewing and Saving Changes | 245 |
| System Configuration | 246 |
| System Error Disable and Recovery Configuration | 249 |
| System Host Log Configuration | 250 |
| SSH Server Configuration | 252 |
| RADIUS Server Configuration | 253 |
| TACACS+ Server Configuration | 255 |
| LDAP Server Configuration | 258 |
| NTP Server Configuration | 260 |
| System SNMP Configuration | 263 |
| SNMPv3 Configuration | 265 |
| User Security Model Configuration | 267 |
| SNMPv3 View Configuration | 268 |
| View-based Access Control Model Configuration | 269 |
| SNMPv3 Group Configuration | 270 |
| SNMPv3 Community Table Configuration | 271 |
| SNMPv3 Target Address Table Configuration | 272 |
| SNMPv3 Target Parameters Table Configuration | 273 |
| SNMPv3 Notify Table Configuration | 274 |
| System Access Configuration | 275 |
| Management Network Configuration | 277 |
| User Access Control Configuration | 278 |
| System User ID Configuration | 279 |
| Strong Password Configuration | 280 |
| HTTPS Access Configuration | 281 |
| Custom Daylight Saving Time Configuration | 282 |
| sFlow Configuration | 283 |
| sFlow Port Configuration | 283 |

| | |
|---|-----|
| Port Configuration | 284 |
| Port Error Disable and Recovery Configuration | 287 |
| Port Link Configuration | 287 |
| Temporarily Disabling a Port | 288 |
| Unidirectional Link Detection Configuration | 289 |
| Port OAM Configuration | 290 |
| Port ACL Configuration | 290 |
| Port Spanning Tree Configuration | 291 |
| Port Spanning Tree Guard Configuration | 291 |
| Port WRED Configuration | 292 |
| Port WRED Transmit Queue Configuration | 293 |
| Management Port Configuration | 293 |
| Stacking Configuration | 295 |
| Stacking Switch Configuration | 296 |
| Quality of Service Configuration | 297 |
| 802.1p Configuration | 297 |
| DSCP Configuration | 298 |
| Control Plane Protection | 299 |
| Weighted Random Early Detection Configuration | 300 |
| WRED Transmit Queue Configuration | 301 |
| Access Control Configuration | 302 |
| Access Control List Configuration | 303 |
| Ethernet Filtering Configuration | 304 |
| IPv4 Filtering Configuration | 305 |
| TCP/UDP Filtering Configuration | 306 |
| Packet Format Filtering Configuration | 307 |
| ACL IPv6 Configuration | 307 |
| IPv6 Filtering Configuration | 308 |
| IPv6 TCP/UDP Filtering Configuration | 309 |
| IPv6 Re-Mark Configuration | 310 |
| Management ACL Filtering Configuration | 311 |
| TCP/UDP Filtering Configuration | 312 |
| VMAP Configuration | 313 |
| ACL Group Configuration | 317 |
| ACL Metering Configuration | 318 |
| ACL Re-Mark Configuration | 319 |
| Re-Marking In-Profile Configuration | 320 |
| Re-Marking Out-of-Profile Configuration | 320 |
| IPv6 Re-Marking Configuration | 321 |
| IPv6 Re-Marking In-Profile Configuration | 322 |
| Port Mirroring | 323 |
| Port Mirroring Configuration | 323 |
| Layer 2 Configuration | 324 |
| 802.1X Configuration | 325 |
| 802.1X Global Configuration | 325 |
| 802.1X Guest VLAN Configuration | 327 |
| 802.1X Port Configuration | 328 |
| Spanning Tree Configuration | 330 |
| MSTP/RSTP/PVRST Configuration | 332 |
| Common Internal Spanning Tree Configuration | 333 |
| CIST Bridge Configuration | 333 |
| RSTP/PVRST Configuration | 335 |
| Forwarding Database Configuration | 338 |

| | |
|---|-----|
| Static FDB Configuration | 339 |
| Static Multicast MAC Configuration | 340 |
| ECP Configuration | 341 |
| LLDP Configuration | 341 |
| LLDP Port Configuration | 342 |
| LLDP Optional TLV configuration | 343 |
| Trunk Configuration | 345 |
| IP Trunk Hash Configuration | 346 |
| Layer 2 Trunk Hash | 346 |
| Layer 3 Trunk Hash | 347 |
| Virtual Link Aggregation Control Protocol Configuration | 348 |
| vLAG Health Check Configuration | 349 |
| vLAG ISL Configuration | 350 |
| Link Aggregation Control Protocol Configuration | 351 |
| LACP Port Configuration | 352 |
| Layer 2 Failover Configuration | 353 |
| Failover Trigger Configuration | 354 |
| Auto Monitor Configuration | 354 |
| Failover Manual Monitor Port Configuration | 355 |
| Failover Manual Monitor Control Configuration | 356 |
| Hot Links Configuration | 357 |
| Hot Links Trigger Configuration | 358 |
| Hot Links Master Configuration | 359 |
| Hot Links Backup Configuration | 360 |
| VLAN Configuration | 361 |
| Protocol-Based VLAN Configuration | 363 |
| Private VLAN Configuration | 365 |
| Layer 3 Configuration | 366 |
| IP Interface Configuration | 368 |
| IPv6 Neighbor Discovery Configuration | 370 |
| Default Gateway Configuration | 372 |
| IPv4 Static Route Configuration | 373 |
| IP Multicast Route Configuration | 374 |
| ARP Configuration | 375 |
| ARP Static Configuration | 376 |
| IP Forwarding Configuration | 377 |
| Network Filter Configuration | 378 |
| Routing Map Configuration | 379 |
| IP Access List Configuration | 381 |
| Autonomous System Filter Path Configuration | 382 |
| Routing Information Protocol Configuration | 383 |
| Routing Information Protocol Interface Configuration | 384 |
| RIP Route Redistribution Configuration | 386 |
| Open Shortest Path First Configuration | 387 |
| Area Index Configuration | 389 |
| OSPF Summary Range Configuration | 391 |
| OSPF Interface Configuration | 392 |
| OSPF Virtual Link Configuration | 394 |
| OSPF Host Entry Configuration | 395 |
| OSPF Route Redistribution Configuration | 396 |
| OSPF MD5 Key Configuration | 396 |
| Border Gateway Protocol Configuration | 397 |
| BGP Peer Configuration | 399 |

| | |
|--|-----|
| BGP Redistribution Configuration | 402 |
| BGP Aggregation Configuration | 403 |
| Multicast Listener Discovery Protocol Configuration | 404 |
| IGMP Configuration | 406 |
| IGMP Snooping Configuration | 407 |
| IGMPv3 Configuration | 408 |
| IGMP Relay Configuration | 409 |
| IGMP Relay Multicast Router Configuration | 410 |
| IGMP Static Multicast Router Configuration | 411 |
| IGMP Filtering Configuration | 412 |
| IGMP Filter Definition | 413 |
| IGMP Filtering Port Configuration | 414 |
| IGMP Advanced Configuration | 415 |
| IGMP Querier Configuration | 415 |
| IKEv2 Configuration | 418 |
| IKEv2 Proposal Configuration | 418 |
| IKEv2 Preshare Key Configuration | 419 |
| IKEv2 Identification Configuration | 419 |
| IPsec Configuration | 420 |
| IPsec Transform Set Configuration | 421 |
| IPsec Traffic Selector Configuration | 422 |
| IPsec Dynamic Policy Configuration | 423 |
| IPsec Manual Policy Configuration | 424 |
| Domain Name System Configuration | 426 |
| Bootstrap Protocol Relay Configuration | 427 |
| BOOTP Relay Broadcast Domain Configuration | 427 |
| VRRP Configuration | 429 |
| Virtual Router Configuration | 430 |
| Virtual Router Priority Tracking Configuration | 432 |
| Virtual Router Group Configuration | 433 |
| Virtual Router Group Priority Tracking Configuration | 435 |
| VRRP Interface Configuration | 436 |
| VRRP Tracking Configuration | 437 |
| Protocol Independent Multicast Configuration | 438 |
| PIM Component Configuration | 438 |
| RP Candidate Configuration | 439 |
| RP Static Configuration | 439 |
| PIM Interface Configuration | 440 |
| IPv6 Default Gateway Configuration | 442 |
| IPv6 Static Route Configuration | 443 |
| IPv6 Neighbor Discovery Cache Configuration | 443 |
| IPv6 Path MTU Configuration | 444 |
| IPv6 Neighbor Discovery Prefix Configuration | 444 |
| IPv6 Prefix Policy Table Configuration | 446 |
| Open Shortest Path First Version 3 Configuration | 446 |
| OSPFv3 Area Index Configuration | 448 |
| OSPFv3 Summary Range Configuration | 450 |
| OSPFv3 AS-External Range Configuration | 451 |
| OSPFv3 Interface Configuration | 452 |
| OSPFv3 Virtual Link Configuration | 456 |
| OSPFv3 Host Entry Configuration | 457 |
| OSPFv3 Redist Entry Configuration | 458 |
| OSPFv3 Redistribute Configuration | 459 |

| | |
|--|------------|
| IP Loopback Interface Configuration | 460 |
| Converged Enhanced Ethernet Configuration | 461 |
| ETS Global Configuration | 462 |
| ETS Global Priority Group Configuration | 462 |
| Priority Flow Control Configuration | 463 |
| Port-level 802.1p PFC Configuration | 463 |
| DCBX Port Configuration | 464 |
| Fibre Channel over Ethernet Configuration | 466 |
| FIPS Port Configuration | 467 |
| Remote Monitoring Configuration | 468 |
| RMON History Configuration | 468 |
| RMON Event Configuration | 469 |
| RMON Alarm Configuration | 470 |
| Virtualization Configuration | 472 |
| VM Policy Bandwidth Management | 472 |
| Virtual NIC Configuration | 473 |
| vNIC Port Configuration | 474 |
| Virtual NIC Group Configuration | 474 |
| UFP Configuration | 476 |
| VM Group Configuration | 478 |
| VM Check Configuration | 481 |
| VM Profile Configuration | 482 |
| VMWare Configuration | 483 |
| Miscellaneous VMready Configuration | 484 |
| Edge Virtual Bridge Configuration | 485 |
| Edge Virtual Bridge Profile Configuration | 486 |
| OpenFlow Configuration | 487 |
| Static Flows Configuration | 492 |
| Switch Partition (SPAR) Configuration | 495 |
| Precision Time Protocol Configuration | 497 |
| Service Location Protocol Configuration | 498 |
| Configuration Dump | 500 |
| Saving the Active Switch Configuration | 501 |
| Restoring the Active Switch Configuration | 502 |
| | |
| Chapter 5. Operations Commands | 503 |
| Operations-Level Port Commands | 504 |
| Operations-Level Port 802.1X Commands | 505 |
| Operations-Level FCoE Commands | 506 |
| Operations-Level VRRP Commands | 507 |
| Operations-Level BGP Commands | 508 |
| Protected Mode Options | 509 |
| VMware Operations | 511 |
| VMware Distributed Virtual Switch Operations | 513 |
| VMware Distributed Port Group Operations | 514 |
| Edge Virtual Bridge Operations | 515 |
| | |
| Chapter 6. Boot Options | 517 |
| Stacking Boot Options | 517 |
| Scheduled Reboot | 519 |
| Netboot Configuration | 520 |
| QSFP Port Configuration | 521 |
| Updating the Switch Software Image | 522 |

| | |
|---|------------|
| Loading New Software to Your Switch | 522 |
| Selecting a Software Image to Run. | 523 |
| Uploading a Software Image from Your Switch | 523 |
| Selecting a Configuration Block. | 525 |
| Resetting the Switch | 526 |
| Accessing the Networking OS CLI. | 527 |
| Changing the Switch Profile | 528 |
| Using the Boot Management Menu | 529 |
| Recovering from a Failed Software Upgrade | 529 |
| Recovering a Failed Boot Image. | 531 |
| Chapter 7. Maintenance Commands | 533 |
| Forwarding Database Maintenance | 535 |
| Debugging Commands | 537 |
| IP Security Debugging. | 538 |
| DCBX Debugging Commands | 539 |
| ARP Cache Maintenance | 540 |
| IP Route Manipulation | 541 |
| LLDP Cache Manipulation | 542 |
| IGMP Group Maintenance | 543 |
| IGMP Multicast Routers Maintenance | 544 |
| IPv6 Neighbor Discovery Cache Manipulation | 546 |
| IPv6 Route Maintenance | 547 |
| Uuencode Flash Dump | 548 |
| TFTP, SFTP or FTP System Dump Put. | 549 |
| Clearing Dump Information | 550 |
| Unscheduled System Dumps. | 551 |
| Appendix A. Networking OS System Log Messages | 553 |
| LOG_ALERT | 554 |
| LOG_CRIT | 556 |
| LOG_ERR | 557 |
| LOG_INFO. | 558 |
| LOG_NOTICE | 561 |
| LOG_WARNING | 565 |
| Appendix B. Getting help and technical assistance. | 567 |
| Before you call | 568 |
| Using the documentation | 569 |
| Getting help and information on the World Wide Web | 570 |
| Software service and support | 571 |
| Hardware service and support | 572 |
| IBM Taiwan product service | 573 |
| Index | 575 |

Preface

The *IBM Flex System Fabric EN4093 and EN4093R 10Gb Scalable Switch ISCLI Command Reference* describes how to configure and use the Networking OS 7.7 software with your IBM Flex System Fabric EN4093 and EN4093R 10Gb Scalable Switch. This guide lists each command, together with the complete syntax and a functional description, from the IS Command Line Interface (ISCLI).

For documentation on installing the switches physically, see the *Installation Guide* for your EN4093 and EN4093R. For details about the configuration and operation of the EN4093 and EN4093R, see the *IBM N/OS 7.7 Application Guide*.

Who Should Use This Book

This book is intended for network installers and system administrators engaged in configuring and maintaining a network. The administrator should be familiar with Ethernet concepts, IP addressing, the IEEE 802.1D Spanning Tree Protocol, and SNMP configuration parameters.

How This Book Is Organized

Chapter 1, “ISCLI Basics,” describes how to connect to the switch and access the information and configuration commands. This chapter provides an overview of the command syntax, including command modes, global commands, and shortcuts.

Chapter 2, “Information Commands,” shows how to view switch configuration parameters.

Chapter 3, “Statistics Commands,” shows how to view switch performance statistics.

Chapter 4, “Configuration Commands,” shows how to configure switch system parameters, ports, VLANs, Spanning Tree Protocol, SNMP, Port Mirroring, IP Routing, Port Trunking, and more.

Chapter 5, “Operations Commands,” shows how to use commands which affect switch performance immediately, but do not alter permanent switch configurations (such as temporarily disabling ports). The commands describe how to activate or deactivate optional software features.

Chapter 6, “Boot Options,” describes the use of the primary and alternate switch images, how to load a new software image, and how to reset the software to factory defaults.

Chapter 7, “Maintenance Commands,” shows how to generate and access a dump of critical switch state information, how to clear it, and how to clear part or all of the forwarding database.

Appendix A, “Networking OS System Log Messages,” lists Networking OS System Log Messages.

Appendix B, “Getting help and technical assistance,” contains information on how to get help, service, technical assistance, or more information about IBM products.

“Index” includes pointers to the description of the key words used throughout the book.

Typographic Conventions

The following table describes the typographic styles used in this book.

Table 1. *Typographic Conventions*

| Typeface or Symbol | Meaning |
|-----------------------------|---|
| plain fixed-width text | <p>This type is used for names of commands, files, and directories used within the text. For example:</p> <p>View the <code>readme.txt</code> file.</p> <p>It also depicts on-screen computer output and prompts.</p> |
| bold fixed-width text | <p>This bold type appears in command examples. It shows text that must be typed in exactly as shown. For example:</p> <pre>show sys-info</pre> |
| bold body text | <p>This bold type indicates objects such as window names, dialog box names, and icons, as well as user interface objects such as buttons, and tabs.</p> |
| <i>italicized body text</i> | <p>This italicized type indicates book titles, special terms, or words to be emphasized.</p> |
| angle brackets < > | <p>Indicate a variable to enter based on the description inside the brackets. Do not type the brackets when entering the command.</p> <p>Example: If the command syntax is</p> <pre>ping <IP address></pre> <p>you enter</p> <pre>ping 192.32.10.12</pre> |
| braces { } | <p>Indicate required elements in syntax descriptions where there is more than one option. You must choose only one of the options. Do not type the braces when entering the command.</p> <p>Example: If the command syntax is</p> <pre>show portchannel {<I-64> hash information}</pre> <p>you enter:</p> <pre>show portchannel <I-64></pre> <p>or</p> <pre>show portchannel hash</pre> <p>or</p> <pre>show portchannel information</pre> |

Table 1. *Typographic Conventions*

| Typeface or Symbol | Meaning |
|--------------------|---|
| brackets [] | <p>Indicate optional elements in syntax descriptions. Do not type the brackets when entering the command.</p> <p>Example: If the command syntax is <code>show interface ip [<1-128>]</code></p> <p>you enter <code>show interface ip</code></p> <p>or <code>show interface ip <1-128></code></p> |
| vertical line | <p>Separates choices for command keywords and arguments. Enter only one of the choices. Do not type the vertical line when entering the command.</p> <p>Example: If the command syntax is <code>show portchannel {<1-64> hash information}</code></p> <p>you must enter: <code>show portchannel <1-64></code></p> <p>or <code>show portchannel hash</code></p> <p>or <code>show portchannel information</code></p> |

Chapter 1. ISCLI Basics

Your EN4093 and EN4093R 10Gb Scalable Switch (EN4093 and EN4093R) is ready to perform basic switching functions right out of the box. Some of the more advanced features, however, require some administrative configuration before they can be used effectively.

This guide describes the individual ISCLI commands available for the EN4093 and EN4093R.

The ISCLI provides a direct method for collecting switch information and performing switch configuration. Using a basic terminal, the ISCLI allows you to view information and statistics about the switch, and to perform any necessary configuration.

This chapter explains how to access the IS Command Line Interface (ISCLI) for the switch.

Accessing the ISCLI

The first time you start the EN4093 and EN4093R, it boots into Networking OS CLI. To access the ISCLI, enter the following command and reset the EN4093 and EN4093R:

```
Main# boot/mode iscli
```

To access the Networking OS CLI, enter the following command from the ISCLI and reload the EN4093 and EN4093R:

```
Router(config)# boot cli-mode ibmnos-cli
```

The switch retains your CLI selection, even when you reset the configuration to factory defaults. The CLI boot mode is not part of the configuration settings.

If you downgrade the switch software to an earlier release, it will boot into Networking OS CLI. However, the switch retains the CLI boot mode, and will restore your CLI choice.

ISCLI Command Modes

The ISCLI has three major command modes listed in order of increasing privileges, as follows:

- **User EXEC mode**

This is the initial mode of access. By default, password checking is disabled for this mode, on console.

- **Privileged EXEC mode**

This mode is accessed from User EXEC mode. This mode can be accessed using the following command: `enable`

- **Global Configuration mode**

This mode allows you to make changes to the running configuration. If you save the configuration, the settings survive a reload of the EN4093 and EN4093R. Several sub-modes can be accessed from the Global Configuration mode. For more details, see [Table 1](#).

Each mode provides a specific set of commands. The command set of a higher-privilege mode is a superset of a lower-privilege mode—all lower-privilege mode commands are accessible when using a higher-privilege mode.

[Table 1](#) lists the ISCLI command modes.

Table 1. ISCLI Command Modes

| Command Mode/Prompt | Command used to enter or exit |
|---|---|
| User EXEC Router> | Default mode, entered automatically on console Exit: <code>exit</code> or <code>logout</code> |
| Privileged EXEC Router# | Enter Privileged EXEC mode, from User EXEC mode: <code>enable</code> Exit to User EXEC mode: <code>disable</code> Quit ISCLI: <code>exit</code> or <code>logout</code> |
| Global Configuration Router(config)# | Enter Global Configuration mode, from Privileged EXEC mode: <code>configure terminal</code> Exit to Privileged EXEC: <code>end</code> or <code>exit</code> |
| Interface IP Router(config-ip-if)# | Enter Interface IP Configuration mode, from Global Configuration mode: <code>interface ip <interface number></code> Exit to Global Configuration mode: <code>exit</code> Exit to Privileged EXEC mode: <code>end</code> |
| Interface Loopback Router(config-ip-loopback)# | Enter Interface Loopback Configuration mode, from Global Configuration mode: <code>interface ip loopback <1-5></code> Exit to Global Configuration mode: <code>exit</code> Exit to Privileged EXEC mode: <code>end</code> |

Table 1. ISCLI Command Modes (continued)

| Command Mode/Prompt | Command used to enter or exit |
|--|--|
| Interface Port Router(config-if)# | Enter Port Configuration mode, from Global Configuration mode: interface port <port number or alias> Exit to Privileged EXEC mode: exit Exit to Global Configuration mode: end |
| Interface PortChannel Router(config-PortChannel)# | Enter PortChannel (trunk group) Configuration mode, from Global Configuration mode: interface portchannel {<trunk number> lacp <key>} Exit to Privileged EXEC mode: exit Exit to Global Configuration mode: end |
| VLAN Router(config-vlan)# | Enter VLAN Configuration mode, from Global Configuration mode: vlan <VLAN number> Exit to Global Configuration mode: exit Exit to Privileged EXEC mode: end |
| Router OSPF Router(config-router-ospf)# | Enter OSPF Configuration mode, from Global Configuration mode: router ospf Exit to Global Configuration mode: exit Exit to Privileged EXEC mode: end |
| Router BGP Router(config-router-bgp)# | Enter BGP Configuration mode, from Global Configuration mode: router bgp Exit to Global Configuration mode: exit Exit to Privileged EXEC mode: end |
| Router RIP Router(config-router-rip)# | Enter RIP Configuration mode, from Global Configuration mode: router rip Exit to Global Configuration mode: exit Exit to Privileged EXEC mode: end |
| Route Map Router(config-route-map)# | Enter Route Map Configuration mode, from Global Configuration mode: route-map <1-32> Exit to Global Configuration mode: exit Exit to Privileged EXEC mode: end |

Table 1. ISCLI Command Modes (continued)

| Command Mode/Prompt | Command used to enter or exit |
|---|---|
| Router VRRP Router(config-vrrp)# | Enter VRRP Configuration mode, from Global Configuration mode: router vrrp Exit to Global Configuration mode: exit Exit to Privileged EXEC mode: end |
| IKEv2 Proposal Router(config-ikev2-prop)# | Enter IKEv2 Proposal Configuration mode, from Global Configuration mode: ikev2 proposal Exit to Global Configuration mode: exit Exit to Privileged EXEC mode: end |
| MLD Configuration Router(config-router-mld)# | Enter Multicast Listener Discovery Protocol Configuration mode, from Global Configuration mode: ipv6 mld Exit to Global Configuration mode: exit Exit to Privileged EXEC mode: end |
| OpenFlow Instance EN4093 and EN4093R(config-openflow-instance)# | Enter OpenFlow Instance Configuration mode, from Global Configuration mode: openflow instance Exit to Global Configuration mode: exit Exit to Privileged EXEC mode: end |
| VSI Database EN4093 and EN4093R(conf-vsldb)# | Enter Virtual Station Interface Database Configuration mode, from Global Configuration mode: virt evb vsldb <VSIDB_number> Exit to Global Configuration mode: exit Exit to Privileged EXEC mode: end |
| EVB Profile EN4093 and EN4093R(conf-evbprof)# | Enter Edge Virtual Bridging Profile Configuration mode, from Global Configuration mode: virt evb profile <1-16> Exit to Global Configuration mode: exit Exit to Privileged EXEC mode: end |

Table 1. ISCLI Command Modes (continued)

| Command Mode/Prompt | Command used to enter or exit |
|--|---|
| UFP Virtual Port Configuration EN4093 and EN4093R(config_ufp_vport)# | Enter Unified Fabric Port Virtual Port Configuration mode, from Global Configuration mode: ufp port <port no.> vport <1-4> Exit to Global Configuration mode: exit Exit to Privileged EXEC mode: end |
| SPAR Configuration EN4093 and EN4093R(config-spar)# | Enter Switch Partition Configuration mode, from Global Configuration mode: spar <1-8> Exit to Global Configuration mode: exit Exit to Privileged EXEC mode: end |

Global Commands

Some basic commands are recognized throughout the ISCLI command modes. These commands are useful for obtaining online help, navigating through the interface, and for saving configuration changes.

For help on a specific command, type the command, followed by `help`.

Table 2. Description of Global Commands

| Command | Action |
|------------------------------------|---|
| ? | Provides more information about a specific command or lists commands available at the current level. |
| list | Lists the commands available at the current level. |
| exit | Go up one level in the command mode structure. If already at the top level, exit from the command line interface and log out. |
| copy running-config startup-config | Write configuration changes to non-volatile flash memory. |
| logout | Exit from the command line interface and log out. |
| ping | <p>Use this command to verify station-to-station connectivity across the network. The format is as follows:</p> <pre>ping <host name> <IP address> [-n <tries (0-4294967295)>] [-w <msec delay (0-4294967295)>] [-l <length (0/32-65500/2080)>] [-s <IP source>] [-v <tos (0-255)>] [-f] [-t]</pre> <p>Where:</p> <ul style="list-style-type: none"> - -n: Sets the number of attempts (optional). - -w: Sets the number of milliseconds between attempts (optional). - -l: Sets the ping request payload size (optional). - -s: Sets the IP source address for the IP packet (optional). - -v: Sets the Type Of Service bits in the IP header. - -f: Sets the <i>don't fragment</i> bit in the IP header (only for IPv4 addresses). - -t: Pings continuously (same as -n 0). <p>Where the <i>IP address</i> or <i>hostname</i> specify the target device. Use of a hostname requires DNS parameters to be configured on the switch.</p> <p><i>Tries</i> (optional) is the number of attempts (1-32), and <i>msec delay</i> (optional) is the number of milliseconds between attempts.</p> |

Table 2. Description of Global Commands (continued)

| Command | Action |
|--------------|--|
| tracert | <p>Use this command to identify the route used for station-to-station connectivity across the network. The format is as follows:</p> <pre>tracert {<hostname> <IP address>} [<max-hops (1-32)> [<msec delay>]]</pre> <pre>tracert <hostname> <IP address> [<max-hops (1-32)> [<msec-delay (1-4294967295)>]]</pre> <p>Where <i>hostname/IP address</i> is the hostname or IP address of the target station, <i>max-hops</i> (optional) is the maximum distance to trace (1-32 devices), and <i>msec-delay</i> (optional) is the number of milliseconds to wait for the response.</p> <p>As with <code>ping</code>, the DNS parameters must be configured if specifying hostnames.</p> |
| telnet | <p>This command is used to form a Telnet session between the switch and another network device. The format is as follows:</p> <pre>telnet {<hostname> <IP address>} [<port>]</pre> <p>Where <i>IP address</i> or <i>hostname</i> specifies the target station. Use of a hostname requires DNS parameters to be configured on the switch.</p> <p><i>Port</i> is the logical Telnet port or service number.</p> |
| show history | This command displays the last ten issued commands. |
| show who | Displays a list of users who are currently logged in. |
| show line | Displays a list of users who are currently logged in, in table format. |

Command Line Interface Shortcuts

The following shortcuts allow you to enter commands quickly and easily.

CLI List and Range Inputs

For VLAN and port commands that allow an individual item to be selected from within a numeric range, lists and ranges of items can now be specified. For example, the `vlan` command permits the following options:

| | |
|----------------------------|------------------------------------|
| # vlan 1,3,4095 | (access VLANs 1, 3, and 4095) |
| # vlan 1-20 | (access VLANs 1 through 20) |
| # vlan 1-5,90-99,4090-4095 | (access multiple ranges) |
| # vlan 1-5,19,20,4090-4095 | (access a mix of lists and ranges) |

The numbers in a range must be separated by a dash: `<start of range> - <end of range>`

Multiple ranges or list items are permitted using a comma: `<range or item 1> , <range or item 2>`

Do not use spaces within list and range specifications.

Ranges can also be used to apply the same command option to multiple items. For example, to access multiple ports with one command:

| | |
|----------------------|----------------------------|
| # interface port 1-4 | (Access ports 1 through 4) |
|----------------------|----------------------------|

Command Abbreviation

Most commands can be abbreviated by entering the first characters which distinguish the command from the others in the same mode. For example, consider the following full command and a valid abbreviation:

| |
|--|
| Router(config)# spanning-tree stp 2 bridge hello 2 |
| or |
| Router(config)# sp stp 2 br h 2 |

Tab Completion

By entering the first letter of a command at any prompt and pressing `<Tab>`, the ISCLI displays all available commands or options that begin with that letter. Entering additional letters further refines the list of commands or options displayed. If only one command fits the input text when `<Tab>` is pressed, that command is supplied on the command line, waiting to be entered.

User Access Levels

To enable better switch management and user accountability, three levels or *classes* of user access have been implemented on the EN4093 and EN4093R. Levels of access to CLI, Web management functions, and screens increase as needed to perform various switch management tasks. Conceptually, access classes are defined as follows:

- **user**
Interaction with the switch is completely passive—nothing can be changed on the EN4093 and EN4093R. Users may display information that has no security or privacy implications, such as switch statistics and current operational state information.
- **oper**
Operators can make temporary changes on the EN4093 and EN4093R. These changes are lost when the switch is rebooted/reset. Operators have access to the switch management features used for daily switch operations. Because any changes an operator makes are undone by a reset of the switch, operators cannot severely impact switch operation.
- **admin**
Administrators are the only ones that may make permanent changes to the switch configuration—changes that are persistent across a reboot or reset of the switch. Administrators can access switch functions to configure and troubleshoot problems on the EN4093 and EN4093R. Because administrators can also make temporary (operator-level) changes as well, they must be aware of the interactions between temporary and permanent changes.

Access to switch functions is controlled through the use of unique surnames and passwords. Once you are connected to the switch via local Telnet, remote Telnet, or SSH, you are prompted to enter a password. The default user names/password for each access level are listed in the following table.

Note: It is recommended that you change default switch passwords after initial configuration and as regularly as required under your network security policies.

Table 3. User Access Levels

| User Account | Description and Tasks Performed | Password |
|---------------|--|----------|
| User | The User has no direct responsibility for switch management. He or she can view all switch status information and statistics, but cannot make any configuration changes to the switch. | user |
| Operator | The Operator can make temporary changes that are lost when the switch is rebooted/reset. Operators have access to the switch management features used for daily switch operations. | |
| Administrator | The superuser Administrator has complete access to all command modes, information, and configuration commands on the EN4093 and EN4093R 10Gb Scalable Switch, including the ability to change both the user and administrator passwords. | admin |

Note: With the exception of the “admin” user, access to each user level can be disabled by setting the password to an empty value.

Idle Timeout

By default, the switch will disconnect your Telnet session after ten minutes of inactivity. This function is controlled by the following command, which can be set from 1 to 60 minutes, or disabled when set to 0:

```
system idle <0-60>
```

Command mode: Global Configuration

Chapter 2. Information Commands

You can view configuration information for the switch in both the user and administrator command modes. This chapter discusses how to use the command line interface to display switch information.

Table 4. Information Commands

| Command Syntax and Usage |
|--|
| <pre>show interface status <port alias or number></pre> <p>Displays configuration information about the selected port(s), including:</p> <ul style="list-style-type: none">– Port alias and number– Port speed– Duplex mode (half, full, or auto)– Flow control for transmit and receive (no, yes, or both)– Link status (up, down, or disabled) <p>For details, see page 112.</p> <p>Command mode: All</p> |
| <pre>show interface trunk <port alias or number></pre> <p>Displays port status information, including:</p> <ul style="list-style-type: none">– Port alias and number– Whether the port uses VLAN Tagging or not– Port VLAN ID (PVID)– Port name– VLAN membership– FDB Learning status– Flooding status <p>For details, see page 114.</p> <p>Command mode: All</p> |
| <pre>show interface transceiver</pre> <p>Displays the status of the port transceiver module on each external port. For details, see page 116.</p> <p>Command mode: All</p> |
| <pre>show software-key</pre> <p>Displays the enabled software features.</p> <p>Command mode: All</p> |
| <pre>show information-dump</pre> <p>Dumps all switch information available (10K or more, depending on your configuration).</p> <p>If you want to capture dump data to a file, set your communication software on your workstation to capture session data prior to issuing the dump commands.</p> <p>Command mode: All</p> |

System Information

The information provided by each command option is briefly described in [Table 5 on page 14](#), with pointers to where detailed information can be found.

Table 5. System Information Commands

| Command Syntax and Usage |
|--|
| <pre>show sys-info</pre> <p>Displays system information, including:</p> <ul style="list-style-type: none">– System date and time– Switch model name and number– Switch name and location– Time of last boot– MAC address of the switch management processor– IP address of management interface– Hardware version and part number– Software image file and version number– Configuration name– Log-in banner, if one is configured– Internal temperatures <p>For details, see page 25.</p> <p>Command mode: All</p> |
| <pre>show logging [severity <0-7>] [reverse]</pre> <p>Displays the current syslog configuration, followed by the most recent 2000 syslog messages, as displayed by the <code>show logging messages</code> command. For details, see page 27.</p> <p>Command mode: All</p> |
| <pre>show access user</pre> <p>Displays configured user names and their status.</p> <p>Command mode: Privileged EXEC</p> |

CLI Display Information

These commands allow you to display information about the number of lines per screen displayed in the CLI.

Table 6. CLI Display Information Options

| Command Syntax and Usage |
|---|
| <pre>show terminal-length</pre> <p>Displays the number of lines per screen displayed in the CLI for the current session. A value of 0 means paging is disabled.</p> <p>Command mode: All</p> |
| <pre>show line console length</pre> <p>Displays the current line console length setting. For details, see page 246.</p> <p>Command mode: All</p> |
| <pre>show line vty length</pre> <p>Displays the current line vty length setting. For details, see page 246.</p> <p>Command mode: All</p> |

Error Disable and Recovery Information

These commands allow you to display information about the Error Disable and Recovery feature for interface ports.

Table 7. Error Disable Information Commands

| Command Syntax and Usage |
|--|
| <pre>show errdisable recovery</pre> <p>Displays a list ports with their Error Recovery status.</p> <p>Command mode: All</p> |
| <pre>show errdisable timers</pre> <p>Displays a list of active recovery timers, if applicable.</p> <p>Command mode: All</p> |
| <pre>show errdisable information</pre> <p>Displays all Error Disable and Recovery information.</p> <p>Command mode: All</p> |

SNMPv3 System Information

SNMP version 3 (SNMPv3) is an extensible SNMP Framework that supplements the SNMPv2 framework by supporting the following:

- a new SNMP message format
- security for messages
- access control
- remote configuration of SNMP parameters

For more details on the SNMPv3 architecture please refer to RFC2271 to RFC2276.

Table 8. SNMPv3 Commands

| Command Syntax and Usage |
|---|
| <pre>show snmp-server v3 user</pre> <p>Displays User Security Model (USM) table information. To view the table, see page 18.</p> <p>Command mode: All</p> |
| <pre>show snmp-server v3 view</pre> <p>Displays information about view, subtrees, mask and type of view. To view a sample, see page 19.</p> <p>Command mode: All</p> |
| <pre>show snmp-server v3 access</pre> <p>Displays View-based Access Control information. To view a sample, see page 20.</p> <p>Command mode: All</p> |
| <pre>show snmp-server v3 group</pre> <p>Displays information about the group, including the security model, user name, and group name. To view a sample, see page 20.</p> <p>Command mode: All</p> |
| <pre>show snmp-server v3 community</pre> <p>Displays information about the community table information. To view a sample, see page 21.</p> <p>Command mode: All</p> |
| <pre>show snmp-server v3 target-address</pre> <p>Displays the Target Address table information. To view a sample, see page 21.</p> <p>Command mode: All</p> |
| <pre>show snmp-server v3 target-parameters</pre> <p>Displays the Target parameters table information. To view a sample, see page 23.</p> <p>Command mode: All</p> |

Table 8. SNMPv3 Commands (continued)

| Command Syntax and Usage |
|--|
| <pre>show snmp-server v3 notify</pre> <p>Displays the Notify table information. To view a sample, see page 23.</p> <p>Command mode: All</p> |
| <pre>show snmp-server v3</pre> <p>Displays all the SNMPv3 information. To view a sample, see page 24.</p> <p>Command mode: All</p> |

SNMPv3 USM User Table Information

The User-based Security Model (USM) in SNMPv3 provides security services such as authentication and privacy of messages. This security model makes use of a defined set of user identities displayed in the USM user table. The following command displays SNMPv3 user information:

```
show snmp-server v3 user
```

Command mode: All

The USM user table contains the following information:

- the user name
- a security name in the form of a string whose format is independent of the Security Model
- an authentication protocol, which is an indication that the messages sent on behalf of the user can be authenticated
- the privacy protocol

| usmUser Table: | |
|----------------|-----------------------|
| User Name | Protocol |
| ----- | ----- |
| adminmd5 | HMAC_MD5, DES PRIVACY |
| adminsha | HMAC_SHA, DES PRIVACY |
| v1v2only | NO AUTH, NO PRIVACY |

Table 9. USM User Table Information Parameters

| Field | Description |
|-----------|---|
| User Name | This is a string that represents the name of the user that you can use to access the switch. |
| Protocol | This indicates whether messages sent on behalf of this user are protected from disclosure using a privacy protocol. Networking OS supports DES algorithm for privacy. The software also supports two authentication algorithms: MD5 and HMAC-SHA. |

SNMPv3 View Table Information

The user can control and restrict the access allowed to a group to only a subset of the management information in the management domain that the group can access within each context by specifying the group's rights in terms of a particular MIB view for security reasons.

The following command displays the SNMPv3 View Table:

```
show snmp-server v3 view
```

Command mode: All

| View Name | Subtree | Mask | Type |
|-----------|----------------|------|----------|
| iso | 1 | | included |
| v1v2only | 1 | | included |
| v1v2only | 1.3.6.1.6.3.15 | | excluded |
| v1v2only | 1.3.6.1.6.3.16 | | excluded |
| v1v2only | 1.3.6.1.6.3.18 | | excluded |

Table 10. SNMPv3 View Table Information Parameters

| Field | Description |
|-----------|---|
| View Name | Displays the name of the view. |
| Subtree | Displays the MIB subtree as an OID string. A view subtree is the set of all MIB object instances which have a common Object Identifier prefix to their names. |
| Mask | Displays the bit mask. |
| Type | Displays whether a family of view subtrees is included or excluded from the MIB view. |

SNMPv3 Access Table Information

The access control subsystem provides authorization services.

The `vacmAccessTable` maps a group name, security information, a context, and a message type, which could be the read or write type of operation or notification into a MIB view.

The View-based Access Control Model defines a set of services that an application can use for checking access rights of a group. This group's access rights are determined by a read-view, a write-view and a notify-view. The read-view represents the set of object instances authorized for the group while reading the objects. The write-view represents the set of object instances authorized for the group when writing objects. The notify-view represents the set of object instances authorized for the group when sending a notification.

The following command displays SNMPv3 access information:

```
show snmp-server v3 access
```

Command mode: All

| Group Name | Model | Level | ReadV | WriteV | NotifyV |
|------------|--------|--------------|-------|--------|----------|
| v1v2grp | snmpv1 | noAuthNoPriv | iso | iso | v1v2only |
| admingrp | usm | authPriv | iso | iso | iso |

Table 11. SNMPv3 Access Table Information

| Field | Description |
|------------|---|
| Group Name | Displays the name of group. |
| Model | Displays the security model used, for example, SNMPv1, or SNMPv2 or USM. |
| Level | Displays the minimum level of security required to gain rights of access. For example, <code>noAuthNoPriv</code> , <code>authNoPriv</code> , or <code>authPriv</code> . |
| ReadV | Displays the MIB view to which this entry authorizes the read access. |
| WriteV | Displays the MIB view to which this entry authorizes the write access. |
| NotifyV | Displays the Notify view to which this entry authorizes the notify access. |

SNMPv3 Group Table Information

A group is a combination of security model and security name that defines the access rights assigned to all the security names belonging to that group. The group is identified by a group name.

The following command displays SNMPv3 group information:

```
show snmp-server v3 group
```

Command mode: All

| Sec Model | User Name | Group Name |
|-----------|-----------|------------|
| snmpv1 | v1v2only | v1v2grp |
| usm | adminmd5 | admingrp |
| usm | adminsha | admingrp |

Table 12. SNMPv3 Group Table Information Parameters

| Field | Description |
|------------|---|
| Sec Model | Displays the security model used, which is any one of: USM, SNMPv1, SNMPv2, and SNMPv3. |
| User Name | Displays the name for the group. |
| Group Name | Displays the access name of the group. |

SNMPv3 Community Table Information

This command displays the community table information stored in the SNMP engine. The following command displays SNMPv3 community information:

```
show snmp-server v3 community
```

Command mode: All

| Index | Name | User Name | Tag |
|-------|--------|-----------|----------|
| trap1 | public | v1v2only | v1v2trap |

Table 13. SNMPv3 Community Table Information Parameters

| Field | Description |
|-----------|---|
| Index | Displays the unique index value of a row in this table |
| Name | Displays the community string, which represents the configuration. |
| User Name | Displays the User Security Model (USM) user name. |
| Tag | Displays the community tag. This tag specifies a set of transport endpoints from which a command responder application accepts management requests and to which a command responder application sends an SNMP trap. |

SNMPv3 Target Address Table Information

The following command displays SNMPv3 target address information:

```
show snmp-server v3 target-address
```

Command mode: All

This command displays the SNMPv3 target address table information, which is stored in the SNMP engine.

| Name | Transport Addr | Port | Taglist | Params |
|-------|----------------|-------|----------|-----------|
| ----- | ----- | ----- | ----- | ----- |
| trap1 | 47.81.25.66 | 162 | v1v2trap | v1v2param |

Table 14. SNMPv3 Target Address Table Information Parameters

| Field | Description |
|----------------|--|
| Name | Displays the locally arbitrary, but unique identifier associated with this <code>snmpTargetAddrEntry</code> . |
| Transport Addr | Displays the transport addresses. |
| Port | Displays the SNMP UDP port number. |
| Taglist | This column contains a list of tag values which are used to select target addresses for a particular SNMP message. |
| Params | The value of this object identifies an entry in the <code>snmpTargetParamsTable</code> . The identified entry contains SNMP parameters to be used when generating messages to be sent to this transport address. |

SNMPv3 Target Parameters Table Information

The following command displays SNMPv3 target parameters information:

```
show snmp-server v3 target-parameters
```

Command mode: All

| Name | MP Model | User Name | Sec Model | Sec Level |
|-----------|----------|-----------|-----------|--------------|
| v1v2param | snmpv2c | v1v2only | snmpv1 | noAuthNoPriv |

Table 15. SNMPv3 Target Parameters Table Information

| Field | Description |
|-----------|--|
| Name | Displays the locally arbitrary, but unique identifier associated with this <code>snmpTargetParamsEntry</code> . |
| MP Model | Displays the Message Processing Model used when generating SNMP messages using this entry. |
| User Name | Displays the <code>securityName</code> , which identifies the entry on whose behalf SNMP messages will be generated using this entry. |
| Sec Model | Displays the security model used when generating SNMP messages using this entry. The system may choose to return an <code>inconsistentValue</code> error if an attempt is made to set this variable to a value for a security model which the system does not support. |
| Sec Level | Displays the level of security used when generating SNMP messages using this entry. |

SNMPv3 Notify Table Information

The following command displays the SNMPv3 Notify table:

```
show snmp-server v3 notify
```

Command mode: All

| Name | Tag |
|----------|----------|
| v1v2trap | v1v2trap |

Table 16. SNMPv3 Notify Table Information

| Field | Description |
|-------|---|
| Name | The locally arbitrary, but unique identifier associated with this <code>snmpNotifyEntry</code> . |
| Tag | This represents a single tag value which is used to select entries in the <code>snmpTargetAddrTable</code> . Any entry in the <code>snmpTargetAddrTable</code> that contains a tag value equal to the value of this entry, is selected. If this entry contains a value of zero length, no entries are selected. |

SNMPv3 Dump Information

The following command displays SNMPv3 information:

```
show snmp-server v3
```

Command mode: All

```

usmUser Table:
User Name                Protocol
-----
adminmd5                 HMAC_MD5, DES PRIVACY
adminsha                 HMAC_SHA, DES PRIVACY
v1v2only                 NO AUTH, NO PRIVACY

vacmAccess Table:
Group Name Prefix Model  Level      Match  ReadV  WriteV  NotifyV
-----
v1v2grp          snmpv1  noAuthNoPriv  exact  iso    iso    v1v2only
admingrp         usm     authPriv      exact  iso    iso    iso

vacmViewTreeFamily Table:
View Name      Subtree      Mask          Type
-----
iso            1            included
v1v2only      1            included
v1v2only      1.3.6.1.6.3.15  excluded
v1v2only      1.3.6.1.6.3.16  excluded
v1v2only      1.3.6.1.6.3.18  excluded

vacmSecurityToGroup Table:
Sec Model  User Name                Group Name
-----
snmpv1     v1v2only                 v1v2grp
usm        adminmd5                 admingrp
usm        adminsha                 admingrp

snmpCommunity Table:
Index      Name      User Name      Tag
-----

snmpNotify Table:
Name                Tag
-----

snmpTargetAddr Table:
Name      Transport Addr  Port  Taglist  Params
-----

snmpTargetParams Table:
Name                MP Model  User Name                Sec Model  Sec Level
-----

```

General System Information

The following command displays system information:

```
show sys-info
```

Command mode: All

```
System Information at 16:50:45 Wed Nov 16, 2011
Time zone: America/US/Pacific
Daylight Savings Time Status: Disabled

IBM Flex System Fabric EN4093 and EN4093R 10Gb Scalable Switch for IBM BladeCenter
IBM Flex System Fabric EN4093 and EN4093R 10Gb Scalable Switch (BW build)

Switch has been up 5 days, 2 hours, 16 minutes and 42 seconds.
Last boot: 0:00:47 Wed Jan 3, 2010 (reset from console)

MAC address: 00:00:00:00:00:00   IP (If 1) address: 0.0.0.0
Internal Management Port MAC Address: 00:00:00:00:00:ef
Internal Management Port IP Address (if 128): 9.43.95.121
External Management Port MAC Address: 00:00:00:00:00:fe
External Management Port IP Address (if 127):
Software Version 7.7.1 (FLASH image2), active configuration.

PCBA Part Number:      BAC-00042-00
Hardware Part Number:  46C7193
FAB Number:           BN-RZZ000
Serial Number:        PROTO2C04E
Manufacturing Date:   43/08
Hardware Revision:    0
Board Revision:       1
PLD Firmware Version: 4.0

Temperature Sensor 1 (Warning): 42.0 C (Warn at 88.0 C/Recover at 78.0 C)
Temperature Sensor 2 (Shutdown): 42.5 C (Shutdown at 98.0 C/Recover at 88.0 C)
Temperature Sensor 3 (Exhaust): 37.5 C
Temperature Sensor 4 (Inlet): 32.5 C
```

Note: The display of temperature will come up only if the temperature of any of the sensors exceeds the temperature threshold. There will be a warning from the software if any of the sensors exceeds this temperature threshold. The switch will shut down if the power supply overheats.

System information includes:

- System date and time
- Switch model
- Switch name and location
- Time of last boot
- MAC address of the switch management processor
- Software image file and version number, and configuration name.
- IP address of the management interface
- Hardware version and part number
- Log-in banner, if one is configured
- Internal temperatures

Show Software Version Brief Information

The following command displays brief software version information:

```
show version brief
```

Command mode: All

```
Software Version 7.7.1.0 (FLASH image2), active configuration.
```

Displays the software version number, image file, and configuration name.

Show Specific System Information

[Table 17](#) lists commands used for displaying specific entries from the general system information screen

Table 17. Specific System Information Options

| Command Syntax and Usage |
|--|
| <pre>show environment fan</pre> <p>Displays information about internal temperatures and fan status.</p> <p>Command mode: All</p> |
| <pre>show environment power</pre> <p>Displays information about power supply status.</p> <p>Command mode: All</p> |
| <pre>show version brief</pre> <p>Displays the software version number, image file, and configuration name.</p> <p>Command mode: All</p> |

Show Recent Syslog Messages

The following command displays system log messages:

```
show logging messages [severity <0-7>] [reverse]
```

Command mode: All

| Date | Time | Criticality level | Message |
|-------|----------|-------------------|------------------------------|
| Jul 8 | 17:25:41 | NOTICE | system: link up on port INT1 |
| Jul 8 | 17:25:41 | NOTICE | system: link up on port INT8 |
| Jul 8 | 17:25:41 | NOTICE | system: link up on port INT7 |
| Jul 8 | 17:25:41 | NOTICE | system: link up on port INT2 |
| Jul 8 | 17:25:41 | NOTICE | system: link up on port INT1 |
| Jul 8 | 17:25:41 | NOTICE | system: link up on port INT4 |
| Jul 8 | 17:25:41 | NOTICE | system: link up on port INT3 |
| Jul 8 | 17:25:41 | NOTICE | system: link up on port INT6 |
| Jul 8 | 17:25:41 | NOTICE | system: link up on port INT5 |
| Jul 8 | 17:25:41 | NOTICE | system: link up on port EXT4 |
| Jul 8 | 17:25:41 | NOTICE | system: link up on port EXT1 |
| Jul 8 | 17:25:41 | NOTICE | system: link up on port EXT3 |
| Jul 8 | 17:25:41 | NOTICE | system: link up on port EXT2 |
| Jul 8 | 17:25:41 | NOTICE | system: link up on port INT3 |
| Jul 8 | 17:25:42 | NOTICE | system: link up on port INT2 |
| Jul 8 | 17:25:42 | NOTICE | system: link up on port INT4 |
| Jul 8 | 17:25:42 | NOTICE | system: link up on port INT3 |
| Jul 8 | 17:25:42 | NOTICE | system: link up on port INT6 |

Each syslog message has a severity level associated with it, included in text form as a prefix to the log message. One of eight different prefixes is used, depending on the condition for which the administrator is being notified.

- EMERG Indicates the system is unusable
- ALERT Indicates action should be taken immediately
- CRIT Indicates critical conditions
- ERR Indicates error conditions or errored operations
- WARNING Indicates warning conditions
- NOTICE Indicates a normal but significant condition
- INFO Indicates an information message
- DEBUG Indicates a debug-level message

The `severity` option filters only syslog messages with a specific severity level between 0 and 7, from EMERG to DEBUG correspondingly.

The `reverse` option displays the output in reverse order, from the newest entry to the oldest.

User Status

The following command displays user status information:

```
show access user
```

Command mode: All except User EXEC

```
Usernames:
  user      - enabled - offline
  oper      - disabled - offline
  admin     - Always Enabled - online 1 session
Current User ID table:
  1: name paul      , dis, cos user      , password valid, offline
Current strong password settings:
  strong password status: disabled
```

This command displays the status of the configured usernames.

Stacking Information

Table 18 lists the Stacking information options.

Table 18. Stacking Information Commands

| Command Syntax and Usage |
|--|
| <pre>show stack switch</pre> <p>Displays information about each switch in the stack, including:</p> <ul style="list-style-type: none">– Configured Switch Number (csnum)– Attached Switch Number (asnum) when run on master switch– MAC address– Stacking state <p>Command mode: All</p> |
| <pre>show stack attached-switches</pre> <p>Displays information about each attached switch in the stack. Available only on the master switch.</p> <p>Command mode: All</p> |
| <pre>show stack link</pre> <p>Displays link information for each switch in the stack, listed by assigned switch number.</p> <p>Command mode: All</p> |
| <pre>show stack name</pre> <p>Displays the name of the stack.</p> <p>Command mode: All</p> |
| <pre>show stack backup</pre> <p>Displays the unit number of the backup switch.</p> <p>Command mode: All</p> |
| <pre>show stack version</pre> <p>Displays the firmware version number for the selected switch.</p> <p>Command mode: All</p> |
| <pre>show stack path-map [csnum <1-8>]</pre> <p>Displays the Stacking packet path map that shows how a specific switch or all switches in the stack are connected.</p> <p>Command mode: All</p> |

Table 18. Stacking Information Commands

| Command Syntax and Usage |
|--|
| <pre>show stack push-status</pre> <p>Displays the status of the most recent firmware and configuration file push from the master to member switches.</p> <p>Command mode: All</p> |
| <pre>show stack dynamic</pre> <p>Displays all stacking information.</p> <p>Command mode: All</p> |

Stacking Switch Information

The following command displays Stacking switch information:

```
show stack switch
```

Command mode: All

```
Stack name: MyStack
Local switch is the master.

Local switch:
  csnum          - 1
  MAC            - 00:25:03:1c:96:00
  Switch Type    - 9
  Switch Mode (cfg) - Master
  Priority        - 225
  Stack MAC      - 00:25:03:1c:96:1f

Master switch:
  csnum          - 1
  MAC            - 00:25:03:1c:96:00

Backup switch:
  csnum          - 2
  MAC            - 00:ef:61:79:00:00

Configured Switches:
-----
csnum          MAC          asnum
-----
C1             00:25:03:1c:96:00  A1
C2             00:ef:61:79:00:00  A2

Attached Switches in Stack:
-----
asnum          MAC          csnum  State
-----
A1             00:25:03:1c:96:00  C1     IN_STACK
A2             00:ef:61:79:00:00  C2     IN_STACK
```



```

Stack name: STK
Local switch is the master.

Local switch:
  csnum          - 1
  MAC            - 74:99:75:21:8d:00
  UUID          - 534c8ca1605846299148305adc9a1f6d
  Bay Number    - 1
  Switch Type   - 14
  Chassis Type  - 6 (Flex Enterprise)
  Switch Mode (cfg) - Master
  Priority       - 250
  Stack MAC     - 74:99:75:21:8d:1f

Master switch:
  csnum          - 1
  MAC            - 74:99:75:21:8d:00
  UUID          - 534c8ca1605846299148305adc9a1f6d
  Bay Number    - 1

Backup switch:
  csnum          - 5
  MAC            - 74:99:75:21:8c:00
  UUID          - 98c587636548429aba5010f8c62d4e27
  Bay Number    - 1

Configured Switches:
-----
csnum          UUID          Bay          MAC          asnum
-----
C1  534c8ca1605846299148305adc9a1f6d  1  74:99:75:21:8d:00  A1
C2  534c8ca1605846299148305adc9a1f6d  2  08:17:f4:84:34:00  A3
C3  534c8ca1605846299148305adc9a1f6d  3  08:17:f4:0a:2d:00  A2
C4  534c8ca1605846299148305adc9a1f6d  4  74:99:75:1c:77:00  A4
C5  98c587636548429aba5010f8c62d4e27  1  74:99:75:21:8c:00  A5

Attached Switches in Stack:
-----
asnum          UUID          Bay          MAC          csnum  State
-----
A1  534c8ca1605846299148305adc9a1f6d  1  74:99:75:21:8d:00  C1  IN_STACK
A2  534c8ca1605846299148305adc9a1f6d  3  08:17:f4:0a:2d:00  C3  IN_STACK
A3  534c8ca1605846299148305adc9a1f6d  2  08:17:f4:84:34:00  C2  IN_STACK
A4  534c8ca1605846299148305adc9a1f6d  4  74:99:75:1c:77:00  C4  IN_STACK
A5  98c587636548429aba5010f8c62d4e27  1  74:99:75:21:8c:00  C5  IN_STACK

```

Stack switch information includes the following:

- Stack name
- Details about the local switch from which the command was issued
- Configured switch number and MAC of the Stack Master and Stack Backup
- Configured switch numbers and their associated assigned switch numbers
- Attached switch numbers and their associated configured switch numbers

Attached Switches Information

The following command displays information about attached switches, when run on master switch:

```
show stack attached-switches
```

Command mode: All

```
Attached Switches in Stack:
-----
asnum          UUID                               Bay    MAC                               csnum  State
-----
A1  534c8ca1605846299148305adc9a1f6d  1  74:99:75:21:8d:00  C1  IN_STACK
A2  534c8ca1605846299148305adc9a1f6d  3  08:17:f4:0a:2d:00  C3  IN_STACK
A3  534c8ca1605846299148305adc9a1f6d  2  08:17:f4:84:34:00  C2  IN_STACK
A4  534c8ca1605846299148305adc9a1f6d  4  74:99:75:1c:77:00  C4  IN_STACK
A5  98c587636548429aba5010f8c62d4e27  1  74:99:75:21:8c:00  C5  IN_STACK
```

Stack Name Information

The following command displays the name of the stack:

```
show stack name
```

Command mode: All

```
Stack name: STK
```

Stack Backup Switch Information

The following command displays the unit number for the backup switch:

```
show stack backup
```

Command mode: All

```
Current config Backup unit number = 5
```

Stack Version Information

The following command displays firmware version information for each switch in the stack:

```
show stack version
```

Command mode: All

```
Switch Firmware Versions:
-----
asnum  csnum  MAC                               S/W    Version                          Serial #
-----
A1     C1     74:99:75:21:8d:00  image1  7.7.1.10                        Y250CM28Y653
A2     C3     08:17:f4:0a:2d:00  image1  7.7.1.10                        US7049000Y
A3     C2     08:17:f4:84:34:00  image1  7.7.1.10                        Y010CM161680
A4     C4     74:99:75:1c:77:00  image1  7.7.1.10                        Y010CM28E857
A5     C5     74:99:75:21:8c:00  image1  7.7.1.10                        Y250CM28Y639
```

Stack Packet Path Information

The following command displays packet path information which maps switch connections in the stack:

```
show stack path-map
```

Command mode: All

| Packet path Information: | | | | | | | | | | | | | | | | |
|--------------------------|-----|------|-----|------|-----|------|-----|------|-----|------|-----|---|-----|---|-----|---|
| To-> | Swu | 1 | Swu | 2 | Swu | 3 | Swu | 4 | Swu | 5 | Swu | 6 | Swu | 7 | Swu | 8 |
| Swu 1 | | 0 | | 1:45 | | 1:45 | | 1:49 | | 1:49 | | 0 | | 0 | | 0 |
| Swu 2 | | 2:61 | | 0 | | 2:61 | | 2:57 | | 2:57 | | 0 | | 0 | | 0 |
| Swu 3 | | 3:57 | | 3:61 | | 0 | | 3:57 | | 3:61 | | 0 | | 0 | | 0 |
| Swu 4 | | 4:57 | | 4:61 | | 4:57 | | 0 | | 4:61 | | 0 | | 0 | | 0 |
| Swu 5 | | 5:45 | | 5:49 | | 5:49 | | 5:45 | | 0 | | 0 | | 0 | | 0 |
| Swu 6 | | 0 | | 0 | | 0 | | 0 | | 0 | | 0 | | 0 | | 0 |
| Swu 7 | | 0 | | 0 | | 0 | | 0 | | 0 | | 0 | | 0 | | 0 |
| Swu 8 | | 0 | | 0 | | 0 | | 0 | | 0 | | 0 | | 0 | | 0 |

Stack Push Status Information

The following command displays the status of the most recent firmware and configuration file push from the master to member switches:

```
show stack push-status
```

Command mode: All

```
Image 1 transfer status info:
Switch 08:17:f4:0a:2d:00:
    not received - file not sent or transfer in progress
Switch 08:17:f4:84:34:00:
    not received - file not sent or transfer in progress
Switch 74:99:75:1c:77:00:
    not received - file not sent or transfer in progress
Switch 74:99:75:21:8c:00:
    not received - file not sent or transfer in progress

Image 2 transfer status info:
Switch 08:17:f4:0a:2d:00:
    not received - file not sent or transfer in progress
Switch 08:17:f4:84:34:00:
    not received - file not sent or transfer in progress
Switch 74:99:75:1c:77:00:
    not received - file not sent or transfer in progress
Switch 74:99:75:21:8c:00:
    not received - file not sent or transfer in progress

Boot image transfer status info:
Switch 08:17:f4:0a:2d:00:
    not received - file not sent or transfer in progress
Switch 08:17:f4:84:34:00:
    not received - file not sent or transfer in progress
Switch 74:99:75:1c:77:00:
    not received - file not sent or transfer in progress
Switch 74:99:75:21:8c:00:
    not received - file not sent or transfer in progress

Config file transfer status info:
Switch 08:17:f4:0a:2d:00:
    last receive successful
Switch 08:17:f4:84:34:00:
    last receive successful
Switch 74:99:75:1c:77:00:
    last receive successful
Switch 74:99:75:21:8c:00:
    last receive successful
```

Layer 2 Information

The following commands display Layer 2 information.

Table 19. Layer 2 Information Commands

| Command Syntax and Usage |
|--|
| <pre>show dot1x information</pre> <p>Displays 802.1X Information.</p> <p>Command mode: All</p> <p>For details, see page 48.</p> |
| <pre>show spanning-tree</pre> <p>Displays Spanning Tree information, including the status (on or off), Spanning Tree mode (RSTP, PVRST, or MSTP), and VLAN membership.</p> <p>In addition to seeing if spanning tree groups (STGs) are enabled or disabled, you can view the following STG bridge information:</p> <ul style="list-style-type: none">– Priority– Hello interval– Maximum age value– Forwarding delay– Aging time <p>You can also see the following port-specific STG information:</p> <ul style="list-style-type: none">– Port alias and priority– Cost– State <p>Command mode: All</p> |
| <pre>show spanning-tree stp <1-128> information</pre> <p>Displays information about a specific Spanning Tree Group.</p> <p>Command mode: All</p> <p>For details, see page 50.</p> |

Table 19. Layer 2 Information Commands (continued)

| Command Syntax and Usage |
|--|
| <pre>show spanning-tree mstp cist information</pre> <p>Displays Common Internal Spanning Tree (CIST) information, including the MSTP digest and VLAN membership.</p> <p>CIST bridge information includes:</p> <ul style="list-style-type: none"> – Priority – Hello interval – Maximum age value – Forwarding delay – Root bridge information (priority, MAC address, path cost, root port) <p>CIST port information includes:</p> <ul style="list-style-type: none"> – Port number and priority – Cost – State <p>For details, see page 54.</p> <p>Command mode: All</p> |
| <pre>show spanning-tree mstp {mrst cist}</pre> <p>Displays the current Common Internal Spanning Tree or Multiple and Rapid Spanning Tree settings.</p> |
| <pre>show portchannel information</pre> <p>Displays the state of each port in the various static or LACP trunk groups. For details, see page 56.</p> <p>Command mode: All</p> |
| <pre>show vlan</pre> <p>Displays VLAN configuration information for all configured VLANs, including:</p> <ul style="list-style-type: none"> – VLAN Number – VLAN Name – Status – Port membership of the VLAN <p>For details, see page 57.</p> <p>Command mode: All</p> |
| <pre>show failover trigger <trigger number></pre> <p>Displays Layer 2 Failover information. For details, see page 41.</p> <p>Command mode: All</p> |

Table 19. Layer 2 Information Commands (continued)

| Command Syntax and Usage |
|---|
| <pre>show hotlinks information</pre> <p>Displays Hot Links information. For details, see page 42.</p> <p>Command mode: All</p> |
| <pre>show layer2 information</pre> <p>Dumps all Layer 2 switch information available (10K or more, depending on your configuration).</p> <p>If you want to capture dump data to a file, set your communication software on your workstation to capture session data prior to issuing the dump commands.</p> <p>Command mode: All</p> |

FDB Information

The forwarding database (FDB) contains information that maps the media access control (MAC) address of each known device to the switch port where the device address was learned. The FDB also shows which other ports have seen frames destined for a particular MAC address.

Note: The master forwarding database supports up to K MAC address entries on the MP per switch.

Table 20. FDB Information Commands

| Command Syntax and Usage |
|--|
| <pre>show mac-address-table address <MAC address></pre> <p>Displays a single database entry by its MAC address. You are prompted to enter the MAC address of the device. Enter the MAC address using the format, xx:xx:xx:xx:xx:xx. For example, 08:00:20:12:34:56</p> <p>You can also enter the MAC address using the format, xxxxxxxxxxxx. For example, 080020123456</p> <p>Command mode: All</p> |
| <pre>show mac-address-table interface port <port alias or number></pre> <p>Displays all FDB entries for a particular port.</p> <p>Command mode: All</p> |
| <pre>show mac-address-table vlan <VLAN number></pre> <p>Displays all FDB entries on a single VLAN.</p> <p>Command mode: All</p> |
| <pre>show mac-address-table state {unknown forward trunk}</pre> <p>Displays all FDB entries for a particular state.</p> <p>Command mode: All</p> |
| <pre>show mac-address-table multicast</pre> <p>Displays all Multicast MAC entries in the FDB.</p> <p>Command mode: All</p> |

Table 20. FDB Information Commands (continued)

| Command Syntax and Usage |
|---|
| <pre>show mac-address-table static</pre> <p>Displays all static MAC entries in the FDB.</p> <p>Command mode: All</p> |
| <pre>show mac-address-table configured static</pre> <p>Displays all configured static MAC entries in the FDB.</p> <p>Command mode: All</p> |
| <pre>show mac-address-table</pre> <p>Displays all entries in the Forwarding Database.</p> <p>Command mode: All</p> <p>For more information, see page 38.</p> |
| <pre>show mac-address-table all</pre> <p>Displays both unicast (static and dynamix) and multicast (static) entries in the Forwarding Database.</p> <p>Command mode: All</p> |

Show All FDB Information

The following command displays Forwarding Database information:

```
show mac-address-table
```

Command mode: All

| MAC address | VLAN | Port | Trnk | State | Permanent |
|-------------------|------|-------|------|-------|-----------|
| 00:04:38:90:54:18 | 1 | EXT4 | | FWD | |
| 00:09:6b:9b:01:5f | 1 | INT13 | | FWD | |
| 00:09:6b:ca:26:ef | 4095 | MGT1 | | FWD | |
| 00:0f:06:ec:3b:00 | 4095 | MGT1 | | FWD | |
| 00:11:43:c4:79:83 | 1 | EXT4 | | FWD | P |

An address that is in the forwarding (FWD) state, means that it has been learned by the switch. When in the trunking (TRK) state, the port field represents the trunk group number. If the state for the port is listed as unknown (UNK), the MAC address has not yet been learned by the switch, but has only been seen as a destination address.

When an address is in the unknown state, no outbound port is indicated, although ports that reference the address as a destination will be listed under “Reference ports.”

Show FDB Multicast Address Information

The following commands display Multicast Forwarding Database information..

Table 21. Multicast FDB Information Commands

| Command Syntax and Usage |
|---|
| <pre>show mac-address-table multicast address <MAC address></pre> <p>Displays a single FDB multicast entry by its MAC address. You are prompted to enter the MAC address of the device. Enter the MAC address using the format, xx:xx:xx:xx:xx:xx. For example, 03:00:20:12:34:56</p> <p>You can also enter the MAC address using the format, xxxxxxxxxxxx. For example, 030020123456</p> <p>Command mode: All</p> |
| <pre>show mac-address-table multicast interface port <port alias or number></pre> <p>Displays all FDB multicast entries for a particular port.</p> <p>Command mode: All</p> |
| <pre>show mac-address-table vlan <VLAN number></pre> <p>Displays all FDB multicast entries on a single VLAN.</p> <p>Command mode: All</p> |
| <pre>show mac-address-table multicast</pre> <p>Displays all Multicast MAC entries in the FDB.</p> <p>Command mode: All</p> |

Clearing Entries from the Forwarding Database

To clear the entire FDB, refer to [“Forwarding Database Maintenance” on page 535](#).

Link Aggregation Control Protocol Information

Use these commands to display LACP status information about each port on the EN4093 and EN4093R.

Table 22. LACP Information Commands

| Command Syntax and Usage |
|--|
| <pre>show lacp aggregator <aggregator ID></pre> <p>Displays detailed information about the LACP aggregator.</p> <p>Command mode: All</p> |
| <pre>show interface port <port alias or number> lacp information</pre> <p>Displays LACP information about the selected port.</p> <p>Command mode: All</p> |
| <pre>show lacp information</pre> <p>Displays a summary of LACP information.</p> <p>Command mode: All</p> <p>For details, see page 40.</p> |

Link Aggregation Control Protocol

The following command displays LACP information:

```
show lacp information
```

Command mode: All

| port | mode | adminkey | operkey | selected | prio | aggr | trunk | status | minlinks |
|------|------|----------|---------|----------|-------|------|-------|--------|----------|
| 1 | off | 1 | 1 | no | 32768 | -- | -- | -- | 1 |
| 2 | off | 2 | 2 | no | 32768 | -- | -- | -- | 1 |
| 3 | off | 3 | 3 | no | 32768 | -- | -- | -- | 1 |
| ... | | | | | | | | | |

LACP dump includes the following information for each external port in the EN4093 and EN4093R:

- **mode** Displays the port's LACP mode (active, passive, or off).
- **adminkey** Displays the value of the port's *adminkey*.
- **operkey** Shows the value of the port's operational key.
- **selected** Indicates whether the port has been selected to be part of a Link Aggregation Group.
- **prio** Shows the value of the port priority.
- **aggr** Displays the aggregator associated with each port.
- **trunk** This value represents the LACP trunk group number.
- **status** Displays the status of LACP on the port (up, down or standby).
- **minlinks** Displays the minimum number of active links in the LACP trunk.

Layer 2 Failover Information Commands

Table 23. Layer 2 Failover Information Commands

| Command Syntax and Usage |
|---|
| <pre>show failover trigger <trigger number></pre> <p>Displays detailed information about the selected Layer 2 Failover trigger.</p> <p>Command mode: All</p> |
| <pre>show failover trigger</pre> <p>Displays a summary of Layer 2 Failover information. For details, see page 41.</p> <p>Command mode: All</p> |

Layer 2 Failover Information

The following command displays Layer 2 Failover information:

```
show failover trigger
```

Command mode: All

| |
|--|
| <pre>Trigger 1 Auto Monitor: Enabled Trigger 1 limit: 0 Monitor State: Up Member Status ----- trunk 1 EXT2 Operational EXT3 Operational Control State: Auto Disabled Member Status ----- INT1 Operational INT2 Operational INT3 Operational INT4 Operational ... </pre> |
|--|

A monitor port's Failover status is `Operational` only if all the following conditions hold true:

- Port link is up.
- If Spanning-Tree is enabled, the port is in the `Forwarding` state.
- If the port is a member of an LACP trunk group, the port is aggregated.

If any of these conditions are not true, the monitor port is considered to be failed.

A control port is considered to be operational if the monitor trigger state is `Up`. Even if a port's link status is `Down`, Spanning-Tree status is `Blocking`, and the LACP status is `Not Aggregated`, from a teaming perspective the port status is `Operational`, since the trigger is `Up`.

A control port's status is displayed as `Failed` only if the monitor trigger state is `Down`.

Hot Links Information

The following command displays Hot Links information:

```
show hotlinks information
```

Command mode: All

```
Hot Links Info: Trigger

Current global Hot Links setting: ON
Hot Links BPDU flood: disabled
Hot Links FDB update: disabled
FDB update rate (pps): 500

Current Trigger 1 setting: enabled
name "Test", preempt enabled, fdelay 30 sec

Active state: None

Master settings:
  port EXT22
Backup settings:
  port EXT1
```

Hot Links information includes the following:

- Hot Links status (on or off)
- Status of BPDU flood option
- Status of FDB send option
- Status and configuration of each Hot Links trigger

Edge Control Protocol Information

Table 24. ECP Information Options

| Command Syntax and Usage |
|--|
| <pre>show ecp channels</pre> <p>Displays all Edge Control Protocol (ECP) channels.</p> <p>Command mode: All</p> |
| <pre>show ecp upper-layer-protocols</pre> <p>Displays all registered Upper-Level Protocols (ULPs).</p> <p>Command mode: All</p> |

LLDP Information

The following commands display LLDP information.

Table 25. LLDP Information Commands

| Command Syntax and Usage |
|--|
| <pre>show lldp port</pre> <p>Displays Link Layer Discovery Protocol (LLDP) port information.</p> <p>Command mode: All</p> |
| <pre>show lldp receive</pre> <p>Displays information about the LLDP receive state machine.</p> <p>Command mode: All</p> |
| <pre>show lldp transmit</pre> <p>Displays information about the LLDP transmit state machine.</p> <p>Command mode: All</p> |
| <pre>show lldp remote-device [<1-256> detail]</pre> <p>Displays information received from LLDP-capable devices. To view a sample display, see page 44.</p> |
| <pre>show lldp port <1-16> tlv evb</pre> <p>Displays Edge Virtual Bridge (EVB) type-length-value (TLV) information.</p> <p>Command mode: All</p> |
| <pre>show lldp information</pre> <p>Displays all LLDP information.</p> <p>Command mode: All</p> |

LLDP Remote Device Information

The following command displays LLDP remote device information:

```
show lldp remote-device [<1-256>|detail]
```

Command mode: All

| LLDP Remote Devices Information | | | | |
|---------------------------------|-------|-------------------|------------|---------------------------|
| LocalPort | Index | Remote Chassis ID | RemotePort | Remote System Name |
| MGT | 210 | 00 16 ca ff 7e 00 | 15 | BNT Gb Ethernet Switch... |
| EXT4 | 15 | 00 16 60 f9 3b 00 | 20 | BNT Gb Ethernet Switch... |

LLDP remote device information provides a summary of information about remote devices connected to the switch. To view detailed information about a device, as shown below, follow the command with the index number of the remote device. To view detailed information about all devices, use the `detail` option.

| | |
|---|---------------------|
| Local Port Alias: EXT1 | |
| Remote Device Index | : 15 |
| Remote Device TTL | : 99 |
| Remote Device RxChanges | : false |
| Chassis Type | : Mac Address |
| Chassis Id | : 00-18-b1-33-1d-00 |
| Port Type | : Locally Assigned |
| Port Id | : 23 |
| Port Description | : EXT1 |
| System Name : | |
| System Description : IBM Networking Operating System IBM Flex System Fabric EN4093 and EN4093R 10Gb Scalable Switch, IBM Networking OS: version 7.6.1,0 Boot image: version 7.7.1 | |
| System Capabilities Supported : bridge, router | |
| System Capabilities Enabled : bridge, router | |
| Remote Management Address: | |
| Subtype | : IPv4 |
| Address | : 10.100.120.181 |
| Interface Subtype | : ifIndex |
| Interface Number | : 128 |
| Object Identifier | : |

Unidirectional Link Detection Information

The following commands show unidirectional link detection information.

Table 26. UDLD Information Commands

| Command Syntax and Usage |
|--|
| <pre>show interface port <port alias or number> udld</pre> <p>Displays UDLD information about the selected port.</p> <p>Command mode: All</p> |
| <pre>show udld</pre> <p>Displays all UDLD information.</p> <p>Command mode: All</p> |

UDLD Port Information

The following command displays UDLD information for the selected port:

```
show interface port <port alias or number> udld
```

Command mode: All

```
UDLD information on port EXT1
Port enable administrative configuration setting: Enabled
Port administrative mode: normal
Port enable operational state: link up
Port operational state: advertisement
Port bidirectional status: bidirectional
Message interval: 15
Time out interval: 5
Neighbor cache: 1 neighbor detected

Entry #1
Expiration time: 31 seconds
Device Name:
Device ID: 00:da:c0:00:04:00
Port ID: EXT1
```

UDLD information includes the following:

- Status (enabled or disabled)
- Mode (normal or aggressive)
- Port state (link up or link down)
- Bi-directional status (unknown, unidirectional, bidirectional, TX-RX loop, neighbor mismatch)

OAM Discovery Information

Table 27. OAM Discovery Information Commands

| Command Syntax and Usage |
|--|
| <pre>show interface port <port alias or number> oam</pre> <p>Displays OAM information about the selected port.</p> <p>Command mode: All</p> |
| <pre>show oam</pre> <p>Displays all OAM information.</p> <p>Command mode: All</p> |

OAM Port Information

The following command displays OAM information for the selected port:

```
show interface port <port alias or number> oam
```

Command mode: All

| |
|--|
| <pre>OAM information on port EXT1 State enabled Mode active Link up Satisfied Yes Evaluating No Remote port information: Mode active MAC address 00:da:c0:00:04:00 Stable Yes State valid Yes Evaluating No</pre> |
|--|

OAM port display shows information about the selected port and the peer to which the link is connected.

vLAG Information

The following table lists the information commands for Virtual Link Aggregation Group (vLAG) protocol.

Table 28. vLAG Information Options

| Command Syntax and Usage |
|--|
| <pre>show vlag adminkey <1-65535></pre> <p>Displays vLAG LACP information.</p> <p>Command mode: All</p> |
| <pre>show vlag portchannel <trunk group number></pre> <p>Displays vLAG static trunk group information.</p> <p>Command mode: All</p> |
| <pre>show vlag isl</pre> <p>Displays vLAG Inter-Switch Link (ISL) information.</p> <p>Command mode: All</p> |
| <pre>show vlag information</pre> <p>Displays all vLAG information.</p> <p>Command mode: All</p> |

vLAG Trunk Information

The following command displays vLAG information for the trunk group:

```
show vlag portchannel <trunk group number>
```

Command mode: All

```
vLAG is enabled on trunk 3
Protocol - Static
Current settings: enabled
  ports: 60
Current L2 trunk hash settings:
  smac
Current L3 trunk hash settings:
  sip dip
Current ingress port hash: disabled
Current L4 port hash: disabled
```

802.1X Information

The following command displays 802.1X information:

```
show dot1x information
```

Command mode: All

```

System capability : Authenticator
System status    : disabled
Protocol version : 1
Guest VLAN status : disabled
Guest VLAN      : none

```

| Port | Auth Mode | Auth Status | Authenticator PAE State | Backend Auth State | Assigned VLAN |
|--------|------------|--------------|----------------------------|-----------------------|------------------|
| *INT1 | force-auth | unauthorized | initialize | initialize | none |
| *INT2 | force-auth | unauthorized | initialize | initialize | none |
| INT3 | force-auth | unauthorized | initialize | initialize | none |
| *INT4 | force-auth | unauthorized | initialize | initialize | none |
| *INT5 | force-auth | unauthorized | initialize | initialize | none |
| *INT6 | force-auth | unauthorized | initialize | initialize | none |
| *INT7 | force-auth | unauthorized | initialize | initialize | none |
| INT8 | force-auth | unauthorized | initialize | initialize | none |
| INT9 | force-auth | unauthorized | initialize | initialize | none |
| *INT10 | force-auth | unauthorized | initialize | initialize | none |
| *INT11 | force-auth | unauthorized | initialize | initialize | none |
| *INT12 | force-auth | unauthorized | initialize | initialize | none |
| EXT1 | force-auth | unauthorized | initialize | initialize | none |
| EXT2 | force-auth | unauthorized | initialize | initialize | none |
| *EXT3 | force-auth | unauthorized | initialize | initialize | none |
| *EXT4 | force-auth | unauthorized | initialize | initialize | none |
| *EXT11 | force-auth | unauthorized | initialize | initialize | none |

```

-----
* - Port down or disabled

```

Note: The sample screens that appear in this document might differ slightly from the screens displayed by your system. Screen content varies based on the type of BladeCenter unit that you are using and the firmware versions and options that are installed.

The following table describes the IEEE 802.1X parameters.

Table 29. 802.1X Parameter Descriptions

| Parameter | Description |
|-------------|---|
| Port | Displays each port's alias. |
| Auth Mode | Displays the Access Control authorization mode for the port. The Authorization mode can be one of the following: <ul style="list-style-type: none"> – force-unauth – auto – force-auth |
| Auth Status | Displays the current authorization status of the port, either authorized or unauthorized. |

Table 29. 802.1X Parameter Descriptions (continued)

| Parameter | Description |
|-------------------------|---|
| Authenticator PAE State | <p>Displays the Authenticator Port Access Entity State. The PAE state can be one of the following:</p> <ul style="list-style-type: none"> – initialize – disconnected – connecting – authenticating – authenticated – aborting – held – forceAuth |
| Backend Auth State | <p>Displays the Backend Authorization State. The Backend Authorization state can be one of the following:</p> <ul style="list-style-type: none"> – initialize – request – response – success – fail – timeout – idle |

Spanning Tree Information

The following command displays Spanning Tree information:

```
show spanning-tree stp <1-128> information
```

Command mode: All

```
Spanning Tree Group 1: On (PVRST)
VLANs: 1

Current Root:          Path-Cost  Port Hello MaxAge FwdDel
8063 08:17:f4:34:4c:00  2000   EXT5   2    20    15

Parameters:  Priority Hello  MaxAge  FwdDel  Aging  Topology Change Counts
              61441    2      20      15      300           3

  Port      Prio  Cost    State  Role Designated Bridge      Des Port Type
  -----
INT3        0     0    FWD *
INT5        0     0    FWD *
INT10       0     0    FWD *
INT13       0     0    FWD *
EXT5       128  2000!  FWD  ROOT 8063-08:17:f4:34:4c:00  8001 P2P
EXT6       128  2000!  FWD  DESG f001-fc:cf:62:0a:49:00  8016 P2P
* = STP turned off for this port.
! = Automatic path cost.
```

Note: The sample screens that appear in this document might differ slightly from the screens displayed by your system. Screen content varies based on the type of BladeCenter unit that you are using and the firmware versions and options that are installed.

The switch software uses the Per VLAN Rapid Spanning Tree Protocol (PVRST) spanning tree mode, with IEEE 802.1w Rapid Spanning Tree Protocol (RSTP) or IEEE 802.1s Multiple Spanning Tree Protocol (MSTP), as alternatives. For details see [“RSTP/MSTP/PVRST Information” on page 52](#).

When STP is used, in addition to seeing if STG is enabled or disabled, you can view the following STG bridge information:

Table 30. PVRST/RSTP/MSTP Bridge Parameter Descriptions

| Parameter | Description |
|-------------------|--|
| Current Root | The Current Root shows information about the root bridge for the Spanning Tree. Information includes the priority (in hexadecimal notation) and the MAC address of the root. |
| Priority (bridge) | The Bridge Priority parameter controls which bridge on the network will become the STG root bridge. |
| Hello | The Hello Time parameter specifies, in seconds, how often the root bridge transmits a configuration bridge protocol data unit (BPDU). Any bridge that is not the root bridge uses the root bridge hello value. |

Table 30. PVRST/RSTP/MSTP Bridge Parameter Descriptions (continued)

| Parameter | Description |
|-----------------------|---|
| MaxAge | The Maximum Age parameter specifies, in seconds, the maximum time the bridge waits without receiving a configuration bridge protocol data unit before it reconfigure the STG network. |
| FwdDel | The Forward Delay parameter specifies, in seconds, the amount of time that a bridge port has to wait before it changes from DISC state to LRN state and from LRN state to FWD state. |
| Aging | The Aging Time parameter specifies, in seconds, the amount of time the bridge waits without receiving a packet from a station before removing the station from the Forwarding Database. |
| Topology Change Count | The Topology Change Count shows the number of Topology Changes detected since the last initialization of the Spanning Tree Group (either by reboot or by Spanning Tree mode change). |

The following port-specific information is also displayed:

Table 31. PVRST/RSTP/MSTP Port Parameter Descriptions

| Parameter | Description |
|-------------------|--|
| Priority (port) | The Port Priority parameter helps determine which bridge port becomes the designated port. In a network topology that has multiple bridge ports connected to a single segment, the port with the lowest port priority becomes the designated port for the segment. |
| Cost | The Port Path cost parameter is used to help determine the designated port for a segment. Generally speaking, the faster the port, the lower the path cost. A setting of 0 indicates that the cost will be set to the appropriate default after the link speed has been auto negotiated. |
| State | The State field shows the current state of the port. The State field can be one of the following: Discarding (DISC), Learning (LRN), or Forwarding (FWD). |
| Role | The Role field shows the current role of this port in the Spanning Tree. The port role can be one of the following: Designated (DESG), Root (ROOT), Alternate (ALTN), Backup (BKUP). |
| Designated Bridge | The Designated Bridge shows information about the bridge connected to each port, if applicable. Information includes the priority (in hexadecimal notation) and MAC address of the Designated Bridge. |
| Designated Port | The Designated Port field shows the port on the Designated Bridge to which this port is connected. |

RSTP/MSTP/PVRST Information

The following command displays RSTP/MSTP/PVRST information:

```
show spanning-tree stp <1-128> information
```

Command mode: All

```
Spanning Tree Group 1: On (RSTP)
VLANs: 1

Current Root:          Path-Cost  Port Hello MaxAge FwdDel
ffff 00:13:0a:4f:7d:d0      0    EXT4    2    20    15

Parameters:  Priority Hello  MaxAge  FwdDel  Aging
              61440    2      20     15     300

Port  Prio  Cost    State  Role Designated Bridge      Des Port  Type
-----
INT1   0      0    DSB *
INT2   0      0    DSB *
INT3   0      0    FWD *
INT4   0      0    DSB *
INT5   0      0    DSB *
INT6   0      0    DSB *
INT7   0      0    DSB *
INT8   0      0    DSB *
INT9   0      0    DSB *
INT10  0      0    DSB *
INT11  0      0    DSB *
INT12  0      0    DSB *
INT13  0      0    DSB *
INT14  0      0    DSB *
EXT1  128    2000  FWD  DESG 8000-00:11:58:ae:39:00  8011    P2P
EXT2  128    2000  DISC BKUP 8000-00:11:58:ae:39:00  8011    P2P
EXT3  128    2000  FWD  DESG 8000-00:11:58:ae:39:00  8013    P2P
EXT4  128   20000  DISC BKUP 8000-00:11:58:ae:39:00  8013    Shared
...
* = STP turned off for this port.
```

Note: The sample screens that appear in this document might differ slightly from the screens displayed by your system. Screen content varies based on the type of BladeCenter unit that you are using and the firmware versions and options that are installed.

You can configure the switch software to use the IEEE 802.1w Rapid Spanning Tree Protocol (RSTP), the IEEE 802.1s Multiple Spanning Tree Protocol (MSTP), or Per VLAN Rapid Spanning Tree Protocol (PVRST).

If RSTP/MSTP/PVRST is turned on, you can view the following bridge information for the Spanning Tree Group:.

Table 32. RSTP/MSTP/PVRST Bridge Parameter Descriptions

| Parameter | Description |
|-------------------|--|
| Current Root | The Current Root shows information about the root bridge for the Spanning Tree. Information includes the priority (in hexadecimal notation) and the MAC address of the root. |
| Priority (bridge) | The Bridge Priority parameter controls which bridge on the network will become the STP root bridge. |
| Hello | The Hello Time parameter specifies, in seconds, how often the root bridge transmits a configuration bridge protocol data unit (BPDU). Any bridge that is not the root bridge uses the root bridge hello value. |
| MaxAge | The Maximum Age parameter specifies, in seconds, the maximum time the bridge waits without receiving a configuration bridge protocol data unit before it reconfigures the STP network. |
| FwdDel | The Forward Delay parameter specifies, in seconds, the amount of time that a bridge port has to wait before it changes from listening to learning and from learning state to forwarding state. |
| Aging | The Aging Time parameter specifies, in seconds, the amount of time the bridge waits without receiving a packet from a station before removing the station from the Forwarding Database. |

The following port-specific information is also displayed:

Table 33. RSTP/MSTP/PVRST Port Parameter Descriptions

| Parameter | Description |
|-------------|--|
| Prio (port) | The Port Priority parameter helps determine which bridge port becomes the designated port. In a network topology that has multiple bridge ports connected to a single segment, the port with the lowest port priority becomes the designated port for the segment. |
| Cost | The port Path Cost parameter is used to help determine the designated port for a segment. Generally speaking, the faster the port, the lower the path cost. A setting of 0 indicates that the cost will be set to the appropriate default after the link speed has been auto negotiated. |
| State | The State field shows the current state of the port. The State field in RSTP or MSTP mode can be one of the following: Discarding (DISC), Learning (LRN), Forwarding (FWD), or Disabled (DSB). |

Table 33. RSTP/MSTP/PVRST Port Parameter Descriptions (continued)

| Parameter | Description |
|-------------------|---|
| Role | The Role field shows the current role of this port in the Spanning Tree. The port role can be one of the following: Designated (DESG), Root (ROOT), Alternate (ALTN), Backup (BKUP), Disabled (DSB), Master (MAST). |
| Designated Bridge | The Designated Bridge shows information about the bridge connected to each port, if applicable. Information includes the priority (in hexadecimal notation) and MAC address of the Designated Bridge. |
| Designated Port | The port ID of the port on the Designated Bridge to which this port is connected. |
| Type | Type of link connected to the port, and whether the port is an edge port. Link type values are AUTO, P2P, or SHARED. |

Common Internal Spanning Tree Information

The following command displays Common Internal Spanning Tree (CIST) information:

```
show spanning-tree mstp cist information
```

Command mode: All

```
Mstp Digest: 0xac36177f50283cd4b83821d8ab26de62

Common Internal Spanning Tree:

VLANs MAPPED: 1-4094
VLANs: 1 2 4095

Current Root:          Path-Cost  Port MaxAge FwdDel
8000 00:11:58:ae:39:00    2026      0    20    15

Cist Regional Root:    Path-Cost
8000 00:11:58:ae:39:00      0

Parameters:  Priority  MaxAge  FwdDel  Hops
              32768    20     15     20

Port  Prio  Cost    State  Role  Designated Bridge      Des Port Hello Type
-----
1     128    2000!   FWD    ROOT  fffe-00:13:0a:4f:7d:d0  8011  2    P2P#
23    128    2000!   DISC   ALTN  fffe-00:22:00:24:46:00  8012  2    P2P#
MGT   0       0       FWD   *

* = STP turned off for this port.
! = Automatic path cost.
# = PVST Protection enabled for this port.
```


In addition to seeing if Common Internal Spanning Tree (CIST) is enabled or disabled, you can view the following CIST bridge information:

Table 34. CIST Parameter Descriptions

| Parameter | Description |
|--------------------|--|
| CIST Root | The CIST Root shows information about the root bridge for the Common Internal Spanning Tree (CIST). Values on this row of information refer to the CIST root. |
| CIST Regional Root | The CIST Regional Root shows information about the root bridge for this MSTP region. Values on this row of information refer to the regional root. |
| Priority (bridge) | The bridge priority parameter controls which bridge on the network will become the STP root bridge. |
| Hello | The hello time parameter specifies, in seconds, how often the root bridge transmits a configuration bridge protocol data unit (BPDU). Any bridge that is not the root bridge uses the root bridge hello value. |
| MaxAge | The maximum age parameter specifies, in seconds, the maximum time the bridge waits without receiving a configuration bridge protocol data unit before it reconfigure the STP network. |
| FwdDel | The forward delay parameter specifies, in seconds, the amount of time that a bridge port has to wait before it changes from learning state to forwarding state. |
| Hops | The maximum number of bridge hops a packet can traverse before it is dropped. The default value is 20. |

The following port-specific CIST information is also displayed:

Table 35. CIST Parameter Descriptions

| Parameter | Description |
|-------------|--|
| Prio (port) | The port priority parameter helps determine which bridge port becomes the designated port. In a network topology that has multiple bridge ports connected to a single segment, the port with the lowest port priority becomes the designated port for the segment. |
| Cost | The port path cost parameter is used to help determine the designated port for a segment. Generally speaking, the faster the port, the lower the path cost. A setting of 0 indicates that the cost will be set to the appropriate default after the link speed has been auto negotiated. |
| State | The state field shows the current state of the port. The state field can be either Discarding (DISC), Learning (LRN), or Forwarding (FWD). |

Table 35. CIST Parameter Descriptions (continued)

| Parameter | Description |
|-------------------|---|
| Role | The Role field shows the current role of this port in the Spanning Tree. The port role can be one of the following: Designated (DESG), Root (ROOT), Alternate (ALTN), Backup (BKUP), Disabled (DSB), Master (MAST), or Unknown (UNK). |
| Designated Bridge | The Designated Bridge shows information about the bridge connected to each port, if applicable. Information includes the priority (in hexadecimal notation) and MAC address of the Designated Bridge. |
| Designated Port | The port ID of the port on the Designated Bridge to which this port is connected. |
| Type | Type of link connected to the port, and whether the port is an edge port. Link type values are AUTO, P2P, or SHARED. |

Trunk Group Information

The following command displays Trunk Group information:

```
show portchannel information
```

Command mode: All

```
Trunk group 1: Enabled
Protocol - Static
Port state:
  EXT1: STG 1 forwarding
  EXT2: STG 1 forwarding
```

When trunk groups are configured, you can view the state of each port in the various trunk groups.

Note: If Spanning Tree Protocol on any port in the trunk group is set to `forwarding`, the remaining ports in the trunk group will also be set to `forwarding`.

VLAN Information

Table 36. VLAN Information Commands

| |
|--|
| Command Syntax and Usage |
| <pre>show vlan <VLAN number></pre> <p>Displays general VLAN information.</p> |
| <pre>show protocol-vlan <protocol number></pre> <p>Displays protocol VLAN information.</p> <p>Command mode: All</p> |
| <pre>show private-vlan <VLAN number></pre> <p>Displays private VLAN information.</p> <p>Command mode: All</p> |
| <pre>show vlan information</pre> <p>Displays information about all VLANs, including:</p> <ul style="list-style-type: none"> – VLAN number and name – Port membership – VLAN status (enabled or disabled) – Protocol VLAN status – Private VLAN status – Spanning Tree membership – VMAP configuration |

The following command displays VLAN information:

```
show vlan <VLAN number>
```

Command mode: All

| VLAN | Name | Status | MGT | Ports |
|------|--------------|--------|-----|--|
| 1 | Default VLAN | ena | dis | INT1A-INT14B EXT1-EXT10 EXT15-EXT22 |
| 4095 | Mgmt VLAN | ena | ena | MGT1 EXTM |

Note: The sample screens that appear in this document might differ slightly from the screens displayed by your system. Screen content varies based on the type of BladeCenter unit that you are using and the firmware versions and options that are installed.

This information display includes all configured VLANs and all member ports that have an active link state. Port membership is represented in slot/port format.

VLAN information includes:

- VLAN Number
- VLAN Type

- Status
- Management status of the VLAN
- Port membership of the VLAN
- Protocol-based VLAN information
- Private VLAN configuration

Layer 3 Information

Table 37. Layer 3 Information Commands

| Command Syntax and Usage |
|--|
| <pre>show ip route</pre> <p>Displays all routes configured on the switch. For details, see page 63.</p> <p>Command mode: All</p> |
| <pre>show arp</pre> <p>Displays Address Resolution Protocol (ARP) information. For details, see page 64.</p> <p>Command mode: All</p> |
| <pre>show ip bgp information [IPv4 address] [IPv4 mask]</pre> <p>Displays Border Gateway Protocol (BGP) information. For details, see page 67.</p> <p>Command mode: All</p> |
| <pre>show ip ospf information</pre> <p>Displays OSPF information. For more OSPF information options, see page 68.</p> <p>Command mode: All</p> |
| <pre>show ipv6 ospf information</pre> <p>Displays OSPFv3 information. For more OSPFv3 information options, see page 73.</p> <p>Command mode: All</p> |
| <pre>show ip rip interface</pre> <p>Displays RIP user's configuration. For details, see page 77.</p> <p>Command mode: All</p> |
| <pre>show ipv6 route</pre> <p>Displays IPv6 routing information. For more information options, see page 78.</p> <p>Command mode: All</p> |
| <pre>show ipv6 neighbors</pre> <p>Displays IPv6 Neighbor Discovery cache information. For more information options, see page 79.</p> <p>Command mode: All</p> |
| <pre>show ipv6 prefix</pre> <p>Displays IPv6 Neighbor Discovery prefix information. For details, see page 80.</p> <p>Command mode: All</p> |
| <pre>show ip ecmp</pre> <p>Displays ECMP static route information. For details, see page 80.</p> <p>Command mode: All</p> |

Table 37. Layer 3 Information Commands (continued)

| |
|--|
| Command Syntax and Usage |
| <p>show ip igmp groups</p> <p>Displays IGMP Information. For more IGMP information options, see page 81.</p> <p>Command mode: All</p> |
| <p>show ipv6 mld groups</p> <p>Displays Multicast Listener Discovery (MLD) information. For more MLD information options, see page 85.</p> <p>Command mode: All</p> |
| <p>show ip vrrp information</p> <p>Displays VRRP information. For details, see page 87.</p> <p>Command mode: All</p> |
| <p>show interface ip</p> <p>Displays IPv4 interface information. For details, see page 87.</p> <p>Command mode: All</p> |
| <p>show ipv6 interface <interface number></p> <p>Displays IPv6 interface information. For details, see page 88.</p> <p>Command mode: All</p> |
| <p>show ipv6 pmtu [<destination IPv6 address>]</p> <p>Displays IPv6 Path MTU information. For details, see page 88.</p> <p>Command mode: All</p> |
| <p>show ip interface brief</p> <p>Displays IP Information. For details, see page 89.</p> <p>IP information, includes:</p> <ul style="list-style-type: none"> – IP interface information: Interface number, IP address, subnet mask, VLAN number, and operational status. – Default gateway information: Metric for selecting which configured gateway to use, gateway number, IP address, and health status – IP forwarding settings, network filter settings, route map settings <p>Command mode: All</p> |
| <p>show ikev2</p> <p>Displays IKEv2 information. For more information options, see page 91.</p> <p>Command mode: All</p> |
| <p>show ipsec manual-policy</p> <p>Displays information about manual key management policy for IP security. For more information options, see page 93.</p> <p>Command mode: All</p> |

Table 37. Layer 3 Information Commands (continued)

| Command Syntax and Usage |
|---|
| <pre>show ip pim component [<1-2>]</pre> <p>Displays Protocol Independent Multicast (PIM) component information. For more PIM information options, see page 94.</p> <p>Command mode: All</p> |
| <pre>show layer3</pre> <p>Dumps all Layer 3 switch information available (10K or more, depending on your configuration).</p> <p>If you want to capture dump data to a file, set your communication software on your workstation to capture session data prior to issuing the dump commands.</p> <p>Command mode: All</p> |

IP Routing Information

Using the commands listed below, you can display all or a portion of the IP routes currently held in the switch.

Table 38. Route Information Commands

| Command Syntax and Usage |
|--|
| <pre>show ip route address <IP address></pre> <p>Displays a single route by destination IP address.</p> <p>Command mode: All</p> |
| <pre>show ip route gateway <IP address></pre> <p>Displays routes to a single gateway.</p> <p>Command mode: All</p> |
| <pre>show ip route type {indirect direct local broadcast martian multicast}</pre> <p>Displays routes of a single type. For a description of IP routing types, see Table 39 on page 63.</p> <p>Command mode: All</p> |
| <pre>show ip route tag {fixed static addr rip ospf bgp broadcast martian multicast}</pre> <p>Displays routes of a single tag. For a description of IP routing tags, see Table 40 on page 63.</p> <p>Command mode: All</p> |
| <pre>show ip route interface <interface number></pre> <p>Displays routes on a single interface.</p> <p>Command mode: All</p> |
| <pre>show ip route ecmphash</pre> <p>Displays the current ECMP hashing mechanism.</p> <p>Command mode: All</p> |
| <pre>show ip route static</pre> <p>Displays static routes configured on the switch.</p> <p>Command mode: All</p> |
| <pre>show ip route</pre> <p>Displays all routes configured in the switch.</p> <p>Command mode: All</p> <p>For more information, see page 63.</p> |

Show All IP Route Information

The following command displays IP route information:

```
show ip route
```

Command mode: All

| Status code: * - best | | | | | | |
|-----------------------|-----------------|----------------|-----------|-----------|------|-----|
| Destination | Mask | Gateway | Type | Tag | Metr | If |
| * 12.0.0.0 | 255.0.0.0 | 11.0.0.1 | direct | fixed | | 128 |
| * 12.0.0.1 | 255.255.255.255 | 11.0.0.1 | local | addr | | 128 |
| * 12.255.255.255 | 255.255.255.255 | 11.255.255.255 | broadcast | broadcast | | 128 |
| * 12.0.0.0 | 255.0.0.0 | 12.0.0.1 | direct | fixed | | 12 |
| * 12.0.0.1 | 255.255.255.255 | 12.0.0.1 | local | addr | | 12 |
| * 255.255.255.255 | 255.255.255.255 | 12.255.255.255 | broadcast | broadcast | | 2 |
| * 224.0.0.0 | 224.0.0.0 | 0.0.0.0 | martian | martian | | |
| * 224.0.0.5 | 255.255.255.255 | 0.0.0.0 | multicast | addr | | |

The following table describes the `Type` parameters.

Table 39. IP Routing Type Parameters

| Parameter | Description |
|-----------|--|
| indirect | The next hop to the host or subnet destination will be forwarded through a router at the <code>Gateway</code> address. |
| direct | Packets will be delivered to a destination host or subnet attached to the switch. |
| local | Indicates a route to one of the switch's IP interfaces. |
| broadcast | Indicates a broadcast route. |
| martian | The destination belongs to a host or subnet which is filtered out. Packets to this destination are discarded. |
| multicast | Indicates a multicast route. |

The following table describes the `Tag` parameters.

Table 40. IP Routing Tag Parameters

| Parameter | Description |
|-----------|---|
| fixed | The address belongs to a host or subnet attached to the switch. |
| static | The address is a static route which has been configured on the EN4093 and EN4093R 10Gb Scalable Switch. |
| addr | The address belongs to one of the switch's IP interfaces. |
| rip | The address was learned by the Routing Information Protocol (RIP). |
| ospf | The address was learned by Open Shortest Path First (OSPF). |
| bgp | The address was learned via Border Gateway Protocol (BGP) |

Table 40. IP Routing Tag Parameters (continued)

| Parameter | Description |
|-----------|--|
| broadcast | Indicates a broadcast address. |
| martian | The address belongs to a filtered group. |
| multicast | Indicates a multicast address. |

ARP Information

The ARP information includes IP address and MAC address of each entry, address status flags (see [Table 42 on page 65](#)), VLAN and port for the address, and port referencing information.

Table 41. ARP Information Commands

| Command Syntax and Usage |
|--|
| <pre>show arp find <IP address></pre> <p>Displays a single ARP entry by IP address.</p> <p>Command mode: All</p> |
| <pre>show arp interface port <port alias or number></pre> <p>Displays the ARP entries on a single port.</p> <p>Command mode: All</p> |
| <pre>show arp vlan <VLAN number></pre> <p>Displays the ARP entries on a single VLAN.</p> <p>Command mode: All</p> |
| <pre>show arp</pre> <p>Displays all ARP entries. including:</p> <ul style="list-style-type: none"> – IP address and MAC address of each entry – Address status flag (see below) – The VLAN and port to which the address belongs – The ports which have referenced the address (empty if no port has routed traffic to the IP address shown) <p>For more information, see page 65.</p> <p>Command mode: All</p> |
| <pre>show arp reply</pre> <p>Displays the ARP address list: IP address, IP mask, MAC address, and VLAN flags.</p> <p>Command mode: All</p> |

Show All ARP Entry Information

The following command displays ARP information:

```
show arp
```

Command mode: All

| IP address | Flags | MAC address | VLAN | Age | Port |
|--------------|-------|-------------------|------|-----|------|
| 12.20.1.1 | | 00:15:40:07:20:42 | 4095 | 0 | INT8 |
| 12.20.20.16 | | 00:30:13:e3:44:14 | 4095 | 2 | INT8 |
| 12.20.20.18 | | 00:30:13:e3:44:14 | 4095 | 2 | INT6 |
| 12.20.23.111 | | 00:1f:29:95:f7:e5 | 4095 | 6 | INT6 |

The `Port` field shows the target port of the ARP entry.

The `Flags` field is interpreted as follows:

Table 42. ARP Dump Flag Parameters

| Flag | Description |
|------|---|
| P | Permanent entry created for switch IP interface. |
| R | Indirect route entry. |
| U | Unresolved ARP entry. The MAC address has not been learned. |

ARP Address List Information

The following command displays owned ARP address list information:

```
show arp reply
```

Command mode: All

| IP address | IP mask | MAC address | VLAN | Pass-Up |
|---------------|-----------------|-------------------|------|---------|
| 205.178.18.66 | 255.255.255.255 | 00:70:cf:03:20:04 | | P |
| 205.178.50.1 | 255.255.255.255 | 00:70:cf:03:20:06 | 1 | |
| 205.178.18.64 | 255.255.255.255 | 00:70:cf:03:20:05 | 1 | |

BGP Information

Table 43. BGP Peer Information Commands

| Command Syntax and Usage |
|--|
| <pre>show ip bgp neighbor information</pre> <p>Displays BGP peer information.</p> <p>Command mode: All</p> <p>See page 67 for a sample output.</p> |
| <pre>show ip bgp neighbor summary</pre> <p>Displays peer summary information such as AS, message received, message sent, up/down, state.</p> <p>Command mode: All</p> <p>See page 67 for a sample output.</p> |
| <pre>show ip bgp aggregate-address</pre> <p>Displays BGP peer routes.</p> <p>Command mode: All</p> <p>See page 67 for a sample output.</p> |
| <pre>show ip bgp information</pre> <p>Displays the BGP routing table.</p> <p>Command mode: All</p> <p>See page 67 for a sample output.</p> |

BGP Peer information

Following is an example of the information provided by the following command:

```
show ip bgp neighbor information
```

Command mode: All

```
BGP Peer Information:

3: 2.1.1.1          , version 4, TTL 225
  Remote AS: 100, Local AS: 100, Link type: IBGP
  Remote router ID: 3.3.3.3,   Local router ID: 1.1.201.5
  BGP status: idle, Old status: idle
  Total received packets: 0, Total sent packets: 0
  Received updates: 0, Sent updates: 0
  Keepalive: 60, Holdtime: 180, MinAdvTime: 60
  LastErrorCode: unknown(0), LastErrorSubcode: unspecified(0)
  Established state transitions: 1

4: 2.1.1.4          , version 4, TTL 225
  Remote AS: 100, Local AS: 100, Link type: IBGP
  Remote router ID: 4.4.4.4,   Local router ID: 1.1.201.5
  BGP status: idle, Old status: idle
  Total received packets: 0, Total sent packets: 0
  Received updates: 0, Sent updates: 0
  Keepalive: 60, Holdtime: 180, MinAdvTime: 60
  LastErrorCode: unknown(0), LastErrorSubcode: unspecified(0)
  Established state transitions: 1
```

BGP Summary Information

Following is an example of the information provided by the following command:

```
show ip bgp neighbor summary
```

Command mode: All

```
BGP Peer Summary Information:
  Peer          V   AS   MsgRcvd  MsgSent  Up/Down   State
  -----
1: 205.178.23.142 4   142    113     121 00:00:28 established
2: 205.178.15.148 0   148     0       0 never      connect
```

BGP Peer Routes Information

Following is an example of the information provided by the following command:

```
show ip bgp aggregate-address
```

Command mode: All

```
Current BGP aggregation settings:
1: addr 4.2.0.0, mask 255.0.0.0, enabled
2: addr 5.5.0.0, mask 255.255.0.0, enabled
```

Dump BGP Information

Following is an example of the information provided by the following command:

```
show ip bgp information [<IPv4 network> <IPv4 mask>]
```

Command mode: All

| Network | Mask | Next Hop | Metr | LcPrf | Wght | Path |
|-----------------|---------------|----------|------|-------|------|------|
| *> 1.1.1.0 | 255.255.255.0 | 0.0.0.0 | | | 0 | ? |
| *> 10.100.100.0 | 255.255.255.0 | 0.0.0.0 | | | 0 | ? |
| *> 10.100.120.0 | 255.255.255.0 | 0.0.0.0 | | | 0 | ? |

The 13.0.0.0 is filtered out by rrmmap; or, a loop detected.

The IPv4 network and mask options restrict the output to a specific network in the BGP routing table.

OSPF Information

Table 44. OSPF Information Commands

| Command Syntax and Usage |
|---|
| <pre>show ip ospf general-information</pre> <p>Displays general OSPF information.</p> <p>Command mode: All</p> <p>See page 70 for a sample output.</p> |
| <pre>show ip ospf area information</pre> <p>Displays area information for all areas.</p> <p>Command mode: All</p> |
| <pre>show ip ospf area <0-2></pre> <p>Displays area information for a particular area index.</p> <p>Command mode: All</p> |
| <pre>show ip ospf interface loopback <1-5></pre> <p>Displays loopback information for a particular interface. If no parameter is supplied, it displays loopback information for all the interfaces.</p> <p>Command mode: All</p> <p>See page 70 for a sample output.</p> |
| <pre>show interface ip {<interface number>} ospf</pre> <p>Displays interface information for a particular interface. If no parameter is supplied, it displays information for all the interfaces.</p> <p>Command mode: All</p> <p>See page 70 for a sample output.</p> |
| <pre>show ip ospf area-virtual-link information</pre> <p>Displays information about all the configured virtual links.</p> <p>Command mode: All</p> |

Table 44. OSPF Information Commands (continued)

| Command Syntax and Usage |
|--|
| <pre>show ip ospf neighbor</pre> <p>Displays the status of all the current neighbors.</p> <p>Command mode: All</p> |
| <pre>show ip ospf summary-range <0-2></pre> <p>Displays the list of summary ranges belonging to non-NSSA areas.</p> <p>Command mode: All</p> |
| <pre>show ip ospf summary-range-nssa <0-2></pre> <p>Displays the list of summary ranges belonging to NSSA areas.</p> <p>Command mode: All</p> |
| <pre>show ip ospf routes</pre> <p>Displays OSPF routing table.</p> <p>Command mode: All</p> <p>See page 72 for a sample output.</p> |
| <pre>show ip ospf information</pre> <p>Displays OSPF information.</p> <p>Command mode: All</p> |

OSPF General Information

The following command displays general OSPF information:

```
show ip ospf general-information
```

Command mode: All

```
OSPF Version 2
Router ID: 10.10.10.1
Started at 1663 and the process uptime is 4626
Area Border Router: yes, AS Boundary Router: no
LS types supported are 6
External LSA count 0
External LSA checksum sum 0x0
Number of interfaces in this router is 2
Number of virtual links in this router is 1
16 new lsa received and 34 lsa originated from this router
Total number of entries in the LSDB 10
Database checksum sum 0x0
Total neighbors are 1, of which
                2 are >=INIT state,
                2 are >=EXCH state,
                2 are =FULL state

Number of areas is 2, of which 3-transit 0-nssa
  Area Id : 0.0.0.0
  Authentication : none
  Import ASEextern : yes
  Number of times SPF ran : 8
  Area Border Router count : 2
  AS Boundary Router count : 0
  LSA count : 5
  LSA Checksum sum : 0x2237B
  Summary : noSummary
```

OSPF Interface Loopback Information

The following command displays OSPF interface loopback information:

```
show ip ospf interface loopback <interface number>
```

Command mode: All

```
Ip Address 5.5.5.5, Area 0.0.0.1, Passive interface, Admin Status UP
Router ID 1.1.1.2, State Loopback, Priority 1
Designated Router (ID) 0.0.0.0, Ip Address 0.0.0.0
Backup Designated Router (ID) 0.0.0.0, Ip Address 0.0.0.0
Timer intervals, Hello 10, Dead 40, Wait 40, Retransmit 5, Transit delay
1
Neighbor count is 0 If Events 1, Authentication type none
```

OSPF Interface Information

The following command displays OSPF interface information:

```
show ip ospf interface <interface number>
```

Command mode: All

```
Ip Address 10.10.12.1, Area 0.0.0.1, Admin Status UP
Router ID 10.10.10.1, State DR, Priority 1
Designated Router (ID) 10.10.10.1, Ip Address 10.10.12.1
Backup Designated Router (ID) 10.10.14.1, Ip Address 10.10.12.2
Timer intervals, Hello 10, Dead 40, Wait 1663, Retransmit 5,
Neighbor count is 1 If Events 4, Authentication type none
```


OSPF Database Information

Table 45. OSPF Database Information Commands

| Command Syntax and Usage |
|--|
| <pre>show ip ospf database advertising-router <router ID></pre> <p>Takes advertising router as a parameter. Displays all the Link State Advertisements (LSAs) in the LS database that have the advertising router with the specified router ID, for example: 20.1.1.1.</p> <p>Command mode: All</p> |
| <pre>show ip ospf database asbr-summary [advertising-router <router ID> link-state-id <A.B.C.D> self]</pre> <p>Displays ASBR summary LSAs. The use of this command is as follows:</p> <ol style="list-style-type: none"> asbr-summary advertising-router 20.1.1.1 displays ASBR summary LSAs having the advertising router 20.1.1.1. asbr-summary link-state-id 10.1.1.1 displays ASBR summary LSAs having the link state ID 10.1.1.1. asbr-summary self displays the self advertised ASBR summary LSAs. asbr-summary with no parameters displays all the ASBR summary LSAs. <p>Command mode: All</p> |
| <pre>show ip ospf database database-summary</pre> <p>Displays the following information about the LS database in a table format:</p> <ol style="list-style-type: none"> Number of LSAs of each type in each area. Total number of LSAs for each area. Total number of LSAs for each LSA type for all areas combined. Total number of LSAs for all LSA types for all areas combined. <p>No parameters are required.</p> <p>Command mode: All</p> |
| <pre>show ip ospf database external [advertising-router <router ID> link-state-id <A.B.C.D> self]</pre> <p>Displays the AS-external (type 5) LSAs with detailed information of each field of the LSAs.</p> <p>Command mode: All</p> |
| <pre>show ip ospf database network [advertising-router <router ID> link-state-id <A.B.C.D> self]</pre> <p>Displays the network (type 2) LSAs with detailed information of each field of the LSA.network LS database.</p> <p>Command mode: All</p> |

Table 45. OSPF Database Information Commands (continued)

| Command Syntax and Usage |
|---|
| <pre>show ip ospf database nssa</pre> <p>Displays the NSSA (type 7) LSAs with detailed information of each field of the LSAs.</p> <p>Command mode: All</p> |
| <pre>show ip ospf database router [advertising-router <router ID> link-state-id <A.B.C.D> self]</pre> <p>Displays the router (type 1) LSAs with detailed information of each field of the LSAs.</p> <p>Command mode: All</p> |
| <pre>show ip ospf database self</pre> <p>Displays all the self-advertised LSAs. No parameters are required.</p> <p>Command mode: All</p> |
| <pre>show ip ospf database summary [advertising-router <router ID> link-state-id <A.B.C.D> self]</pre> <p>Displays the network summary (type 3) LSAs with detailed information of each field of the LSAs.</p> <p>Command mode: All</p> |
| <pre>show ip ospf database</pre> <p>Displays all the LSAs.</p> <p>Command mode: All</p> |

OSPF Information Route Codes

The following command displays OSPF route information:

```
show ip ospf routes
```

Command mode: All

```
Codes: IA - OSPF inter area,
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
IA 10.10.0.0/16 via 200.1.1.2
IA 40.1.1.0/28 via 20.1.1.2
IA 80.1.1.0/24 via 200.1.1.2
IA 100.1.1.0/24 via 20.1.1.2
IA 140.1.1.0/27 via 20.1.1.2
IA 150.1.1.0/28 via 200.1.1.2
E2 172.18.1.1/32 via 30.1.1.2
E2 172.18.1.2/32 via 30.1.1.2
E2 172.18.1.3/32 via 30.1.1.2
E2 172.18.1.4/32 via 30.1.1.2
E2 172.18.1.5/32 via 30.1.1.2
E2 172.18.1.6/32 via 30.1.1.2
E2 172.18.1.7/32 via 30.1.1.2
E2 172.18.1.8/32 via 30.1.1.2
```

OSPFv3 Information

Table 46. OSPFv3 Information Options

| Command Syntax and Usage |
|--|
| <pre>show ipv6 ospf area <area index (0-2)></pre> <p>Displays the area information.</p> <p>Command mode: All</p> |
| <pre>show ipv6 ospf areas</pre> <p>Displays the OSPFv3 Area Table.</p> <p>Command mode: All</p> |
| <pre>show ipv6 ospf interface <interface number></pre> <p>Displays interface information for a particular interface. If no parameter is supplied, it displays information for all the interfaces. To view a sample display, see page 75.</p> <p>Command mode: All</p> |
| <pre>show ipv6 ospf area-virtual-link</pre> <p>Displays information about all the configured virtual links.</p> <p>Command mode: All</p> |
| <pre>show ipv6 ospf neighbor <nbr router-id (A.B.C.D)></pre> <p>Displays the status of a neighbor with a particular router ID. If no router ID is supplied, it displays the information about all the current neighbors.</p> <p>Command mode: All</p> |
| <pre>show ipv6 ospf host</pre> <p>Displays OSPFv3 host configuration information.</p> <p>Command mode: All</p> |
| <pre>show ipv6 ospf request-list <nbr router-id (A.B.C.D)></pre> <p>Displays the OSPFv3 request list. If no router ID is supplied, it displays the information about all the current neighbors.</p> <p>Command mode: All</p> |
| <pre>show ipv6 ospf retrans-list <nbr router-id (A.B.C.D)></pre> <p>Displays the OSPFv3 retransmission list. If no router ID is supplied, it displays the information about all the current neighbors.</p> <p>Command mode: All</p> |
| <pre>show ipv6 ospf summary-prefix <area index (0-2)></pre> <p>Displays the OSPFv3 external summary-address configuration information.</p> <p>Command mode: All</p> |

Table 46. OSPFv3 Information Options

| Command Syntax and Usage |
|---|
| <pre>show ipv6 ospf redist-config</pre> <p>Displays OSPFv3 redistribution information to be applied to routes learned from the route table.</p> <p>Command mode: All</p> |
| <pre>show ipv6 ospf area-range information</pre> <p>Displays OSPFv3 summary ranges.</p> <p>Command mode: All</p> |
| <pre>show ipv6 ospf routes</pre> <p>Displays OSPFv3 routing table. To view a sample display, see page 76.</p> <p>Command mode: All</p> |
| <pre>show ipv6 ospf border-routers</pre> <p>Displays OSPFv3 routes to an ABR or ASBR.</p> <p>Command mode: All</p> |
| <pre>show ipv6 ospf information</pre> <p>Displays all OSPFv3 information. To view a sample display, see page 74.</p> <p>Command mode: All</p> |

OSPFv3 Information Dump

| | |
|--|--------------------------------------|
| Router Id: 1.0.0.1 | ABR Type: Standard ABR |
| SPF schedule delay: 5 secs | Hold time between two SPF's: 10 secs |
| Exit Overflow Interval: 0 | Ref BW: 100000 |
| Trace Value: 0x00008000 | Ext Lsdb Limit: none |
| As Scope Lsa: 2 | Checksum Sum: 0xfe16 |
| Passive Interface: Disable | |
| Nssa Asbr Default Route Translation: Disable | |
| Autonomous System Boundary Router | |
| Redistributing External Routes from connected, metric 10, metric type asExtType1, no tag set | |
| Number of Areas in this router 1 | |
| Area 0.0.0.0 | |
| Number of interfaces in this area is 1 | |
| Number of Area Scope Lsa: 7 | Checksum Sum: 0x28512 |
| Number of Indication Lsa: 0 | SPF algorithm executed: 2 times |

OSPFv3 Interface Information

The following command displays OSPFv3 interface information:

```
show ipv6 ospf interface
```

Command mode: All

| OspfV3 Interface Information | | |
|---|--------------------|------------------|
| Interface Id: 1 | Instance Id: 0 | Area Id: 0.0.0.0 |
| Local Address: fe80::222:ff:fe7d:5d00 | Router Id: 1.0.0.1 | |
| Network Type: BROADCAST | Cost: 1 | State: BACKUP |
| Designated Router Id: 2.0.0.2 | local address: | |
| fe80::218:b1ff:feal:6c01 | | |
| Backup Designated Router Id: 1.0.0.1 | local address: | |
| fe80::222:ff:fe7d:5d00 | | |
| Transmit Delay: 1 sec | Priority: 1 | IfOptions: 0x0 |
| Timer intervals configured: | | |
| Hello: 10, Dead: 40, Retransmit: 5 | | |
| Hello due in 6 sec | | |
| Neighbor Count is: 1, Adjacent neighbor count is: 1 | | |
| Adjacent with neighbor 2.0.0.2 | | |

OSPFv3 Database Information

Table 47. OSPFv3 Database Information Options

| Command Syntax and Usage |
|---|
| <pre>show ipv6 ospf database as-external [detail hex]</pre> <p>Displays AS-External LSAs database information. If no parameter is supplied, it displays condensed information.</p> <p>Command mode: All</p> |
| <pre>show ipv6 ospf database inter-prefix [detail hex]</pre> <p>Displays Inter-Area Prefix LSAs database information. If no parameter is supplied, it displays condensed information.</p> <p>Command mode: All</p> |
| <pre>show ipv6 ospf database inter-router [detail hex]</pre> <p>Displays Inter-Area router LSAs database information. If no parameter is supplied, it displays condensed information.</p> <p>Command mode: All</p> |
| <pre>show ipv6 ospf database intra-prefix [detail hex]</pre> <p>Displays Intra-Area Prefix LSAs database information. If no parameter is supplied, it displays condensed information.</p> <p>Command mode: All</p> |

Table 47. OSPFv3 Database Information Options

| Command Syntax and Usage | |
|---|--|
| <pre>show ipv6 ospf database link [detail hex]</pre> | <p>Displays Link LSAs database information. If no parameter is supplied, it displays condensed information.</p> <p>Command mode: All</p> |
| <pre>show ipv6 ospf database network [detail hex]</pre> | <p>Displays Network LSAs database information. If no parameter is supplied, it displays condensed information.</p> <p>Command mode: All</p> |
| <pre>show ipv6 ospf database router [detail hex]</pre> | <p>Displays the Router LSAs with detailed information of each field of the LSAs. If no parameter is supplied, it displays condensed information.</p> <p>Command mode: All</p> |
| <pre>show ipv6 ospf database nssa [detail hex]</pre> | <p>Displays Type-7 (NSSA) LSA database information. If no parameter is supplied, it displays condensed information.</p> <p>Command mode: All</p> |
| <pre>show ipv6 ospf database [detail hex]</pre> | <p>Displays all the LSAs.</p> <p>Command mode: All</p> |

OSPFv3 Route Codes Information

The following command displays OSPFv3 route information:

```
show ipv6 ospf routes
```

Command mode: All

| Dest/ Prefix-Length | NextHop/ IfIndex | Cost | Rt. Type | Area |
|------------------------|------------------------------------|------|-----------|---------|
| 3ffe::10:0:0:0 /80 | fe80::290:69ff fe90:b4bf /vlan1 | 30 | interArea | 0.0.0.0 |
| 3ffe::20:0:0:0 /80 | fe80::290:69ff fe90:b4bf /vlan1 | 20 | interArea | 0.0.0.0 |
| 3ffe::30:0:0:0 /80 | :: /vlan2 | 10 | intraArea | 0.0.0.0 |
| 3ffe::60:0:0:6 /128 | fe80::211:22ff fe33:4426 /vlan2 | 10 | interArea | 0.0.0.0 |

Routing Information Protocol

Table 48. Routing Information Protocol Commands

| Command Syntax and Usage |
|---|
| <pre>show ip rip routes</pre> <p>Displays RIP routes.</p> <p>Command mode: All</p> <p>For more information, see page 77.</p> |
| <pre>show interface ip <interface number> rip</pre> <p>Displays RIP user's configuration.</p> <p>Command mode: All</p> <p>For more information, see page 77.</p> |

RIP Routes Information

The following command displays RIP route information:

```
show ip rip routes
```

Command mode: All

```
>> IP Routing#  
  
30.1.1.0/24 directly connected  
3.0.0.0/8 via 30.1.1.11 metric 4  
4.0.0.0/16 via 30.1.1.11 metric 16  
10.0.0.0/8 via 30.1.1.2 metric 3  
20.0.0.0/8 via 30.1.1.2 metric 2
```

This table contains all dynamic routes learned through RIP, including the routes that are undergoing garbage collection with metric = 16. This table does not contain locally configured static routes.

RIP Interface Information

The following command displays RIP user information:

```
show ip rip interface <interface number>
```

Command mode: All

```
RIP USER CONFIGURATION :  
  RIP: ON, update 30  
  RIP on Interface   49 : 101.1.1.10,      enabled  
  version 2, listen enabled, supply enabled, default none  
  poison disabled, split horizon enabled, trigg enabled, mcast enabled, metric 1  
  auth none,key none
```

IPv6 Routing Information

[Table 49](#) describes the IPv6 Routing information options.

Table 49. IPv6 Routing Information Commands

| Command Syntax and Usage |
|--|
| <pre>show ipv6 route address <IPv6 address></pre> <p>Displays a single route by destination IP address.</p> <p>Command mode: All</p> |
| <pre>show ipv6 route gateway <default gateway address></pre> <p>Displays routes to a single gateway.</p> <p>Command mode: All</p> |
| <pre>show ipv6 route type {connected static ospf}</pre> <p>Displays routes of a single type. For a description of IP routing types, see Table 39 on page 63.</p> <p>Command mode: All</p> |
| <pre>show ipv6 route interface <interface number></pre> <p>Displays routes on a single interface.</p> <p>Command mode: All</p> |
| <pre>show ipv6 route summary</pre> <p>Displays a summary of IPv6 routing information, including inactive routes.</p> <p>Command mode: All</p> |
| <pre>show ipv6 route</pre> <p>Displays all IPv6 routing information. For more information, see page 78.</p> <p>Command mode: All</p> |

IPv6 Routing Table

The following command displays IPv6 routing information:

```
show ipv6 route
```

Command mode: All

| |
|--|
| <pre>IPv6 Routing Table - 3 entries Codes : C - Connected, S - Static O - OSPF M - Management Gateway, E - Ext-Management Gateway S ::/0 [1/20] via 2001:2:3:4::1, Interface 2 C 2001:2:3:4::/64 [1/1] via ::, Interface 2 C fe80::20f:6aff:feec:f701/128 [1/1] via ::, Interface 2</pre> |
|--|

Note: The first number inside the brackets represents the metric and the second number represents the preference for the route.

IPv6 Neighbor Discovery Cache Information

Table 50. IPv6 Neighbor Discovery Cache Information Commands

| Command Syntax and Usage |
|--|
| <pre>show ipv6 neighbors find <IPv6 address></pre> <p>Shows a single IPv6 Neighbor Discovery cache entry by IP address. Command mode: All</p> |
| <pre>show ipv6 neighbors interface port <port alias or number></pre> <p>Shows IPv6 Neighbor Discovery cache entries on a single port. Command mode: All</p> |
| <pre>show ipv6 neighbors vlan <VLAN number></pre> <p>Shows IPv6 Neighbor Discovery cache entries on a single VLAN. Command mode: All</p> |
| <pre>show ipv6 neighbors static</pre> <p>Displays static IPv6 Neighbor Discovery cache entries. Command mode: All</p> |
| <pre>show ipv6 neighbors</pre> <p>Shows all IPv6 Neighbor Discovery cache entries. For more information, see page 79. Command mode: All</p> |

IPv6 Neighbor Discovery Cache Information

The following command displays a summary of IPv6 Neighbor Discovery cache information:

```
show ipv6 neighbors
```

Command mode: All

| IPv6 Address | Age | Link-layer Addr | State | IF | VLAN | Port |
|--------------------------|-----|-------------------|-----------|----|------|------|
| 2001:2:3:4::1 | 10 | 00:50:bf:b7:76:b0 | Reachable | 2 | 1 | EXT1 |
| fe80::250:bfff:feb7:76b0 | 0 | 00:50:bf:b7:76:b0 | Stale | 2 | 1 | EXT2 |

IPv6 Neighbor Discovery Prefix Information

The following command displays a summary of IPv6 Neighbor Discovery prefix information:

```
show ipv6 prefix
```

Command mode: All

```
Codes: A - Address , P - Prefix-Advertisement
       D - Default , N - Not Advertised
       [L] - On-link Flag is set
       [A] - Autonomous Flag is set

AD 10:: 64 [LA] Valid lifetime 2592000 , Preferred lifetime 604800
P 20:: 64 [LA] Valid lifetime 200 , Preferred lifetime 100
```

Neighbor Discovery prefix information includes information about all configured prefixes.

The following command displays IPv6 Neighbor Discovery prefix information for an interface:

```
show ipv6 prefix interface <interface number>
```

Command mode: All

ECMP Static Route Information

The following command displays Equal Cost Multi-Path (ECMP) route information:

```
show ip ecmp
```

Command mode: All

```
Current ecmp static routes:
Destination      Mask          Gateway      If    GW Status
-----
10.10.1.1        255.255.255.255 100.10.1.1   1     up
                  200.20.2.2     1           down
10.20.2.2        255.255.255.255 10.233.3.3   1     up
10.20.2.2        255.255.255.255 10.234.4.4   1     up
10.20.2.2        255.255.255.255 10.235.5.5   1     up
```

ECMP route information shows the status of each ECMP route configured on the switch.

ECMP Hashing Result

The following command displays the status of ECMP hashing on each switch:

```
show ip route ecmp hash
```

Command mode: All

| |
|-----------------------------|
| ECMP Hash Mechanism: dipsip |
|-----------------------------|

IGMP Multicast Group Information

Table 51. IGMP Multicast Group Information Commands

| Command Syntax and Usage |
|--|
| <pre>show ip igmp querier vlan <VLAN number></pre> <p>Displays IGMP Querier information. For details, see page 82.</p> <p>Command mode: All</p> |
| <pre>show ip igmp snoop</pre> <p>Displays IGMP Snooping information.</p> <p>Command mode: All</p> |
| <pre>show ip igmp relay</pre> <p>Displays IGMP Relay information.</p> <p>Command mode: All</p> |
| <pre>show ip igmp mrouter information</pre> <p>Displays IGMP Multicast Router information. For details, see page 84.</p> <p>Command mode: All</p> |
| <pre>show ip igmp mrouter vlan <VLAN number></pre> <p>Displays IGMP Multicast Router information for the specified VLAN.</p> <p>Command mode: All</p> |
| <pre>show ip igmp filtering</pre> <p>Displays current IGMP Filtering parameters.</p> <p>Command mode: All</p> |
| <pre>show ip igmp profile <1-16></pre> <p>Displays information about the current IGMP filter.</p> <p>Command mode: All</p> |
| <pre>show ip igmp groups address <IP address></pre> <p>Displays a single IGMP multicast group by its IP address.</p> <p>Command mode: All</p> |

Table 51. IGMP Multicast Group Information Commands (continued)

| Command Syntax and Usage |
|---|
| <pre>show ip igmp groups vlan <VLAN number></pre> <p>Displays all IGMP multicast groups on a single VLAN.</p> <p>Command mode: All</p> |
| <pre>show ip igmp groups interface port <port alias or number></pre> <p>Displays all IGMP multicast groups on a single port.</p> <p>Command mode: All</p> |
| <pre>show ip igmp groups portchannel <trunk number></pre> <p>Displays all IGMP multicast groups on a single trunk group.</p> <p>Command mode: All</p> |
| <pre>show ip igmp groups detail <IP address></pre> <p>Displays details about an IGMP multicast group, including source and timer information.</p> <p>Command mode: All</p> |
| <pre>show ip igmp groups</pre> <p>Displays information for all multicast groups. For details, see page 83.</p> <p>Command mode: All</p> |
| <pre>show ip igmp ipmcgrp</pre> <p>Displays information for all IPMC groups. For details, see page 84.</p> <p>Command mode: All</p> |
| <pre>show ip igmp counters</pre> <p>Displays IGMP counters for all VLANs.</p> <p>Command mode: All</p> |
| <pre>show ip igmp vlan <VLAN number> counter</pre> <p>Displays IGMP counters for a specific VLAN.</p> <p>Command mode: All</p> |

IGMP Querier Information

The following command displays IGMP Querier information:

```
show ip igmp querier vlan <VLAN number>
```

Command mode: All

```
Current IGMP Querier information:
IGMP Querier information for vlan 1:
Other IGMP querier - none
Switch-querier enabled, current state: Querier
Switch-querier type: Ipv4, address 0.0.0.0,
Switch-querier general query interval: 125 secs,
Switch-querier max-response interval: 100 'tenths of secs',
Switch-querier startup interval: 31 secs, count: 2
Switch-querier robustness: 2
IGMP configured version is v3
IGMP Operating version is v3
```

IGMP Querier information includes:

- VLAN number
- Querier status
 - Other IGMP querier—none
 - IGMP querier present, address: (IP or MAC address)
Other IGMP querier present, interval (minutes:seconds)
- Querier election type (IPv4 or MAC) and address
- Query interval
- Querier startup interval
- Maximum query response interval
- Querier robustness value
- Other IGMP querier present, interval (minutes:seconds)
- IGMP Querier current state: Querier/Non-Querier
- IGMP version number

IGMP Group Information

The following command displays IGMP Group information:

```
show ip igmp groups
```

Command mode: All

```
Note: Local groups (224.0.0.x) are not snooped/relayed and will not appear.
Source          Group          VLAN    Port    Version  Mode  Expires  Fwd
-----
10.1.1.1        232.1.1.1      2       EXT4    V3       INC   4:16    Yes
10.1.1.5        232.1.1.1      2       EXT4    V3       INC   4:16    Yes
*               232.1.1.1      2       EXT4    V3       INC   -        No
10.10.10.43     235.0.0.1      9       EXT1    V3       INC   2:26    Yes
*               236.0.0.1      9       EXT1    V3       EXC   -        Yes
```

IGMP Group information includes:

- IGMP source address
- IGMP Group address
- VLAN and port
- IGMP version
- IGMPv3 filter mode

- Expiration timer value
- IGMP multicast forwarding state

IGMP Multicast Router Information

The following command displays Mrouter information:

```
show ip igmp mrouter information
```

Command mode: All

| SrcIP | VLAN | Port | Version | Expires | MRT | QRV | QQIC |
|-------------|------|------|---------|---------|---------|-----|------|
| 10.1.1.1 | 2 | EXT4 | V3 | 4:09 | 128 | 2 | 125 |
| 10.1.1.5 | 2 | EXT6 | V2 | 4:09 | 125 | - | - |
| 10.10.10.43 | 9 | EXT7 | V2 | static | unknown | - | - |

IGMP Mrouter information includes:

- Source IP address
- VLAN and port where the Mrouter is connected
- IGMP version
- Mrouter expiration
- Maximum query response time
- Querier's Robustness Variable (QRV)
- Querier's Query Interval Code (QQIC)

IPMC Group Information

The following command displays IGMP IPMC group information:

```
show ip igmp ipmcgrp
```

Command mode: All

```
Total number of displayed ipmc groups: 4
Legend(possible values in Type column) :
SH - static host      DR - dynamic registered
SP - static primary  DU - dynamic unregistered
SB - static backup   M - mrouter
O - other
```

| Source | Group | Vlan | Port | Type | Timeleft |
|--------|-----------|------|------|------|----------|
| * | 232.0.0.1 | 1 | - | DU | 6 sec |
| * | 232.0.0.2 | 1 | - | DU | 6 sec |
| * | 232.0.0.3 | 1 | - | DU | 6 sec |
| * | 232.0.0.4 | 1 | - | DU | 6 sec |

IGMP IPMC Group information includes:

- IGMP source address
- IGMP group address
- VLAN and port
- Type of IPMC group

- Expiration timer value

MLD information

[Table 52](#) describes the commands used to view Multicast Listener Discovery (MLD) information.

Table 52. MLD Information Commands

| Command Syntax and Usage |
|--|
| <pre>show ipv6 mld groups</pre> <p>Displays MLD multicast group information.</p> <p>Command mode: All</p> |
| <pre>show ipv6 mld groups address <IPv6 address></pre> <p>Displays group information for the specified IPv6 address.</p> <p>Command mode: All</p> |
| <pre>show ipv6 mld groups interface port <port alias or number></pre> <p>Displays MLD groups on a single interface port.</p> <p>Command mode: All</p> |
| <pre>show ipv6 mld groups portchannel <trunk group number></pre> <p>Displays groups on a single port channel.</p> <p>Command mode: All</p> |
| <pre>show ipv6 mld groups vlan <VLAN number></pre> <p>Displays groups on a single VLAN.</p> <p>Command mode: All</p> |
| <pre>show ipv6 mld mrouter</pre> <p>Displays all MLD Mrouter ports. See page 86 for sample output.</p> <p>Command mode: All</p> |

MLD Mrouter Information

The following command displays MLD Mrouter information:

```
show ipv6 mld mrouter
```

Command mode: All

```
Source: fe80:0:0:0:200:14ff:fea8:40c9
Port/Vlan: 26/4
Interface: 3
QRV: 2 QQIC:125
Maximum Response Delay: 1000
Version: MLDv2 Expires:1:02
```

The following table describes the MLD Mrouter information displayed in the output.

Table 53. MLD Mrouter

| Statistic | Description |
|------------------------|---|
| Source | Displays the link-local address of the reporter. |
| Port/Vlan | Displays the port/vlan on which the general query is received. |
| Interface | Displays the interface number on which the general query is received. |
| QRV | Displays the Querier's robustness variable value. |
| QQIC | Displays the Querier's query interval code. |
| Maximum Response Delay | Displays the configured maximum query response time. |
| Version | Displays the MLD version configured on the interface. |
| Expires | Displays the amount of time that must pass before the multicast router decides that there are no more listeners for a multicast address or a particular source on a link. |

VRRP Information

Virtual Router Redundancy Protocol (VRRP) support on EN4093 and EN4093R 10Gb Scalable Switch provides redundancy between routers in a LAN. This is accomplished by configuring the same virtual router IP address and ID number on each participating VRRP-capable routing device. One of the virtual routers is then elected as the master, based on a number of priority criteria, and assumes control of the shared virtual router IP address. If the master fails, one of the backup virtual routers will assume routing authority and take control of the virtual router IP address.

The following command displays VRRP information:

```
show ip vrrp information
```

Command mode: All

```
VRRP information:
1: vrid 2, 205.178.18.210, if 1, reater, prio 100, master
2: vrid 1, 205.178.18.202, if 1, reater, prio 100, backup
3: vrid 3, 205.178.18.204, if 1, reater, prio 100, master
```

When virtual routers are configured, you can view the status of each virtual router using this command. VRRP information includes:

- Virtual router number
- Virtual router ID and IP address
- Interface number
- Ownership status
 - `owner` identifies the preferred master virtual router. A virtual router is the owner when the IP address of the virtual router and its IP interface are the same.
 - `reater` identifies virtual routers which are not owned by this device.
- Priority value. During the election process, the virtual router with the highest priority becomes master.
- Activity status
 - `master` identifies the elected master virtual router.
 - `backup` identifies that the virtual router is in backup mode.
 - `init` identifies that the virtual router is waiting for a startup event. For example, once it receives a startup event, it transitions to master if its priority is 255, (the IP address owner), or transitions to backup if it is not the IP address owner.

Interface Information

The following command displays interface information:

```
show interface ip
```

Command mode: All

```
Interface information:
1: IP4 172.31.35.5      255.255.0.0 172.31.255.255,  vlan 1, up
128: IP4 10.90.90.97   255.255.255.0 10.90.90.255,  vlan 4095, up
```

For each interface, the following information is displayed:

- IPv4 interface address and subnet mask
- IPv6 address and prefix
- VLAN assignment
- Status (up, down, disabled)

IPv6 Interface Information

The following command displays IPv6 interface information:

```
show ipv6 interface <interface number>
```

Command mode: All

```
Interface information:
 2: IP6 2001:0:0:0:225:3ff:febb:bb15/64          , vlan 1, up
     fe80::225:3ff:febb:bb15
Link local address:
     fe80::225:3ff:febb:bb15
Global unicast address(es):
     2001::225:3ff:febb:bb15/64
Anycast address(es):
     Not Configured.
Joined group address(es):
     ff02::1
     ff02::2
     ff02::1:ffbb:bb15
MTU is 1500
ICMP redirects are enabled
ND DAD is enabled, Number of DAD attempts: 1
ND router advertisement is disabled
```

For each interface, the following information is displayed:

- IPv6 interface address and prefix
- VLAN assignment
- Status (up, down, disabled)
- Path MTU size
- Status of ICMP redirects
- Status of Neighbor Discovery (ND) Duplicate Address Detection (DAD)
- Status of Neighbor Discovery router advertisements

IPv6 Path MTU Information

The following command displays IPv6 Path MTU information:

```
show ipv6 pmtu [<destination IPv6 address>]
```

Command mode: All

```
Path MTU Discovery info:
Max Cache Entry Number : 10
Current Cache Entry Number: 2
Cache Timeout Interval : 10 minutes
Destination Address          Since      PMTU
5000:1::3                    00:02:26  1400
FE80::203:A0FF:FED6:141D     00:06:55  1280
```

Path MTU Discovery information provides information about entries in the Path MTU cache. The PMTU field indicates the maximum packet size in octets that can successfully traverse the path from the switch to the destination node. It is equal to the minimum link MTU of all the links in the path to the destination node.

IP Information

The following command displays Layer 3 information:

```
show ip interface brief
```

Command mode: All

```
IP information:
  AS number 0

Interface information:
126: IP6 0:0:0:0:0:0:0:0/0          , vlan 4095, up
      fe80::200:ff:fe00:ef
128: IP4 9.43.95.121      255.255.255.0   9.43.95.255,   vlan 4095, up

Loopback interface information:

Default gateway information: metric strict
  4: 9.43.95.254,      FAILED

Default IP6 gateway information:

Current BOOTP relay settings: OFF
Global servers:
-----
Server 1 address 0.0.0.0
Server 2 address 0.0.0.0
Server 3 address 0.0.0.0
Server 4 address 0.0.0.0
Server 5 address 0.0.0.0

Current IP forwarding settings: ON, dirbr disabled, icmprd disabled

Current network filter settings:
  none

Current route map settings:
RIP is disabled.

OSPF is disabled.

OSPFv3 is disabled.

BGP is disabled.
```

IP information includes:

- IP interface information: Interface number, IP address, subnet mask, broadcast address, VLAN number, and operational status.
- Default gateway information: Metric for selecting which configured gateway to use, gateway number, IP address, and health status
- BootP relay settings
- IP forwarding settings, including the forwarding status of directed broadcasts, and the status of ICMP re-directs
- Network filter settings, if applicable
- Route map settings, if applicable

DHCP Snooping Binding Table Information

The following command displays the DHCP binding table:

```
show ip dhcp snooping binding
```

Command mode: All

| Mac Address | IP Address | Lease(seconds) | Type | VLAN | Interface |
|-------------------|-----------------|----------------|---------|------|-----------|
| 00:00:01:00:02:01 | 10.0.0.1 | 1600 | dynamic | 100 | port 1 |
| 02:1c:5f:d1:18:9c | 210.38.197.63 | 86337 | Static | 127 | 1 |
| 06:51:4d:e6:16:2d | 194.116.155.190 | 86337 | Static | 105 | 1 |
| 08:69:0f:1d:ba:3d | 40.90.17.26 | 86337 | Static | 150 | 1 |
| 08:a2:6d:00:36:56 | 40.194.18.213 | 86337 | Static | 108 | 1 |
| 0e:a7:f8:a2:74:2c | 130.254.47.129 | 86337 | Static | 171 | 1 |
| 0e:b7:64:02:97:7c | 35.92.27.110 | 86337 | Static | 249 | 1 |
| 0e:f7:5b:6a:74:d8 | 75.179.93.39 | 86337 | Static | 232 | 1 |

Total number of bindings: 8

The DHCP Snooping binding table displays information for each entry in the table. Each entry has a MAC address, an IP address, the lease time, the interface to which the entry applies, and the VLAN to which the interface belongs.

IKEv2 Information

The following table lists commands that display information about IKEv2.

Table 54. IKEv2 Information Commands

| Command Syntax and Usage |
|---|
| <code>show ikev2</code> Displays all IKEv2 information. See page 92 for sample output. Command mode: All |
| <code>show ikev2 ca-cert</code> Displays the CA certificate. Command mode: All |
| <code>show ikev2 host-cert</code> Displays the host certificate. Command mode: All |
| <code>show ikev2 identity</code> Displays IKEv2 identity information. Command mode: All |
| <code>show ikev2 preshare-key</code> Displays the IKEv2 preshare key. Command mode: All |
| <code>show ikev2 proposal</code> Displays the IKEv2 proposal. Command mode: All |
| <code>show ikev2 retransmit-interval</code> Displays the IKEv2 retransmit interval. Command mode: All |
| <code>show ikev2 sa</code> Displays the IKEv2 SA. Command mode: All |

IKEv2 Information Dump

The following command displays IKEv2 information:

```
show ikev2
```

Command mode: All

```
IKEv2 retransmit time:      20

IKEv2 cookie notification:  disable

IKEv2 authentication method: Pre-shared key

IKEv2 proposal:
Cipher:                     3des
Authentication:            sha1
DH Group:                   dh-2

Local preshare key:        ibm123

IKEv2 choose IPv6 address as ID type
No SAD entries.
```

IKEv2 information includes:

- IKEv2 retransmit time, in seconds.
- Whether IKEv2 cookie notification is enabled.
- The IKEv2 proposal in force. This includes the encryption algorithm (cipher), the authentication algorithm type, and the Diffie-Hellman (DH) group, which determines the strength of the key used in the key exchange process. Higher DH group numbers are more secure but require additional time to compute the key.
- The local preshare key.
- Whether IKEv2 is using IPv4 or IPv6 addresses as the ID type.
- Security Association Database (SAD) entries, if applicable.

IPsec Information

The following table describes the commands used to display information about IPsec.

Table 55. IPsec Information Commands

| Command Syntax and Usage |
|--|
| <code>show ipsec sa</code> Displays all security association information. Command mode: All |
| <code>show ipsec spd</code> Displays all security policy information. Command mode: All |
| <code>show ipsec dynamic-policy <1-10></code> Displays dynamic policy information. Command mode: All |
| <code>show ipsec manual-policy <1-10></code> Displays manual policy information. See page 94 for sample output. Command mode: All |
| <code>show ipsec transform-set <1-10></code> Displays IPsec transform set information. Command mode: All |
| <code>show ipsec traffic-selector <1-10></code> Displays IPsec traffic selector information. Command mode: All |

IPsec Manual Policy Information

The following command displays IPsec manual key management policy information:

```
show ipsec manual-policy
```

Command mode: All

| | |
|---------------------------------|--|
| IPsec manual policy 1 ----- | |
| IP Address: | 2002:0:0:0:0:0:151 |
| Associated transform ID: | 1 |
| Associated traffic selector ID: | 1 |
| IN-ESP SPI: | 9900 |
| IN-ESP encryption KEY: | 3456789abcdef012 |
| IN-ESP authentication KEY: | 23456789abcdef0123456789abcdef0123456789 |
| OUT-ESP SPI: | 7700 |
| OUT-ESP encryption KEY: | 6789abcdef012345 |
| OUT-ESP authentication KEY: | 56789abcdef0123456789abcdef0123456789abc |
| Applied on interface: | |
| interface 1 | |

IPsec manual policy information includes:

- The IP address of the remote peer
- The transform set ID associated with this policy
- Traffic selector ID associated with this policy
- ESP inbound SPI
- ESP inbound encryption key
- ESP inbound authentication key
- ESP outbound SPI
- ESP outbound encryption key
- ESP outbound authentication key
- The interface to which this manual policy has been applied

PIM Information

Table 56. PIM Information Options

| Command Syntax and Usage |
|--|
| <pre>show ip pim bsr [<component ID>]</pre> <p>Displays information about the PIM bootstrap router (BSR).</p> <p>Command mode: All</p> |
| <pre>show ip pim component [<component ID (1-2)>]</pre> <p>Displays PIM component information. For details, see page 96.</p> <p>Command mode: All</p> |
| <pre>show ip pim interface [<interface number> detail port <port number>]</pre> <p>Displays PIM interface information. To view sample output, see page 96.</p> <p>Command mode: All</p> |

Table 56. PIM Information Options (continued)

| Command Syntax and Usage |
|---|
| <pre>show ip pim neighbor [<interface number> port <port number>]</pre> <p>Displays PIM neighbor information. To view sample output, see page 97.</p> <p>Command mode: All</p> |
| <pre>show ip pim neighbor-filters</pre> <p>Displays information about PIM neighbor filters.</p> <p>Command mode: All</p> |
| <pre>show ip pim mroute [<component ID> count flags group <multicast group address> inteface {<interface number> port <port number>} source <multicast source address>]</pre> <p>Displays information about PIM multicast routes. For more information about displaying PIM multicast route information, see page 97.</p> <p>Command mode: All</p> |
| <pre>show ip pim rp-candidate [<component ID>]</pre> <p>Displays a list of the candidate Rendezvous Points configured.</p> <p>Command mode: All</p> |
| <pre>show ip pim rp-set [<RP IP address>]</pre> <p>Displays a list of the Rendezvous Points learned.</p> <p>Command mode: All</p> |
| <pre>show ip pim rp-static [<component ID>]</pre> <p>Displays a list of the static Rendezvous Points configured.</p> <p>Command mode: All</p> |
| <pre>show ip pim elected-rp [group <multicast group address>]</pre> <p>Displays a list of the elected Rendezvous Points.</p> <p>Command mode: All</p> |

PIM Component Information

The following command displays Protocol Independent Multicast (PIM) component information:

```
show ip pim component [<component ID>]
```

Command mode: All

```
PIM Component Information
-----
Component-Id: 1
  PIM Mode: sparse,   PIM Version: 2
  Elected BSR: 0.0.0.0
  Candidate RP Holdtime: 0
```

PIM component information includes the following:

- Component ID
- Mode (sparse, dense)
- PIM Version
- Elected Bootstrap Router (BSR) address
- Candidate Rendezvous Point (RP) hold time, in seconds

PIM Interface Information

The following command displays information about PIM interfaces:

```
show ip pim interface
```

Command mode: All

| Address | IfName/IfId | Ver/Mode | Nbr Count | Qry Interval | DR-Address | DR-Prio |
|----------|-------------|----------|--------------|-----------------|------------|---------|
| 40.0.0.3 | net4/4 | 2/Sparse | 1 | 30 | 40.0.0.3 | 1 |
| 50.0.0.3 | net5/5 | 2/Sparse | 0 | 30 | 50.0.0.3 | 1 |

PIM interface information includes the following for each PIM interface:

- IP address
- Name and ID
- Version and mode
- Neighbor count
- Query interval
- Designated Router address
- Designated Router priority value

PIM Neighbor Information

The following command displays PIM neighbor information:

```
show ip pim neighbor
```

Command mode: All

| Neighbour Address | IfName/Idx | Uptime/Expiry | Ver | DRPri/Mode | CompId | Override Interval | Lan Delay |
|-------------------|------------|---------------|-----|------------|--------|-------------------|-----------|
| 40.0.0.2 | net4/4 | 00:00:37/79 | v2 | 1/S | 1 | 0 | 0 |
| 40.0.0.4 | net1/160 | 00:03:41/92 | v2 | 32/S | 20 | 0 | 0 |

PIM neighbor information includes the following:

- Neighbor IP address, interface name, and interface ID
- Name and ID of interface used to reach the PIM neighbor
- Up time (the time since this neighbor became the neighbor of the local router)
- Expiry Time (the minimum time remaining before this PIM neighbor expires)
- Version number
- Designated Router priority and mode
- Component ID
- Override interval
- LAN delay interval

PIM Multicast Route Information Commands

Table 57. PIM Multicast Route Information Options

| Command Syntax and Usage |
|--|
| <pre>show ip pim mroute [<component ID>]</pre> <p>Displays PIM multicast routes for the selected component.</p> <p>Command mode: All</p> |
| <pre>show ip pim mroute flags [s] [r] [w]</pre> <p>Displays PIM multicast routes based on the selected entry flags. Enter flags in any combination:</p> <ul style="list-style-type: none"> – s: Shortest Path Tree (SPT) bit – r: Rendezvous Point Tree (RPT) bit – w: Wildcard bit <p>Command mode: All</p> |
| <pre>show ip pim mroute group <multicast group IP address></pre> <p>Displays PIM multicast routes for the selected multicast group.</p> <p>Command mode: All</p> |
| <pre>show ip pim mroute interface <interface number></pre> <p>Displays PIM multicast routes for the selected incoming IP interface.</p> <p>Command mode: All</p> |

Table 57. PIM Multicast Route Information Options (continued)

| Command Syntax and Usage |
|---|
| <pre>show ip pim mroute source <multicast source IP address></pre> <p>Displays PIM multicast routes for the selected source IP address.</p> <p>Command mode: All</p> |
| <pre>show ip pim mroute count</pre> <p>Displays a count of PIM multicast routes of each type.</p> <p>Command mode: All</p> |
| <pre>show ip pim mroute</pre> <p>Displays information about all PIM multicast routes.</p> <p>Command mode: All</p> |

PIM Multicast Route Information

The following command displays PIM multicast route information:

```
show ip pim mroute
```

Command mode: All

| |
|---|
| <pre>IP Multicast Routing Table ----- Route Flags S: SPT Bit W: Wild Card Bit R: RPT Bit Timers: Uptime/Expires (8.8.8.111, 224.2.2.100) ,00:42:03/00:01:11 Incoming Interface : net44 ,RPF nbr : 44.44.44.1 ,Route Flags : S Outgoing InterfaceList : net17, Forwarding/Sparse ,00:42:03/--- (*, 224.2.2.100) ,00:45:15/--- ,RP : 88.88.88.2 Incoming Interface : net5 ,RPF nbr : 5.5.5.2 ,Route Flags : WR Outgoing InterfaceList : net17, Forwarding/Sparse ,00:45:15/--- Total number of (*,G) entries : 1 Total number of (S,G) entries : 1</pre> |
|---|

Quality of Service Information

Table 58. QoS Information Options

| Command Syntax and Usage |
|--|
| <pre>show qos transmit-queue</pre> <p>Displays mapping of 802.1p value to Class of Service queue number, and COS queue weight value.</p> <p>Command mode: All</p> |
| <pre>show qos transmit-queue information</pre> <p>Displays all 802.1p information.</p> <p>Command mode: All</p> <p>For details, see page 99.</p> |
| <pre>show qos random-detect</pre> <p>Displays WRED ECN information.</p> <p>Command mode: All</p> |

802.1p Information

The following command displays 802.1p information:

```
show qos transmit-queue information
```

Command mode: All

```

Current priority to COS queue information:
Priority  COSq  Weight
-----  ----  -----
    0         0     1
    1         1     2
    2         2     3
    3         3     4
    4         4     5
    5         5     7
    6         6    15
    7         7     0

Current port priority information:
Port     Priority  COSq  Weight
-----  -
INT1      0         0     1
INT2      0         0     1
...
MGT1      0         0     1
MGT2      0         0     1
EXT1      0         0     1
EXT2      0         0     1
EXT3      0         0     1
EXT4      0         0     1
...

```

The following table describes the IEEE 802.1p priority-to-COS queue information.

Table 59. 802.1p Priority-to-COS Queue Parameter Descriptions

| Parameter | Description |
|-----------|--|
| Priority | Displays the 802.1p Priority level. |
| COSq | Displays the Class of Service queue. |
| Weight | Displays the scheduling weight of the COS queue. |

The following table describes the IEEE 802.1p port priority information.

Table 60. 802.1p Port Priority Parameter Descriptions

| Parameter | Description |
|-----------|--------------------------------------|
| Port | Displays the port alias. |
| Priority | Displays the 802.1p Priority level. |
| COSq | Displays the Class of Service queue. |
| Weight | Displays the scheduling weight. |

WRED and ECN Information

The following command displays WRED and ECN information:

```
show qos random-detect
```

Command mode: All

```

Current wred and ecn configuration:
Global ECN: Disable
Global WRED: Disable

--WRED--TcpMinThr--TcpMaxThr--TcpDrate--NonTcpMinThr--NonTcpMaxThr--NonTcpDrate--
TQ0:  Dis      0      0      0      0      0
0
TQ1:  Dis      0      0      0      0      0
0
TQ2:  Dis      0      0      0      0      0
0
TQ3:  Dis      0      0      0      0      0
0
TQ4:  Dis      0      0      0      0      0
0
TQ5:  Dis      0      0      0      0      0
0
TQ6:  Dis      0      0      0      0      0
0
TQ7:  Dis      0      0      0      0      0
0
...

```

Access Control List Information Commands

Table 61. ACL Information Options

| Command Syntax and Usage |
|---|
| <pre>show access-control list <ACL number></pre> <p>Displays ACL list information. For details, see page 102.</p> <p>Command mode: All</p> |
| <pre>show access-control list6 <ACL number></pre> <p>Displays IPv6 ACL list information.</p> <p>Command mode: All</p> |
| <pre>show access-control group <ACL group number></pre> <p>Displays ACL group information.</p> <p>Command mode: All</p> |
| <pre>show access-control vmap <VMAP number></pre> <p>Displays VMAP information.</p> <p>Command mode: All</p> |

Access Control List Information

The following command displays Access Control List (ACL) information:

```
show access-control list <ACL number>
```

Command mode: All

```
Current ACL information:
-----
Filter 2 profile:
 Ethernet
  - VID      : 2/0xffff
  Actions    : Permit
  Statistics  : enabled
```

Access Control List (ACL) information includes configuration settings for each ACL and ACL Group.

Table 62. ACL Parameter Descriptions

| Parameter | Description |
|-------------------------|--|
| Filter <i>x</i> profile | Indicates the ACL number. |
| Actions | Displays the configured action for the ACL. |
| Statistics | Displays the status of ACL statistics configuration (enabled or disabled). |

OpenFlow Information

The following commands display OpenFlow information.

Table 63. OpenFlow Information Options

| Command Syntax and Usage |
|---|
| <pre>show openflow [flow-allocation information statistics table]</pre> <p>Displays the current OpenFlow configuration. For more information, see page 104.</p> <ul style="list-style-type: none">– <code>flow-allocation</code> displays the configured, current and maximum number of flows for each OpenFlow instance. For more information, see page 104.– <code>information</code> displays the configuration for each OpenFlow instance. For more information, see page 105.– <code>statistics</code> displays traffic statistics for each OpenFlow instance. For more information see page 204.– <code>table</code> displays the basic and emergency flow tables for each OpenFlow instance. For more information, see page 106 <p>Command mode: All</p> |
| <pre>show openflow instance <I-2> [information statistics table]</pre> <p>Displays OpenFlow information for the specified instance ID:</p> <ul style="list-style-type: none">– <code>information</code> displays the instance configuration– <code>statistics</code> displays traffic statistics– <code>table</code> displays the basic and emergency flow tables <p>Command mode: All</p> |

OpenFlow Global Configuration Information

The following command displays the global OpenFlow configuration parameters for all instances:

```
show openflow
```

Command mode: All

```
Protocol Version: 1
Openflow State: Enabled
FDB Table Priority: 1000

Openflow Instance ID: 1
  state: enabled , buffering: disabled
  retry 4, emergency time-out 30
  echo req interval 30, echo reply time-out 15
  min-flow-timeout : 0, use controller provided values.
  max flows acl      : Maximum Available
  max flows unicast fdb : Maximum Available
  max flows multicast fdb : Maximum Available
  emergency feature: enabled
  Controller Id: 1
    Not Active Controller
    IP Address: 10.10.10.10, port: 6633, Mgt-Port

Openflow instance 2 is currently disabled

Openflow Edge ports : None
Openflow Management ports : None
```

OpenFlow Flow Allocation Information

The following command displays the OpenFlow flow allocation for all instances:

```
show openflow flow-allocation
```

Command mode: All

```
Flow Allocation Information

Instance 1

Maximum ACL Count Configured      : Maximum Available
Maximum Unicast FDB Count Configured : Maximum Available
Maximum Multicast FDB Count Configured: Maximum Available

Basic Entries

Current ACL Count                  : 0
Current Unicast FDB Count          : 0
Current Multicast FDB Count        : 0

Emergency Entries

Current ACL Count                  : 0
Current Unicast FDB Count          : 0
Current Multicast FDB Count        : 0

Maximum Current Availability

Maximum Available ACL Count        : 750
Maximum Available Unicast FDB Count : 123904
Maximum Available Multicast FDB Count: 4096

Instance 2
...
```

OpenFlow Configuration Information

The following command displays the OpenFlow configuration for all instances:

```
show openflow information
```

Command mode: All

```
Openflow Instance ID: 1
State : Enabled
DataPath ID: 0x00010817f4aeb500
Max Retries per controller: 4
Echo Request Interval: 30
Echo Reply Timeout: 15
Emergency Timeout: 30
Min-flow-timeout : 0, use controller provided values.
Max ACL Flows: Maximum Available
Max Unicast FDB Flows: Maximum Available
Max Multicast FDB Flows: Maximum Available
Buffering: Disabled
Operational Mode: Emergency
Miss Send Len: 128
...
```

```

...
Switch Support Capabilities:
  Flow Statistics           : enabled
  Table Statistics         : enabled
  Port Statistics          : enabled
  Spanning Tree            : disabled
  Reserved                 : disabled
  Reassemble IP Fragments : disabled
  Queue Statistics         : disabled
  Match IP Addr in ARP Pkts: disabled
Switch Support action:
  Output to Switch Port    : enabled
  Set Vlan ID              : enabled
  Set Priority              : enabled
  Strip dot1q Header       : enabled
  Ethernet Source Addr     : enabled
  Ethernet Destination Addr: enabled
  IP Source Address        : disabled
  IP Destination Address   : disabled
  IP ToS                   : enabled
  TCP/UDP Source Port      : disabled
  TCP/UDP Destination Port : disabled
  Output to Queue          : disabled
  Vendor                   : disabled

PortList  Status  State  Config  Current  Advertised  Supported  Peer

Number of Ports: 0
Configured Controllers:
  Openflow Controller 1:
    IP Address: 10.10.10.10
    Port: 6633
    State: Inactive
    Retry Count: 4
  Configured Controller Count 1

-----
Openflow instance 2 is currently disabled

```

OpenFlow Table Information

The following command displays the basic and emergency flow tables for all instances:

```
show openflow table
```

Command mode: All

```

Openflow Instance Id: 1

BASIC FLOW TABLE

Flow:1 Filter Based, priority:32768, hard-time-out: 0, idle-time-out: 0
  cookie: 0xfffffffffff
  QUALIFIERS: ingress-port:15
  ACTION: set_nw_tos=28, output:4
  STATS: packets=0, bytes=0

Flow:2 Filter Based, priority:65535, hard-time-out: 0, idle-time-out: 0
  cookie: 0xfffffffff22
  QUALIFIERS: ingress-port:15, vlan-id: 20, ether-type:0x806
             src-mac:00-48-47-09-55-39, dst-mac:00-0d-fb-00-00-01, arp-type: 1
             src-ip:192.168.200.20/32
  ACTION: set-vlan-id=20, set_nw_tos=32, output:2, 3, 4, 5, 6, 7, 8
  STATS: packets=0, bytes=0

NEC Vendor Specific:
Flow:1
  Filter Based, priority:50000, hard-time-out: 0, idle-time-out: 0
  cookie: 0xffff34ffffff
  QUALIFIERS: ingress-port:17, vlan-id: 100, vlan-priority: 3, ether-type:0x800
             src-mac:11-22-33-44-55-66, src-mac-mask:00-00-00-00-00-01
  dst-mac:66-55-44-33-22-11, dst-mac-mask:00-00-00-00-00-00
  ACTION: output:41
  STATS: packets=0, bytes=0

STATIC FLOWS

Flow:1 Index:1
  Filter Based, priority:65535
  QUALIFIERS: vlan-id: 100
             dst-mac:00-11-22-33-00-50
  ACTION: output:34, 33
  STATS: packets=0, bytes=0

EMERGENCY FLOW TABLE

Flow:1 Filter Based, priority:65535, hard-time-out: 0, idle-time-out: 0
  cookie: 0xff05ffffff
  QUALIFIERS: ingress-port:31, vlan-id: 14, vlan-priority: 4, ether-type:0x806
             src-mac:00-00-00-00-12-13, dst-mac:00-00-00-00-14-16, arp-type:128,
             src-ip:1.2.3.4/32
  ACTION: set-vlan-id=20, set_nw_tos=32, output:2, 3, 4, 5, 6, 7, 8

Openflow Instance Id: 2

BASIC FLOW TABLE is Empty

STATIC FLOW TABLE is Empty

EMERGENCY FLOW TABLE is Empty

```

OpenFlow table information includes detailed configuration information for each entry in the flow table.

Note: Flow qualifiers used for matching packets are not listed in the display if the qualifier is set to any.

RMON Information Commands

The following table describes the Remote Monitoring (RMON) Information commands.

Table 64. RMON Information commands

| Command Syntax and Usage |
|--|
| <code>show rmon history</code> Displays RMON History information. For details, see page 109 . Command mode: All |
| <code>show rmon alarm</code> Displays RMON Alarm information. For details, see page 110 . Command mode: All |
| <code>show rmon event</code> Displays RMON Event information. For details, see page 111 . Command mode: All |
| <code>show rmon</code> Displays all RMON information. Command mode: All |

RMON History Information

The following command displays RMON History information:

```
show rmon history
```

Command mode: All

```

RMON History group configuration:

Index IFOID                                Interval Rbnum Gbnum
-----
  1  1.3.6.1.2.1.2.2.1.1.24                30     5    5
  2  1.3.6.1.2.1.2.2.1.1.22                30     5    5
  3  1.3.6.1.2.1.2.2.1.1.20                30     5    5
  4  1.3.6.1.2.1.2.2.1.1.19                30     5    5
  5  1.3.6.1.2.1.2.2.1.1.24                1800    5    5

Index                                Owner
-----
  1  dan
  
```

The following table describes the RMON History Information parameters.

Table 65. RMON History Parameter Descriptions

| Parameter | Description |
|-----------|---|
| Index | Displays the index number that identifies each history instance. |
| IFOID | Displays the MIB Object Identifier. |
| Interval | Displays the time interval for each sampling bucket. |
| Rbnum | Displays the number of requested buckets, which is the number of data slots into which data is to be saved. |
| Gbnum | Displays the number of granted buckets that may hold sampled data. |
| Owner | Displays the owner of the history instance. |

RMON Alarm Information

The following command displays RMON Alarm information:

```
show rmon alarm
```

Command mode: All

```

RMON Alarm group configuration:

Index  Interval  Sample  Type      rLimit      fLimit      last value
-----  -----  -----  -----  -----  -----  -----
      1      1800     abs     either           0           0          7822

Index  rEvtIdx  fEvtIdx      OID
-----  -----  -----  -----
      1         0         0  1.3.6.1.2.1.2.2.1.10.1

Index      Owner
-----  -----
      1  dan
  
```

The following table describes the RMON Alarm Information parameters.

Table 66. RMON Alarm Parameter Descriptions

| Parameter | Description |
|------------|--|
| Index | Displays the index number that identifies each alarm instance. |
| Interval | Displays the time interval over which data is sampled and compared with the rising and falling thresholds. |
| Sample | Displays the method of sampling the selected variable and calculating the value to be compared against the thresholds, as follows: <ul style="list-style-type: none"> - <i>abs</i>—absolute value, the value of the selected variable is compared directly with the thresholds at the end of the sampling interval. - <i>delta</i>—delta value, the value of the selected variable at the last sample is subtracted from the current value, and the difference compared with the thresholds. |
| Type | Displays the type of alarm, as follows: <ul style="list-style-type: none"> - <i>falling</i>—alarm is triggered when a falling threshold is crossed. - <i>rising</i>—alarm is triggered when a rising threshold is crossed. - <i>either</i>—alarm is triggered when either a rising or falling threshold is crossed. |
| rLimit | Displays the rising threshold for the sampled statistic. |
| fLimit | Displays the falling threshold for the sampled statistic. |
| Last value | Displays the last sampled value. |

Table 66. RMON Alarm Parameter Descriptions (continued)

| Parameter | Description |
|-----------|---|
| rEvtIdx | Displays the rising alarm event index that is triggered when a rising threshold is crossed. |
| fEvtIdx | Displays the falling alarm event index that is triggered when a falling threshold is crossed. |
| OID | Displays the MIB Object Identifier for each alarm index. |
| Owner | Displays the owner of the alarm instance. |

RMON Event Information

The following command displays RMON Alarm information:

```
show rmon event
```

Command mode: All

```

RMON Event group configuration:

Index Type      Last Sent          Description
-----
  1 both    0D: 0H: 1M:20S   Event_1
  2 none    0D: 0H: 0M: 0S   Event_2
  3 log     0D: 0H: 0M: 0S   Event_3
  4 trap    0D: 0H: 0M: 0S   Event_4
  5 both    0D: 0H: 0M: 0S   Log and trap event for Link Down
 10 both    0D: 0H: 0M: 0S   Log and trap event for Link Up
 11 both    0D: 0H: 0M: 0S   Send log and trap for icmpInMsg
 15 both    0D: 0H: 0M: 0S   Send log and trap for icmpInEchos

Index          Owner
-----
  1 dan
    
```

The following table describes the RMON Event Information parameters.

Table 67. RMON Event Parameter Descriptions

| Parameter | Description |
|-------------|--|
| Index | Displays the index number that identifies each event instance. |
| Type | Displays the type of notification provided for this event, as follows: none, log, trap, both. |
| Last sent | Displays the time that passed since the last switch reboot, when the most recent event was triggered. This value is cleared when the switch reboots. |
| Description | Displays a text description of the event. |
| Owner | Displays the owner of the alarm instance. |

Link Status Information

The following command displays link information:

```
show interface status [<port alias or number>]
```

Command mode: All

| Alias | Port | Speed | Duplex | Flow Ctrl | | Link | Name |
|--------|------|--------|--------|-----------|----------|----------|--------|
| ----- | ---- | ----- | ----- | --TX-- | ---RX--- | ----- | ----- |
| INTA1 | 1 | 1G/10G | full | yes | yes | down | INTA1 |
| INTA2 | 2 | 1G/10G | full | yes | yes | down | INTA2 |
| INTA3 | 3 | 1G/10G | full | yes | yes | down | INTA3 |
| INTA4 | 4 | 1G/10G | full | yes | yes | down | INTA4 |
| ... | | | | | | | |
| INTA14 | 14 | 1G/10G | full | yes | yes | down | INTA14 |
| INTB1 | 15 | 1G/10G | full | yes | yes | down | INTB1 |
| INTB2 | 16 | 1G/10G | full | yes | yes | down | INTB2 |
| INTB3 | 17 | 1G/10G | full | yes | yes | down | INTB3 |
| INTB4 | 18 | 1G/10G | full | yes | yes | down | INTB4 |
| ... | | | | | | | |
| INTC14 | 42 | 1G/10G | full | yes | yes | down | INTC14 |
| EXT1 | 43 | 1G/10G | full | no | no | down | EXT1 |
| EXT2 | 44 | 1G/10G | full | no | no | down | EXT2 |
| EXT3 | 45 | 10000 | full | no | no | up | EXT3 |
| EXT4 | 46 | 1G/10G | full | no | no | down | EXT4 |
| ... | | | | | | | |
| EXT20 | 62 | 10000 | full | no | no | disabled | EXT20 |
| EXT21 | 63 | 10000 | full | no | no | disabled | EXT21 |
| EXT22 | 64 | 10000 | full | no | no | disabled | EXT22 |
| EXTM | 65 | 1000 | full | yes | yes | up | EXTM |
| MGT1 | 66 | 1000 | full | no | no | up | MGT1 |

Note: The sample screens that appear in this document might differ slightly from the screens displayed by your system. Screen content varies based on the type of BladeCenter unit that you are using and the firmware versions and options that are installed.

Use this command to display link status information about each port on the EN4093 and EN4093R, including:

- Port alias and port number
- Port speed and Duplex mode (half, full, any)
- Flow control for transmit and receive (no, yes, or both)
- Link status (up, down, or disabled)

The following display shows link status when Bridge Module connections are enabled:

| Alias | Port | Speed | Duplex | Flow Ctrl | | Link |
|-------|-------|-------|--------|-----------|--------|----------|
| ----- | ---- | ----- | ----- | --TX-- | --RX-- | ----- |
| INT1 | 1 | 10000 | full | yes | yes | down |
| INT2 | 2 | 10000 | full | yes | yes | down |
| INT3 | 3 | 10000 | full | yes | yes | down |
| INT4 | 4 | 10000 | full | yes | yes | down |
| INT5 | 5 | 10000 | full | yes | yes | down |
| INT6 | 6 | 10000 | full | yes | yes | down |
| INT7 | 7 | 10000 | full | yes | yes | down |
| INT8 | 8 | 10000 | full | yes | yes | down |
| INT9 | 9 | 10000 | full | yes | yes | down |
| INT10 | 10 | 10000 | full | yes | yes | down |
| INT11 | 11 | 10000 | full | yes | yes | down |
| INT12 | 12 | 10000 | full | yes | yes | down |
| INT13 | 13 | 10000 | full | yes | yes | down |
| INT14 | 14 | 10000 | full | yes | yes | down |
| MGT1 | 15 | 100 | full | yes | yes | up |
| MGT2 | 16 | 100 | full | yes | yes | disabled |
| KR 1 | 17 | 10000 | full | yes | yes | up |
| KR 2 | 18 | 10000 | full | yes | yes | up |
| KR 3 | 19 | 10000 | full | yes | yes | up |
| KR 4 | 20 | 10000 | full | yes | yes | up |
| EXT5 | 21 | 10000 | full | yes | yes | down |
| EXT6 | 22 | 10000 | full | yes | yes | down |
| KR 8 | 23 | 10000 | full | yes | yes | down |
| KR 7 | 24 | 10000 | full | yes | yes | down |
| KR 6 | 25 | 10000 | full | yes | yes | down |
| KR 5 | 26 | 10000 | full | yes | yes | down |
| EXT11 | 27 | any | any | yes | yes | down |
| ----- | | | | | | |
| Alias | Speed | | | | | |
| ----- | ----- | | | | | |
| BM5 | 40Gbs | | | | | |
| BM3 | 40Gbs | | | | | |

Note: The sample screens that appear in this document might differ slightly from the screens displayed by your system. Screen content varies based on the type of BladeCenter unit that you are using and the firmware versions and options that are installed.

This command displays link status information about each port on the EN4093 and EN4093R, including:

- Ethernet port alias, number, and configuration
- Link status (up, down, or disabled)
- Bridge Module (KR) port alias, port number, and configuration (if applicable)
- Bridge Module alias and speed setting

Port Information

The following command displays port information:

```
show interface trunk <port alias or number>
```

Command mode: All

| Alias | Port | Tag Trk | Type | RMON | Lrn | Fld | PVID NVLAN | DESCRIPTION | VLAN(s) |
|-------|------|---------|----------|------|-----|-----|------------|-------------|---------|
| INT1 | 1 | y | Internal | d | e | e | 1 | INT1 | 1 4095 |
| INT2 | 2 | y | Internal | d | e | e | 1 | INT2 | 1 4095 |
| INT3 | 3 | y | Internal | d | e | e | 1 | INT3 | 1 4095 |
| INT4 | 4 | y | Internal | d | e | e | 1 | INT4 | 1 4095 |
| INT5 | 5 | y | Internal | d | e | e | 1 | INT5 | 1 4095 |
| INT6 | 6 | y | Internal | d | e | e | 1 | INT6 | 1 4095 |
| INT7 | 7 | y | Internal | d | e | e | 1 | INT7 | 1 4095 |
| INT8 | 8 | y | Internal | d | e | e | 1 | INT8 | 1 4095 |
| INT9 | 9 | y | Internal | d | e | e | 1 | INT9 | 1 4095 |
| INT10 | 10 | y | Internal | d | e | e | 1 | INT10 | 1 4095 |
| INT11 | 11 | y | Internal | d | e | e | 1 | INT11 | 1 4095 |
| INT12 | 12 | y | Internal | d | e | e | 1 | INT12 | 1 4095 |
| ISL1 | 13 | n | Isl | d | e | e | 1 | ISL1 | 1 |
| ISL2 | 14 | n | Isl | d | e | e | 1 | ISL2 | 1 |
| MGT1 | 15 | y | Mgmt | d | e | e | 4095* | MGT1 | 4095 |
| MGT2 | 16 | y | Mgmt | d | e | e | 4095* | MGT2 | 4095 |
| EXT1 | 17 | n | External | d | e | e | 1 | EXT1 | 1 |
| EXT2 | 18 | n | External | d | e | e | 2 | EXT2 | 2 |
| EXT3 | 19 | n | External | d | e | e | 1 | EXT3 | 1 |
| EXT4 | 20 | n | External | d | e | e | 1 | EXT4 | 1 |
| EXT5 | 21 | n | External | d | e | e | 1 | EXT5 | 1 |
| EXT6 | 22 | n | External | d | e | e | 1 | EXT6 | 1 |
| EXT7 | 23 | n | External | d | e | e | 1 | EXT7 | 1 |
| EXT8 | 24 | n | External | d | e | e | 1 | EXT8 | 1 |
| EXT9 | 25 | n | External | d | e | e | 1 | EXT9 | 1 |
| EXT10 | 26 | n | External | d | e | e | 1 | EXT10 | 1 |
| EXT11 | 27 | n | External | d | e | e | 1 | EXT11 | 1 |

* = PVID/Native-VLAN is tagged.
= PVID is ingress tagged.
Trk = Trunk mode
NVLAN = Native-VLAN

Note: The sample screens that appear in this document might differ slightly from the screens displayed by your system. Screen content varies based on the type of BladeCenter unit that you are using and the firmware versions and options that are installed.

Port information includes:

- Port alias and number
- Whether the port uses VLAN tagging or not (y or n)
- Whether the port is internal, external or used for management
- Whether the port has Remote Monitoring (RMON) enabled
- Whether the port has FDB Learning enabled (Lrn)
- Whether the port has Port Flooding enabled (Fld)
- Port VLAN ID (PVID)

- Port description
- VLAN membership

Port Transceiver Status

The following command displays the status of the transceiver module on each external port:

```
show interface transceiver
```

Command mode: All

| Name | TX | Link | TXFlt | Volts | DegsC | TXuW | RXuW | Media | Laser | Approval |
|---------|------|-------------------------|----------------------|-------|-------|-------------|----------------------|---------|-------|----------|
| 44 SFP+ | 2 | < NO Device Installed > | | | | | | | | |
| 45 SFP+ | 3 | Ena LINK | no | 3.29 | 29.5 | 556.9 | 580.5 | SR SFP+ | 850nm | Approved |
| | | Blade Network | Part:BN-CKM-SP-SR | | | Date:110329 | S/N:AA1113AG1B1 | | | |
| 46 SFP+ | 4 | < NO Device Installed > | | | | | | | | |
| 47 SFP+ | 5 | N/A LINK | -N/A- | --- | --- | --- | --- | CU SFP | -N/A- | Approved |
| | | Blade Network | Part:BN-CKM-S-T | | | Date:080710 | S/N:BNT0828075 | | | |
| 48 SFP+ | 6 | < NO Device Installed > | | | | | | | | |
| 49 SFP+ | 7 | N/A Down | -N/A- | --- | --- | --- | --- | CU SFP | -N/A- | Approved |
| | | Blade Network | Part:BN-CKM-S-T | | | Date:080710 | S/N:BNT08280W0 | | | |
| 50 SFP+ | 8 | < NO Device Installed > | | | | | | | | |
| 51 SFP+ | 9 | N/A Down | -N/A- | --- | --- | --- | --- | CU SFP | -N/A- | Approved |
| | | Blade Network | Part:BN-CKM-S-T | | | Date:100717 | S/N:BNT10288NM | | | |
| 52 SFP+ | 10 | < NO Device Installed > | | | | | | | | |
| ... | | | | | | | | | | |
| 57 Q10G | 15.1 | < NO Device Installed > | | | | | | | | |
| 58 Q10G | 15.2 | < NO Device Installed > | | | | | | | | |
| 59 Q10G | 15.3 | < NO Device Installed > | | | | | | | | |
| 60 Q10G | 15.4 | < NO Device Installed > | | | | | | | | |
| 61 Q10G | 16.1 | N/A Down | -N/A- | --- | --- | --- | --- | 3m QDAC | -N/A- | Accepted |
| | | BLADE NETWORK | Part:BN-QS-QS-CBL-3M | | | Date:110422 | S/N:3549Y350VT14K0HN | | | |
| 62 Q10G | 16.2 | N/A Down | -N/A- | --- | --- | --- | --- | 3m QDAC | -N/A- | Accepted |
| | | BLADE NETWORK | Part:BN-QS-QS-CBL-3M | | | Date:110422 | S/N:3549Y350VT14K0HN | | | |
| 63 Q10G | 16.3 | N/A Down | -N/A- | --- | --- | --- | --- | 3m QDAC | -N/A- | Accepted |
| | | BLADE NETWORK | Part:BN-QS-QS-CBL-3M | | | Date:110422 | S/N:3549Y350VT14K0HN | | | |
| 64 Q10G | 16.4 | N/A Down | -N/A- | --- | --- | --- | --- | 3m QDAC | -N/A- | Accepted |
| | | BLADE NETWORK | Part:BN-QS-QS-CBL-3M | | | Date:110422 | S/N:3549Y350VT14K0HN | | | |

This command displays information about the transceiver module on each port, as follows:

- Port number and media type
- TX: Transmission status
- RXlos: Receive Loss of Signal indicator
- TXflt: Transmission fault indicator
- Volts: Power usage, in volts
- DegsC: Temperature, in degrees centigrade
- TXuW: Transmit power, in micro-watts
- RXuW: Receive power, in micro-watts
- Media type (LX, LR, SX, SR)
- Laser wavelength, in nano-meters
- Approval status

The optical power levels shown for transmit and receive functions for the transceiver should fall within the expected range defined in the IEEE 802-3-2008 specification for each transceiver type. For convenience, the expected range values are summarized in the following table.

Table 68. Expected Transceiver Optical Power Levels

| Transceiver Type | Tx Minimum | Tx Maximum | Rx Minimum | Rx Maximum |
|-------------------------|-------------------|-------------------|-------------------|-------------------|
| SFP SX | 112 μ W | 1000 μ W | 20 μ W | 1000 μ W |
| SFP LX | 70.8 μ W | 501 μ W | 12.6 μ W | 501 μ W |
| SFP+ SR | 186 μ W | 794 μ W | 102 μ W | 794 μ W |
| SFP+ LR | 151 μ W | 891 μ W | 27.5 μ W | 891 μ W |

Note: Power level values in the IEEE specification are shown in dBm, but have been converted to mW in this table to match the unit of measure shown in the display output.

Virtual Machines Information

The following command display information about Virtual Machines (VMs).

Table 69. Virtual Machines Information Options

| Command Syntax and Usage |
|---|
| <pre>show virt port <port alias or number></pre> <p>Displays Virtual Machine information for the selected port.</p> <p>Command mode: All</p> |
| <pre>show virt vm [-v -r]</pre> <p>Displays all Virtual Machine information.</p> <ul style="list-style-type: none">- -v displays verbose information- -r rescans the data center <p>Command mode: All</p> |

VM Information

The following command displays VM information:

```
show virt vm
```

Command mode: All

| IP Address | VMAC Address | Index | Port | VM Group (Profile) |
|---------------|-------------------|-------|------|--------------------|
| *127.31.46.50 | 00:50:56:4e:62:f5 | 4 | INT3 | |
| *127.31.46.10 | 00:50:56:4f:f2:85 | 2 | INT4 | |
| +127.31.46.51 | 00:50:56:72:ec:86 | 1 | INT3 | |
| +127.31.46.11 | 00:50:56:7c:1c:ca | 3 | INT4 | |
| 127.31.46.25 | 00:50:56:9c:00:c8 | 5 | INT4 | |
| 127.31.46.15 | 00:50:56:9c:21:2f | 0 | INT4 | |
| 127.31.46.35 | 00:50:56:9c:29:29 | 6 | INT3 | |

Number of entries: 8
* indicates VMware ESX Service Console Interface
+ indicates VMware ESX/ESXi VMKernel or Management Interface

VM information includes the following for each Virtual Machine (VM):

- IP address
- MAC address
- Index number assigned to the VM
- Internal port on which the VM was detected
- VM group that contains the VM, if applicable

VM Check Information

The following command displays VM Check information:

```
show virt vmcheck
```

Command mode: All

| |
|---|
| Action to take for spoofed VMs: Basic: Oper disable the link Advanced: Install ACL to drop traffic Maximum number of acls that can be used for mac spoofing: 50 Trusted ports by configuration: empty |
|---|

VMware Information

Use these commands to display information about Virtual Machines (VMs) and VMware hosts in the data center. These commands require the presence of a configured Virtual Center.

Table 70. VMware Information Options

| Command Syntax and Usage |
|--|
| <pre>show virt vmware hosts</pre> <p>Displays a list of VMware hosts.</p> <p>Command mode: All</p> |
| <pre>show virt vmware hello</pre> <p>Displays VMware hello settings.</p> <p>Command mode: All</p> |
| <pre>show virt vmware showhost <host UUID> <host IP address> <host name></pre> <p>Displays detailed information about a specific VMware host.</p> <p>Command mode: All</p> |
| <pre>show virt vmware showvm <VM UUID> <VM IP address> <VM name></pre> <p>Displays detailed information about a specific Virtual Machine (VM).</p> <p>Command mode: All</p> |
| <pre>show virt vmware vms</pre> <p>Displays a list of VMs.</p> <p>Command mode: All</p> |

VMware Host Information

The following command displays VM host information:

```
show virt vmware hosts
```

Command mode: All

| UUID | Name(s), IP Address |
|--------------------------------------|---------------------|
| 80a42681-d0e5-5910-a0bf-bd23bd3f7803 | 127.12.41.30 |
| 3c2e063c-153c-dd11-8b32-a78dd1909a69 | 127.12.46.10 |
| 64f1fe30-143c-dd11-84f2-a8ba2cd7ae40 | 127.12.44.50 |
| c818938e-143c-dd11-9f7a-d8defa4b83bf | 127.12.46.20 |
| fc719af0-093c-dd11-95be-b0adac1bcf86 | 127.12.46.30 |
| 009a581a-143c-dd11-be4c-c9fb65ff04ec | 127.12.46.40 |

VM host information includes the following:

- UUID associated with the VMware host.
- Name or IP address of the VMware host.

EVB Information

The following commands display Edge Virtual Bridge (EVB) Virtual Station Interface (VSI) discovery and configuration information.

Table 71. EVB Information Options

| Command Syntax and Usage |
|---|
| <pre>show virt evb vdp vm</pre> <p>Displays all active Virtual Machines (VMs).</p> <p>Command mode: All</p> |
| <pre>show virt evb profile [<1-16>]</pre> <p>Displays the current EVB profile parameters.</p> <p>Command mode: All</p> |
| <pre>show virt evb vdp tlv</pre> <p>Displays all active Virtual Station Interface (VSI) Discovery and Configuration Protocol (VDP) type-length-values (TLVs).</p> <p>Command mode: All</p> |
| <pre>show virt evb vsidb <VSI_database_number></pre> <p>Displays Virtual Station Interface database information.</p> <p>Command mode: All</p> |
| <pre>show virt evb vsitypes [mgrid <0-255> typeid <1-16777215> version <0-255>]</pre> <p>Displays the current Virtual Station Interface Type database parameters.</p> <p>Command mode: All</p> |

vNIC Information

The following commands display information about Virtual NICs (vNICs).

Table 72. vNIC Information Options

| Command Syntax and Usage |
|--|
| <pre>show vnic vnic</pre> <p>Displays information about each vNIC.</p> <p>Command mode: All</p> |
| <pre>show vnic vnicgroup</pre> <p>Displays information about each vNIC Group, including:</p> <ul style="list-style-type: none"> – Status (enabled or disabled) – VLAN assigned to the vNIC Group – Uplink Failover status (enabled or disabled) – Link status for each vNIC (up, down, or disabled) – Port link status for each port associated with the vNIC Group (up, down, or disabled) <p>Command mode: All</p> |
| <pre>show vnic information-dump</pre> <p>Displays all vNIC information.</p> <p>Command mode: All</p> |

Virtual NIC (vNIC) Information

The following command displays Virtual NIC (vNIC) information:

```
show vnic vnic
```

Command mode: All

| vNIC | vNICGroup | Vlan | MaxBandwidth | Type | MACAddress | Link |
|---|-----------|------|--------------|---------|-------------------|------|
| INT1.1 | 1 | 100 | 25 | Default | 00:00:c9:c6:d0:2a | up |
| INT1.2 | # | * | 0 | FCoE | 00:00:c9:c6:d0:2b | up |
| INT1.3 | 3 | 300 | 25 | Default | 00:00:c9:c6:d0:2c | up |
| INT1.4 | 4 | 400 | 25 | Default | 00:00:c9:c6:d0:2d | up |
| INT2.1 | 1 | 100 | 25 | Default | 00:00:c9:c6:cf:72 | up |
| INT2.2 | # | * | 0 | FCoE | 00:00:c9:c6:cf:73 | up |
| INT2.3 | 3 | 300 | 25 | Default | 00:00:c9:c6:cf:74 | up |
| INT2.4 | 4 | 400 | 25 | Default | 00:00:c9:c6:cf:75 | up |
| INT3.1 | 1 | 100 | 25 | Default | 00:00:c9:e3:09:5c | up |
| INT3.3 | 3 | 300 | 25 | Default | 00:00:c9:e3:09:5e | up |
| INT3.4 | 4 | 400 | 25 | Default | 00:00:c9:e3:09:5f | up |
| INT4.2 | # | * | 0 | FCoE | 00:00:c9:b2:55:6f | up |
| INT9.2 | # | * | 0 | FCoE | 00:00:c9:c6:cf:33 | up |
| # = Not added to any vNIC group | | | | | | |
| * = Not added to any vNIC group or no vlan set for its vNIC group | | | | | | |

vNIC information includes the following for each vNIC:

- vNIC ID
- vNIC Group that contains the vNIC
- VLAN assigned to the vNIC Group
- Maximum bandwidth allocated to the vNIC
- MAC address of the vNIC, if applicable
- Link status (up, down, or disabled)

vNIC Group Information

The following command displays vNIC Group information:

```
show vnic vnicgroup
```

Command mode: All

```
vNIC Group 1: enabled
-----
VLAN          : 100
Failover      : disabled

vNIC          Link
-----
INT1.1       up
INT2.1       up
INT3.1       up

Port          Link
-----

UplinkPort   Link
-----
EXT6         up
```

vNIC Group information includes the following for each vNIC Group:

- Status (enabled or disabled)
- VLAN assigned to the vNIC Group
- Uplink Failover status (enabled or disabled)
- Link status for each vNIC (up, down, or disabled)
- Port link status for each port associated with the vNIC Group (up, down, or disabled)

SLP Information

The following commands display information about Service Location Protocol settings:

Table 73. SLP Information Options

| Command Syntax and Usage |
|---|
| <pre>show ip slp information</pre> <p>Displays the SLP version, whether SLP is enabled or disabled and whether DA auto-discovery is enabled or disabled</p> <p>Command mode: All</p> |
| <pre>show ip slp directory-agents</pre> <p>Lists all detected DAs</p> <p>Command mode: All</p> |
| <pre>show ip slp user-agents</pre> <p>Lists all detected UAs</p> <p>Command mode: All</p> |

UFP Information

The following commands display information about Unified Fabric Port (UFP) settings.

Table 74. UFP Information Options

| Command Syntax and Usage |
|---|
| <pre>show ufp [port <port_no.>] [vport <1-4>] [network qos]</pre> <p>Displays the UFP network and QoS settings applied on all ports or on specified physical and virtual ports.</p> <ul style="list-style-type: none">– <code>network</code> filters only UFP network settings– <code>qos</code> filters only QoS network settings <p>Command mode: All</p> |
| <pre>show ufp information port [<port_no.>]</pre> <p>Displays UFP status for all physical ports or only for a specified physical port. Information includes whether the UFP is enabled on the physical port, how many virtual ports are enabled and the link stats for each virtual port. For details, see page 125.</p> <p>Command mode: All</p> |

Table 74. UFP Information Options

| Command Syntax and Usage |
|--|
| <pre>show ufp information {cdcp qos tlvstat} [port <port_no.>]</pre> <p>Displays global or port-specific UFP information on:</p> <ul style="list-style-type: none"> – cdcp displays S-Channel Discovery and Configuration Protocol (CDCP) information. CDCP allows hypervisor hosts to create on-demand S-channels with the switch. For details, see page 126. – qos displays bandwidth allocation between virtual ports. For details, see page 126. – tlvstat displays status for Type-Length-Values transmitted on UFP-enabled physical ports. For details, see page 127. <p>Command mode: All</p> |
| <pre>show ufp information qos [port <port_no.>] [vport <1-4>]</pre> <p>Displays bandwidth allocation between virtual ports for all physical ports or specified physical and virtual ports.</p> <p>Command mode: All</p> |
| <pre>show ufp information vport [port <port_no.>] [vport <1-4>]</pre> <p>Displays state, operating mode and VLAN related information for all virtual ports, for virtual ports belonging to a specified physical port or for a single virtual port. For details, see page 128.</p> <p>Command mode: All</p> |
| <pre>show ufp information getvlan <2-4094></pre> <p>Displays state, operating mode and VLAN related information for physical and virtual ports associated to a specified VLAN ID.</p> <p>Command mode: All</p> |
| <pre>show ufp information vlan [<1-4094>]</pre> <p>Displays ports associated to all configured VLANs or to a specified VLAN ID. For details, see page 128.</p> <p>Command mode: All</p> |
| <pre>show ufp {receive transmit} {cap cdcp} port <port_no.></pre> <p>Displays received/transmitted Type-Length-Values for the specified ports.</p> <ul style="list-style-type: none"> – cap displays the UFP Capability Discovery TLV – cdcp displays the UFP Channel Discovery and Configuration Protocol TLV <p>For details, see page 129.</p> <p>Command mode: All</p> |

Port Information

The following command displays UFP port information:

```
show ufp information port
```

Command mode: All

```
-----  
Alias   Port state vPorts  chan 1  chan 2  chan 3  chan 4  
-----  
INTA1  1    ena     1  disabled disabled disabled  down  
INTA2  2    ena     0  disabled disabled disabled disabled  
INTA3  3    dis     0  disabled disabled disabled disabled  
INTA4  4    dis     0  disabled disabled disabled disabled  
INTA5  5    dis     0  disabled disabled disabled disabled  
INTA6  6    dis     0  disabled disabled disabled disabled  
INTA7  7    dis     0  disabled disabled disabled disabled  
INTA8  8    dis     0  disabled disabled disabled disabled  
INTA9  9    dis     0  disabled disabled disabled disabled  
INTA10 10   dis     0  disabled disabled disabled disabled  
INTA11 11   dis     0  disabled disabled disabled disabled  
INTA12 12   dis     0  disabled disabled disabled disabled  
INTA13 13   dis     0  disabled disabled disabled disabled  
INTA14 14   dis     0  disabled disabled disabled disabled  
-----
```

Port information includes the following for each physical port:

- Port alias
- Port number
- UFP state
- Number of virtual ports enabled
- Link status on each channel (up, down or disabled)

CDCP Information

The following command displays S-Channel Discovery and Configuration Protocol information:

```
show ufp information cdcp
```

Command mode: All

```
INTA1  : Channel Request  
INTA2  : Channel Request  
INTA3  : TxSVIDs  
INTA4  : TxSVIDs  
INTA5  : Disable  
INTA6  : Disable  
INTA7  : Disable  
INTA8  : Disable  
INTA9  : Disable  
INTA10 : Disable  
INTA11 : Disable  
INTA12 : Disable  
INTA13 : Disable  
INTA14 : Disable
```

CDCP information includes the following for each physical port:

- Whether there is a channel set up
- CDCP communication status for active channels

QoS Information

The following command displays Quality of Service information:


```
show ufp information qos
```

Command mode: All

```
Global UFP QoS mode: UFP QoS BW
```

| Port | Vport | Minbw% | Maxbw% |
|------|-------|--------|--------|
| 1 | 1 | 15 | 100 |
| | 2 | 25 | 50 |
| | 3 | 25 | 100 |
| | 4 | 25 | 100 |
| 2 | 1 | 25 | 100 |
| | 2 | 25 | 100 |
| | 3 | 25 | 100 |
| | 4 | 25 | 100 |
| 3 | 1 | 25 | 100 |
| | 2 | 25 | 100 |
| | 3 | 25 | 100 |
| | 4 | 25 | 100 |
| ... | | | |

QoS information includes the following:

- Physical port number
- Virtual port number
- Minimum guaranteed bandwidth allocated
- Maximum bandwidth achievable

TLV Status Information

The following command displays Type-Length-Values information:

```
show ufp information tlvstat
```

Command mode: All

```
INTA1 : Success
INTA2 : Success
INTA3 : Disabled
INTA4 : Disabled
INTA5 : Disabled
INTA6 : Disabled
INTA7 : Disabled
INTA8 : Disabled
INTA9 : Disabled
INTA10 : Disabled
INTA11 : Disabled
INTA12 : Disabled
INTA13 : Disabled
INTA14 : Disabled
```

TLV status information includes the following:

- Physical port alias
- Type-Length-Values status

Virtual Port Information

The following command displays virtual port information:

```
show ufp information vport
```

Command mode: All

| vPort | state | evbprof | mode | svid | defvlan | deftag | VLANs |
|-------|-------|---------|--------|------|---------|--------|-------|
| 1.1 | dis | dis | tunnel | 0 | 0 | dis | |
| 1.2 | dis | dis | tunnel | 0 | 0 | dis | |
| 1.3 | dis | dis | tunnel | 0 | 0 | dis | |
| 1.4 | down | dis | trunk | 4005 | 22 | ena | 22 |
| 2.1 | dis | dis | tunnel | 0 | 0 | dis | |
| 2.2 | dis | dis | tunnel | 0 | 0 | dis | |
| 2.3 | dis | dis | tunnel | 0 | 0 | dis | |
| 2.4 | dis | dis | tunnel | 0 | 0 | dis | |
| 3.1 | dis | dis | tunnel | 0 | 0 | dis | |
| 3.2 | dis | dis | tunnel | 0 | 0 | dis | |
| 3.3 | dis | dis | tunnel | 0 | 0 | dis | |

Virtual port information includes the following for each virtual port:

- Virtual port number
- Channel status
- Operating mode (trunk, access, tunnel or FCoE)
- S-channel VLAN ID
- Default VLAN ID
- Default VLAN ID tagging enforcement
- VLANs the virtual port is associated with

VLAN Information

The following command displays VLAN information:

```
show ufp information vlan
```

Command mode: All

```
-----
VLAN
-----
  22

vPort list:
  INTA1.4

EXT Port list:

INT Port list:

UFP Port list:
  INTA1
```

VLAN information includes the following for each VLAN:

- VLAN ID
- Associated virtual ports
- Associated external ports
- Associated internal ports
- Associated UFP ports

TLV Information

The following commands display TLV information:

```
show ufp receive cap port <port_no.>
```

Command mode: All

```
UFP Capability Discovery TLV Received on port INTA2:
  tlv      : Type 127 Length 7 OUI 00-18-b1 Subtype 1
  version  : Max 1 Oper 1
  cna     : Req 1 Oper 1 Res 0x00
  switch  : Cap 1 Oper 1 Res 0x00
```

UFP Capability Discovery TLV information includes the following:

- TLV type and length
- IBM Organizationally Unique Identifier
- TLV Subtype
- Max Version and Operation Version
- UFP CNA Status which include UFP Request and UFP Operation
- UFP Switch Status which includes UFP Capable and UFP Operation

```
show ufp transmit cdcp port <port_no.>
```

Command mode: All

```
CDCP TLV Transmitted on port INTA2:
  tlv      : Type 127 Length 23 OUI 00-80-c2 Subtype 14
  local    : Role 0 SComp 1 Channel Cap 5
  SCID 1   : SVID 1
  SCID 2   : SVID 4002
  SCID 3   : SVID 4003
  SCID 4   : SVID 0
  SCID 5   : SVID 0
```

UFP Channel Discovery and Configuration Protocol TLV includes the following:

- TLV type and length
- IBM Organizationally Unique Identifier
- TLV Subtype
- Role bit
- S-Component bit
- Channel Cap
- Corresponding index/SVID pairs

Converged Enhanced Ethernet Information

[Table 75](#) describes the Converged Enhanced Ethernet (CEE) information options.

Table 75. CEE Information Options

| Command Syntax and Usage |
|---|
| <pre>show cee information</pre> <p>Displays all CEE information</p> <p>Command mode: All</p> |

DCBX Information

[Table 76](#) describes the Data Center Bridging Capability Exchange (DCBX) protocol information options.

Table 76. DCBX Information Options

| Command Syntax and Usage |
|---|
| <pre>show cee information dcbx port <port alias or number> control</pre> <p>Displays information about the DCBX Control state machine for the selected port. For details, see page 131.</p> <p>Command mode: All</p> |
| <pre>show cee information dcbx port <port alias or number> feature</pre> <p>Displays information about the DCBX Feature state machine for the selected port. For details, see page 132.</p> <p>Command mode: All</p> |
| <pre>show cee information dcbx port <port alias or number> ets</pre> <p>Displays information about the DCBX ETS state machine. For details, see page 132.</p> <p>Command mode: All</p> |
| <pre>show cee information dcbx port <port alias or number> pfc</pre> <p>Displays information about the DCBX PFC state machine. For details, see page 134.</p> <p>Command mode: All</p> |
| <pre>show cee information dcbx port <port alias or number> app_proto</pre> <p>Displays information about the DCBX Application Protocol state machine on the selected port. For details, see page 135.</p> <p>Command mode: All</p> |
| <pre>show cee information dcbx port <port alias or number></pre> <p>Displays all DCBX information.</p> <p>Command mode: All</p> |

DCBX Control Information

The following command displays DCBX control information:

```
show cee information dcbx port <port alias or number> control
```

Command mode: All

| DCBX Port Control State-machine Info | | | | | | |
|--------------------------------------|------|------------|---------|--------|-------|-------|
| ===== | | | | | | |
| Alias | Port | OperStatus | OperVer | MaxVer | SeqNo | AckNo |
| ----- | | | | | | |
| INTA1 | 1 | enabled | 0 | 0 | 0 | 0 |
| INTA2 | 2 | enabled | 0 | 0 | 4 | 2 |
| INTA3 | 3 | enabled | 0 | 0 | 0 | 0 |
| INTA4 | 4 | enabled | 0 | 0 | 1 | 1 |
| ... | | | | | | |

DCBX control information includes the following:

- Port alias and number
- DCBX status (enabled or disabled)
- Operating version negotiated with the peer device
- Maximum operating version supported by the system
- Sequence number that changes each time a DCBX parameter in one or more DCB feature TLVs changes
- Sequence number of the most recent DCB feature TLV that has been acknowledged

DCBX Feature Information

The following command displays DCBX feature information:

```
show cee information dcbx port <port alias or number> feature
```

Command mode: All

| DCBX Port Feature State-machine Info | | | | | | | | | | | | |
|--------------------------------------|------|---------|----------|------|-------|-------|-------|--------|-------|-----|----------|-------|
| ===== | | | | | | | | | | | | |
| Alias | Port | Type | AdmState | Will | Advrt | OpVer | MxVer | PrWill | SeqNo | Err | OperMode | Syncd |
| ----- | | | | | | | | | | | | |
| INTA2 | 2 | ETS | enabled | No | Yes | 0 | 0 | Yes | 1 | No | enabled | Yes |
| INTA2 | 2 | PFC | enabled | No | Yes | 0 | 0 | Yes | 1 | No | enabled | Yes |
| INTA2 | 2 | AppProt | disabled | No | Yes | 0 | 0 | Yes | 1 | No | disabled | Yes |
| ... | | | | | | | | | | | | |

The following table describes the DCBX feature information.

Table 77. DCBX Feature Information Fields

| Parameter | Description |
|-----------|---|
| Alias | Displays each port's alias. |
| Port | Displays each port's number. |
| Type | Feature type |
| AdmState | Feature status (Enabled or Disabled) |
| Will | Willing flag status (Yes/True or No/Untrue) |
| Advrt | Advertisement flag status (Yes/True or No/Untrue) |
| OpVer | Operating version negotiated with the peer device |
| MxVer | Maximum operating version supported by the system |
| PrWill | Peer's Willing flag status (Yes/True or No/Untrue) |
| SeqNo | Sequence number that changes each time a DCBX parameter in one or more DCB feature TLVs changes |
| Err | Error condition flag (Yes or No). Yes indicates that an error occurred during the exchange of configuration data with the peer. |
| OperMode | Operating status negotiated with the peer device (enabled or disabled) |
| Syncd | Synchronization status between this port and the peer (Yes or No) |

DCBX ETS Information

The following command displays DCBX ETS information:

```
show cee information dcbx port <port alias or number> ets
```

Command mode: All

```

DCBX Port Priority Group - Priority Allocation Table
=====
Alias  Port  Priority  PgIdDes  PgIdOper  PgIdPeer
-----
INTA2  2    0        PGID0    PGID0     PGID0
INTA2  2    1        PGID0    PGID0     PGID0
INTA2  2    2        PGID0    PGID0     PGID0
INTA2  2    3        PGID1    PGID1     PGID1
INTA2  2    4        PGID2    PGID2     PGID0
INTA2  2    5        PGID2    PGID2     PGID0
INTA2  2    6        PGID2    PGID2     PGID0
INTA2  2    7        PGID2    PGID2     PGID0

DCBX Port Priority Group - Bandwidth Allocation Table
=====
Alias  Port  PrioGrp  BwDes  BwOper  BwPeer
-----
INTA2  2    0        10    10     50
INTA2  2    1        50    50     50
INTA2  2    2        40    40     0

```

The following table describes the DCBX ETS information.

Table 78. DCBX Feature Information Fields

| Parameter | Description |
|--|---|
| DCBX Port Priority Group - Priority Allocation Table | |
| Alias | Displays each port's alias |
| Port | Displays each port's number |
| PgIdDes | Priority Group ID configured on this switch |
| PgIdOper | Priority Group negotiated with the peer (operating Priority Group). |
| PgIdPeer | Priority Group ID configured on the peer |
| DCBX Port Priority Group - Bandwidth Allocation Table | |
| BwDes | Bandwidth allocation configured on this switch |
| BwOper | Bandwidth allocation negotiated with the peer (operating bandwidth) |
| BwPeer | Bandwidth allocation configured on the peer |

DCBX PFC Information

The following command displays DCBX Priority Flow Control (PFC) information:

```
show cee information dcbx port <port alias or number> pfc
```

Command mode: All

| DCBX Port Priority Flow Control Table | | | | | |
|---------------------------------------|------|----------|------------|------------|------------|
| ===== | | | | | |
| Alias | Port | Priority | EnableDesr | EnableOper | EnablePeer |
| ----- | | | | | |
| INTA2 | 2 | 0 | disabled | disabled | disabled |
| INTA2 | 2 | 1 | disabled | disabled | disabled |
| INTA2 | 2 | 2 | disabled | disabled | disabled |
| INTA2 | 2 | 3 | enabled | enabled | enabled |
| INTA2 | 2 | 4 | disabled | disabled | disabled |
| INTA2 | 2 | 5 | disabled | disabled | disabled |
| INTA2 | 2 | 6 | disabled | disabled | disabled |
| INTA2 | 2 | 7 | disabled | disabled | disabled |

DCBX PFC information includes the following:

- Port alias and number
- 802.1p value
- **EnableDesr:** Status configured on this switch
- **EnableOper:** Status negotiated with the peer (operating status)
- **EnablePeer:** Status configured on the peer

DCBX Application Protocol Information

The following command displays DCBX Application Protocol information:

```
show cee information dcbx port <port alias or number> app-PROTO
```

Command mode: All

```

DCBX Application Protocol Table
=====

FCoE Priority Information
=====
Protocol ID           : 0x8906
Selector Field        : 0
Organizationally Unique ID: 0x1b21

Alias  Port  Priority  EnableDesr  EnableOper  EnablePeer
-----
INTA2  2    0        disabled   disabled   disabled
INTA2  2    1        disabled   disabled   disabled
INTA2  2    2        disabled   disabled   disabled
INTA2  2    3         enabled   disabled   enabled
INTA2  2    4        disabled   disabled   disabled
INTA2  2    5        disabled   disabled   disabled
INTA2  2    6        disabled   disabled   disabled
INTA2  2    7        disabled   disabled   disabled

FIP Snooping Priority Information
=====
Protocol ID           : 0x8914
Selector Field        : 0
Organizationally Unique ID: 0x1b21

Alias  Port  Priority  EnableDesr  EnableOper  EnablePeer
-----
INTA2  2    0        disabled   disabled   disabled
INTA2  2    1        disabled   disabled   disabled
INTA2  2    2        disabled   disabled   disabled
INTA2  2    3         enabled   disabled   disabled
INTA2  2    4        disabled   disabled   disabled
INTA2  2    5        disabled   disabled   disabled
INTA2  2    6        disabled   disabled   disabled
INTA2  2    7        disabled   disabled   disabled

```

The following table describes the DCBX Application Protocol information.

Table 79. DCBX Application Protocol Information Fields

| Parameter | Description |
|----------------------------|---|
| Protocol ID | Identifies the supported Application Protocol. |
| Selector Field | Specifies the Application Protocol type, as follows: <ul style="list-style-type: none"> - 0 = Ethernet Type - 1 = TCP socket ID |
| Organizationally Unique ID | DCBX TLV identifier |

Table 79. DCBX Application Protocol Information Fields (continued)

| Parameter | Description |
|------------------|--|
| Alias | Port alias |
| Port | Port number |
| Priority | 802.1p value |
| EnableDesr | Status configured on this switch |
| EnableOper | Status negotiated with the peer (operating status) |
| EnablePeer | Status configured on the peer |

ETS Information

[Table 80](#) describes the Enhanced Transmission Selection (ETS) information options

Table 80. ETS Information Options

| Command Syntax and Usage |
|--|
| <pre>show cee global ets information</pre> <p>Displays global ETS information.</p> <p>Command mode: All</p> |

The following command displays ETS information:

```
show cee global ets information
```

Command mode: All

| |
|--|
| <pre>Global ETS information: Number of COSq: 8 Mapping of 802.1p Priority to Priority Groups: Priority PGID COSq ----- ---- ---- 0 0 0 1 0 0 2 0 0 3 1 1 4 2 2 5 2 2 6 2 2 7 2 2 Bandwidth Allocation to Priority Groups: PGID PG% Description ----- --- - 0 10 1 50 2 40</pre> |
|--|

Enhanced Transmission Selection (ETS) information includes the following:

- Number of Class of Service queues (COSq) configured
- 802.1p mapping to Priority Groups and Class of Service queues
- Bandwidth allocated to each Priority Group

PFC Information

[Table 81](#) describes the Priority Flow Control (PFC) information options.

Table 81. PFC Information Options

| Command Syntax and Usage |
|--|
| <pre>show cee port <port alias or number> pfc information</pre> <p>Displays PFC information.</p> |

The following command displays PFC information for a port:

```
show cee port <port alias or number> pfc information
```

Command mode: All

| Global PFC Information: | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
|--|----------|-------------|-------------|-------|-------|-------|---|-----|--|---|-----|--|---|-----|--|---|-----|--|---|-----|--|---|-----|--|---|-----|--|---|-----|--|
| PFC - ON | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| <table><thead><tr><th>Priority</th><th>State</th><th>Description</th></tr><tr><td>-----</td><td>-----</td><td>-----</td></tr></thead><tbody><tr><td>0</td><td>Dis</td><td></td></tr><tr><td>1</td><td>Dis</td><td></td></tr><tr><td>2</td><td>Dis</td><td></td></tr><tr><td>3</td><td>Ena</td><td></td></tr><tr><td>4</td><td>Dis</td><td></td></tr><tr><td>5</td><td>Dis</td><td></td></tr><tr><td>6</td><td>Dis</td><td></td></tr><tr><td>7</td><td>Dis</td><td></td></tr></tbody></table> | Priority | State | Description | ----- | ----- | ----- | 0 | Dis | | 1 | Dis | | 2 | Dis | | 3 | Ena | | 4 | Dis | | 5 | Dis | | 6 | Dis | | 7 | Dis | |
| Priority | State | Description | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| ----- | ----- | ----- | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 0 | Dis | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 1 | Dis | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 2 | Dis | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 3 | Ena | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 4 | Dis | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 5 | Dis | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 6 | Dis | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 7 | Dis | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| ----- | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| State - indicates whether PFC is Enabled/Disabled on a particular priority | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |

FCoE Information

[Table 82](#) describes the Fibre Channel over Ethernet (FCoE) information options.

Table 82. FCoE Information Options

| Command Syntax and Usage |
|--|
| <pre>show fcoe information</pre> <p>Displays all current FCoE information.</p> <p>Command mode: All</p> |

FIP Snooping Information

[Table 83](#) describes the Fibre Channel Initialization Protocol (FIP) Snooping information options

Table 83. FIP Snooping Information Options

| Command Syntax and Usage |
|---|
| <pre>show fcoe fips port <port alias or number> information</pre> <p>Displays FIP Snooping (FIPS) information for the selected port, including a list of current FIPS ACLs.</p> <p>Command mode: All</p> |
| <pre>show fcoe fips fcf</pre> <p>Displays FCF information for all FCFs learned.</p> <p>Command mode: All</p> |
| <pre>show fcoe fips fcoe</pre> <p>Displays FCoE connections established on the switch.</p> <p>Command mode: All</p> |
| <pre>show fcoe fips information</pre> <p>Displays FIP Snooping information for all ports.</p> <p>Command mode: All</p> |

The following command displays FIP Snooping information for the selected port:

```
show fcoe fips port <port alias or number> information
```

Command mode: All

```
FIP Snooping on port INT2:
This port has been configured to automatically detect FCF.
It has currently detected to have 0 FCF connecting to it.

FIPS ACLs configured on this port:
SMAC 00:c0:dd:13:9b:6f, action deny.
SMAC 00:c0:dd:13:9b:70, action deny.
SMAC 00:c0:dd:13:9b:6d, action deny.
SMAC 00:c0:dd:13:9b:6e, action deny.
DMAC 00:c0:dd:13:9b:6f, ethertype 0x8914, action permit.
DMAC 00:c0:dd:13:9b:70, ethertype 0x8914, action permit.
DMAC 00:c0:dd:13:9b:6d, ethertype 0x8914, action permit.
DMAC 00:c0:dd:13:9b:6e, ethertype 0x8914, action permit.
SMAC 0e:fc:00:01:0a:00, DMAC 00:c0:dd:13:9b:6d, ethertype 0x8906, vlan 1002, action
permit.
DMAC 01:10:18:01:00:01, Ethertype 0x8914, action permit.
DMAC 01:10:18:01:00:02, Ethertype 0x8914, action permit.
Ethertype 0x8914, action deny.
Ethertype 0x8906, action deny.
SMAC 0e:fc:00:00:00:00, SMAC mask ff:ff:ff:00:00:00, action deny.
```

FIP Snooping port information includes the following:

- Fibre Channel Forwarding (FCF) mode
- Number of FCF links connected to the port
- List of FIP Snooping ACLs assigned to the port

Information Dump

The following command dumps switch information:

```
show information-dump
```

Command mode: All

Use the dump command to dump all switch information available (10K or more, depending on your configuration). This data is useful for tuning and debugging switch performance.

If you want to capture dump data to a file, set your communication software on your workstation to capture session data prior to issuing the dump commands.

Chapter 3. Statistics Commands

You can use the Statistics Commands to view switch performance statistics in both the user and administrator command modes. This chapter discusses how to use the command line interface to display switch statistics.

Table 84. Statistics Commands

| Command Syntax and Usage |
|--|
| <pre>show layer3 counters</pre> <p>Command mode: All Displays Layer 3 statistics.</p> |
| <pre>show snmp-server counters</pre> <p>Command mode: All Displays SNMP statistics. See page 234 for sample output.</p> |
| <pre>show ntp counters</pre> <p>Displays Network Time Protocol (NTP) Statistics. Command mode: All See page 238 for a sample output and a description of NTP Statistics.</p> |
| <pre>show ptp counters</pre> <p>Displays Precision Time Protocol Statistics. See page 239 for a sample output and a description of PTP Statistics. Command mode: All</p> |
| <pre>show ip slp counter</pre> <p>Displays Service Location Protocol packet counters. See page 240 for a sample output. Command mode: All</p> |
| <pre>show counters</pre> <p>Dumps all switch statistics. Use this command to gather data for tuning and debugging switch performance. If you want to capture dump data to a file, set your communication software on your workstation to capture session data prior to issuing the dump command. Command mode: All For details, see page 242.</p> |

Port Statistics

These commands display traffic statistics on a port-by-port basis. Traffic statistics include SNMP Management Information Base (MIB) objects.

Table 85. Port Statistics Commands

| Command Syntax and Usage |
|---|
| <pre>show interface port <port alias or number> dot1x counters</pre> <p>Displays IEEE 802.1X statistics for the port. See page 146 for sample output.</p> <p>Command mode: All</p> |
| <pre>show interface port <port alias or number> bridging-counters</pre> <p>Displays bridging (“dot1”) statistics for the port. See page 150 for sample output.</p> <p>Command mode: All</p> |
| <pre>show interface port <port alias or number> ethernet-counters</pre> <p>Displays Ethernet (“dot3”) statistics for the port. See page 151 for sample output.</p> <p>Command mode: All</p> |
| <pre>show interface port <port alias or number> interface-counters</pre> <p>Displays interface statistics for the port. See page 154 for sample output.</p> <p>Command mode: All</p> |
| <pre>show interface port <port alias or number> ip-counters</pre> <p>Displays IP statistics for the port. See page 157 for sample output.</p> <p>Command mode: All</p> |
| <pre>show interface port <port alias or number> link-counters</pre> <p>Displays link statistics for the port. See page 157 for sample output.</p> <p>Command mode: All</p> |
| <pre>show interface port <port alias or number> rmon-counters</pre> <p>Displays Remote Monitoring (RMON) statistics for the port. See page 158 for sample output.</p> <p>Command mode: All</p> |
| <pre>show interface port <port alias or number> ptp-counters</pre> <p>Displays Precision Time Protocol statistics for the port. See page 239 for a sample output and a description of PTP Statistics.</p> <p>Command mode: All</p> |
| <pre>show interface port <port alias or number> oam counters</pre> <p>Displays Operation, Administrative, and Maintenance (OAM) protocol statistics for the port.</p> <p>Command mode: All</p> |

Table 85. Port Statistics Commands

| Command Syntax and Usage |
|---|
| <pre>clear interface port <port alias or number> counters</pre> <p>Clears all statistics for the port.</p> <p>Command mode: All except User EXEC</p> |
| <pre>clear counters</pre> <p>Clears statistics for all ports.</p> <p>Command mode: All except User EXEC</p> |

802.1X Authenticator Statistics

Use the following command to display the 802.1X authenticator statistics of the selected port:

```
show interface port <port alias or number> dot1x counters
```

Command mode: All

| | |
|---------------------------|---------------------|
| Authenticator Statistics: | |
| eapolFramesRx | = 925 |
| eapolFramesTx | = 3201 |
| eapolStartFramesRx | = 2 |
| eapolLogoffFramesRx | = 0 |
| eapolRespIdFramesRx | = 463 |
| eapolRespFramesRx | = 460 |
| eapolReqIdFramesTx | = 1820 |
| eapolReqFramesTx | = 1381 |
| invalidEapolFramesRx | = 0 |
| eapLengthErrorFramesRx | = 0 |
| lastEapolFrameVersion | = 1 |
| lastEapolFrameSource | = 00:01:02:45:ac:51 |

Table 86. 802.1X Authenticator Statistics of a Port

| Statistics | Description |
|------------------------|--|
| eapolFramesRx | Total number of EAPOL frames received |
| eapolFramesTx | Total number of EAPOL frames transmitted |
| eapolStartFramesRx | Total number of EAPOL Start frames received |
| eapolLogoffFramesRx | Total number of EAPOL Logoff frames received |
| eapolRespIdFramesRx | Total number of EAPOL Response Identity frames received |
| eapolRespFramesRx | Total number of Response frames received |
| eapolReqIdFramesTx | Total number of Request Identity frames transmitted |
| eapolReqFramesTx | Total number of Request frames transmitted |
| invalidEapolFramesRx | Total number of invalid EAPOL frames received |
| eapLengthErrorFramesRx | Total number of EAP length error frames received |
| lastEapolFrameVersion | The protocol version number carried in the most recently received EAPOL frame. |
| lastEapolFrameSource | The source MAC address carried in the most recently received EAPOL frame. |

802.1X Authenticator Diagnostics

Use the following command to display the 802.1X authenticator diagnostics of the selected port:

```
show interface port <port alias or number> dot1x counters
```

Command mode: All

| | |
|--------------------------------------|--------|
| Authenticator Diagnostics: | |
| authEntersConnecting | = 1820 |
| authEapLogoffsWhileConnecting | = 0 |
| authEntersAuthenticating | = 463 |
| authSuccessesWhileAuthenticating | = 5 |
| authTimeoutsWhileAuthenticating | = 0 |
| authFailWhileAuthenticating | = 458 |
| authReauthsWhileAuthenticating | = 0 |
| authEapStartsWhileAuthenticating | = 0 |
| authEapLogoffWhileAuthenticating | = 0 |
| authReauthsWhileAuthenticated | = 3 |
| authEapStartsWhileAuthenticated | = 0 |
| authEapLogoffWhileAuthenticated | = 0 |
| backendResponses | = 923 |
| backendAccessChallenges | = 460 |
| backendOtherRequestsToSupplicant | = 460 |
| backendNonNakResponsesFromSupplicant | = 460 |
| backendAuthSuccesses | = 5 |
| backendAuthFails | = 458 |

Table 87. 802.1X Authenticator Diagnostics of a Port

| Statistics | Description |
|----------------------------------|--|
| authEntersConnecting | Total number of times that the state machine transitions to the CONNECTING state from any other state. |
| authEapLogoffsWhileConnecting | Total number of times that the state machine transitions from CONNECTING to DISCONNECTED as a result of receiving an EAPOL-Logoff message. |
| authEntersAuthenticating | Total number of times that the state machine transitions from CONNECTING to AUTHENTICATING, as a result of an EAP-Response/Identity message being received from the Supplicant. |
| authSuccessesWhileAuthenticating | Total number of times that the state machine transitions from AUTHENTICATING to AUTHENTICATED, as a result of the Backend Authentication state machine indicating successful authentication of the Supplicant. |
| authTimeoutsWhileAuthenticating | Total number of times that the state machine transitions from AUTHENTICATING to ABORTING, as a result of the Backend Authentication state machine indicating authentication timeout. |

Table 87. 802.1X Authenticator Diagnostics of a Port (continued)

| Statistics | Description |
|-----------------------------------|---|
| authFailWhile Authenticating | Total number of times that the state machine transitions from AUTHENTICATING to HELD, as a result of the Backend Authentication state machine indicating authentication failure. |
| authReauthsWhile Authenticating | Total number of times that the state machine transitions from AUTHENTICATING to ABORTING, as a result of a re-authentication request |
| authEapStartsWhile Authenticating | Total number of times that the state machine transitions from AUTHENTICATING to ABORTING, as a result of an EAPOL-Start message being received from the Supplicant. |
| authEapLogoffWhile Authenticating | Total number of times that the state machine transitions from AUTHENTICATING to ABORTING, as a result of an EAPOL-Logoff message being received from the Supplicant. |
| authReauthsWhile Authenticated | Total number of times that the state machine transitions from AUTHENTICATED to CONNECTING, as a result of a re-authentication request. |
| authEapStartsWhile Authenticated | Total number of times that the state machine transitions from AUTHENTICATED to CONNECTING, as a result of an EAPOL-Start message being received from the Supplicant. |
| authEapLogoffWhile Authenticated | Total number of times that the state machine transitions from AUTHENTICATED to DISCONNECTED, as a result of an EAPOL-Logoff message being received from the Supplicant. |
| backendResponses | Total number of times that the state machine sends an initial Access-Request packet to the Authentication server. Indicates that the Authenticator attempted communication with the Authentication Server. |
| backendAccessChallenges | Total number of times that the state machine receives an initial Access-Challenge packet from the Authentication server. Indicates that the Authentication Server has communication with the Authenticator. |
| backendOtherRequests ToSupplicant | Total number of times that the state machine sends an EAP-Request packet (other than an Identity, Notification, Failure, or Success message) to the Supplicant. Indicates that the Authenticator chose an EAP-method. |

Table 87. 802.1X Authenticator Diagnostics of a Port (continued)

| Statistics | Description |
|--|---|
| backendNonNak ResponsesFromSupplicant | Total number of times that the state machine receives a response from the Supplicant to an initial EAP-Request, and the response is something other than EAP-NAK. Indicates that the Supplicant can respond to the Authenticator.s chosen EAP-method. |
| backendAuthSuccesses | Total number of times that the state machine receives an Accept message from the Authentication Server. Indicates that the Supplicant has successfully authenticated to the Authentication Server. |
| backendAuthFails | Total number of times that the state machine receives a Reject message from the Authentication Server. Indicates that the Supplicant has not authenticated to the Authentication Server. |

Bridging Statistics

Use the following command to display the bridging statistics of the selected port:

```
show interface port <port alias or number> bridging-counters
```

Command mode: All

| | |
|------------------------------------|----------|
| Bridging statistics for port INT1: | |
| dot1PortInFrames: | 63242584 |
| dot1PortOutFrames: | 63277826 |
| dot1PortInDiscards: | 0 |
| dot1TpLearnedEntryDiscards: | 0 |
| dot1StpPortForwardTransitions: | 0 |

Table 88. Bridging Statistics of a Port

| Statistics | Description |
|--------------------------------|---|
| dot1PortInFrames | The number of frames that have been received by this port from its segment. A frame received on the interface corresponding to this port is only counted by this object if and only if it is for a protocol being processed by the local bridging function, including bridge management frames. |
| dot1PortOutFrames | The number of frames that have been transmitted by this port to its segment. Note that a frame transmitted on the interface corresponding to this port is only counted by this object if and only if it is for a protocol being processed by the local bridging function, including bridge management frames. |
| dot1PortInDiscards | Count of valid frames received which were discarded (that is, filtered) by the Forwarding Process. |
| dot1TpLearnedEntry Discards | The total number of Forwarding Database entries, which have been or would have been learnt, but have been discarded due to a lack of space to store them in the Forwarding Database. If this counter is increasing, it indicates that the Forwarding Database is regularly becoming full (a condition which has unpleasant performance effects on the subnetwork). If this counter has a significant value but is not presently increasing, it indicates that the problem has been occurring but is not persistent. |
| dot1StpPortForward Transitions | The number of times this port has transitioned from the Learning state to the Forwarding state. |

Ethernet Statistics

Use the following command to display the ethernet statistics of the selected port:

```
show interface port <port alias or number> ethernet-counters
```

Command mode: All

| | |
|-------------------------------------|----|
| Ethernet statistics for port INT1: | |
| dot3StatsAlignmentErrors: | 0 |
| dot3StatsFCSErrors: | 0 |
| dot3StatsSingleCollisionFrames: | 0 |
| dot3StatsMultipleCollisionFrames: | 0 |
| dot3StatsLateCollisions: | 0 |
| dot3StatsExcessiveCollisions: | 0 |
| dot3StatsInternalMacTransmitErrors: | NA |
| dot3StatsFrameTooLongs: | 0 |
| dot3StatsInternalMacReceiveErrors: | 0 |

Table 89. Ethernet Statistics for Port

| Statistics | Description |
|---------------------------|--|
| dot3StatsAlignment Errors | <p>A count of frames received on a particular interface that are not an integral number of octets in length and do not pass the Frame Check Sequence (FCS) check.</p> <p>The count represented by an instance of this object is incremented when the <code>alignmentError</code> status is returned by the MAC service to the Logical Link Control (LLC) (or other MAC user). Received frames for which multiple error conditions obtained are, according to the conventions of IEEE 802.3 Layer Management, counted exclusively according to the error status presented to the LLC.</p> |
| dot3StatsFCSErrors | <p>A count of frames received on a particular interface that are an integral number of octets in length but do not pass the Frame Check Sequence (FCS) check.</p> <p>The count represented by an instance of this object is incremented when the <code>frameCheckError</code> status is returned by the MAC service to the LLC (or other MAC user). Received frames for which multiple error conditions obtained are, according to the conventions of IEEE 802.3 Layer Management, counted exclusively according to the error status presented to the LLC.</p> |

Table 89. Ethernet Statistics for Port (continued)

| Statistics | Description |
|------------------------------------|---|
| dot3StatsSingleCollisionFrames | <p>A count of successfully transmitted frames on a particular interface for which transmission is inhibited by exactly one collision.</p> <p>A frame that is counted by an instance of this object is also counted by the corresponding instance of either the <code>ifOutUcastPkts</code>, <code>ifOutMulticastPkts</code>, or <code>ifOutBroadcastPkts</code>, and is not counted by the corresponding instance of the <code>dot3StatsMultipleCollisionFrame</code> object.</p> |
| dot3StatsMultipleCollisionFrames | <p>A count of successfully transmitted frames on a particular interface for which transmission is inhibited by more than one collision.</p> <p>A frame that is counted by an instance of this object is also counted by the corresponding instance of either the <code>ifOutUcastPkts</code>, <code>ifOutMulticastPkts</code>, or <code>ifOutBroadcastPkts</code>, and is not counted by the corresponding instance of the <code>dot3StatsSingleCollisionFrames</code> object.</p> |
| dot3StatsLateCollisions | <p>The number of times that a collision is detected on a particular interface later than 512 bit-times into the transmission of a packet.</p> <p>Five hundred and twelve bit-times corresponds to 51.2 microseconds on a 10 Mbit/s system. A (late) collision included in a count represented by an instance of this object is also considered as a (generic) collision for purposes of other collision-related statistics.</p> |
| dot3StatsExcessiveCollisions | <p>A count of frames for which transmission on a particular interface fails due to excessive collisions.</p> |
| dot3StatsInternalMacTransmitErrors | <p>A count of frames for which transmission on a particular interface fails due to an internal MAC sub layer transmit error. A frame is only counted by an instance of this object if it is not counted by the corresponding instance of either the <code>dot3StatsLateCollisions</code> object, the <code>dot3StatsExcessiveCollisions</code> object, or the <code>dot3StatsCarrierSenseErrors</code> object.</p> <p>The precise meaning of the count represented by an instance of this object is implementation-specific. In particular, an instance of this object may represent a count of transmission errors on a particular interface that are not otherwise counted.</p> |

Table 89. Ethernet Statistics for Port (continued)

| Statistics | Description |
|------------------------------------|---|
| dot3StatsFrameTooLongs | <p>A count of frames received on a particular interface that exceed the maximum permitted frame size.</p> <p>The count represented by an instance of this object is incremented when the <code>frameTooLong</code> status is returned by the MAC service to the LLC (or other MAC user). Received frames for which multiple error conditions obtained are, according to the conventions of IEEE 802.3 Layer Management, counted exclusively according to the error status presented to the LLC.</p> |
| dot3StatsInternalMac ReceiveErrors | <p>A count of frames for which reception on a particular interface fails due to an internal MAC sub layer receive error. A frame is only counted by an instance of this object if it is not counted by the corresponding instance of either the <code>dot3StatsFrameTooLongs</code> object, the <code>dot3StatsAlignmentErrors</code> object, or the <code>dot3StatsFCSErrors</code> object.</p> <p>The precise meaning of the count represented by an instance of this object is implementation-specific. In particular, an instance of this object may represent a count of received errors on a particular interface that are not otherwise counted.</p> |

Interface Statistics

Use the following command to display the interface statistics of the selected port:

```
show interface port <port alias or number> interface-counters
```

Command mode: All

| Interface statistics for port EXT1: | | | |
|-------------------------------------|-----------------|-------------------------|----|
| | ifHCIn Counters | ifHCOOut Counters | |
| Octets: | 0 | 648329 | |
| UcastPkts: | 0 | 0 | |
| BroadcastPkts: | 0 | 271 | |
| MulticastPkts: | 0 | 7654 | |
| FlowCtrlPkts: | 0 | 0 | |
| PriFlowCtrlPkts: | 0 | 0 | |
| Discards: | 0 | 11 | |
| Errors: | 0 | 0 | |
| Ingress Discard reasons: | | Egress Discard reasons: | |
| VLAN Discards: | 0 | HOL-blocking Discards: | 0 |
| Filter Discards: | 0 | MMU Discards: | 0 |
| Policy Discards: | 0 | Cell Error Discards: | 0 |
| Non-Forwarding State: | 0 | MMU Aging Discards: | 0 |
| IBP/CBP Discards: | 0 | Other Discards: | 11 |

Table 90. Interface Statistics for Port

| Statistics | Description |
|---------------------|---|
| ifInOctets | The total number of octets received on the interface, including framing characters. |
| ifInUcastPkts | The number of packets, delivered by this sub-layer to a higher sub-layer, which were not addressed to a multicast or broadcast address at this sub-layer. |
| ifInBroadcastPkts | The number of packets, delivered by this sub-layer to a higher sub-layer, which were addressed to a broadcast address at this sub-layer. |
| ifInMulticastPkts | The total number of packets that higher-level protocols requested to be transmitted, and which were addressed to a multicast address at this sub-layer, including those that were discarded or not sent. For a MAC layer protocol, this includes both Group and Functional addresses. |
| ifInFlowControlPkts | The total number of flow control <code>pause</code> packets received on the interface. |
| ifInDiscards | The number of inbound packets which were chosen to be discarded even though no errors had been detected to prevent their being delivered to a higher-layer protocol. One possible reason for discarding such a packet could be to free up buffer space. |

Table 90. Interface Statistics for Port (continued)

| Statistics | Description |
|----------------------|--|
| ifInErrors | For packet-oriented interfaces, the number of inbound packets that contained errors preventing them from being delivered to a higher-layer protocol. For character-oriented or fixed-length interfaces, the number of inbound transmission units that contained errors preventing them from being deliverable to a higher-layer protocol. |
| ifOutOctets | The total number of octets transmitted out of the interface, including framing characters. |
| ifOutUcastPkts | The total number of packets that higher-level protocols requested to be transmitted, and which were not addressed to a multicast or broadcast address at this sub-layer, including those that were discarded or not sent. |
| ifOutBroadcastPkts | The total number of packets that higher-level protocols requested to be transmitted, and which were addressed to a broadcast address at this sub-layer, including those that were discarded or not sent. This object is a 64-bit version of <code>ifOutBroadcastPkts</code> . |
| ifOutMulticastPkts | The total number of packets that higher-level protocols requested to be transmitted, and which were addressed to a multicast address at this sub-layer, including those that were discarded or not sent. For a MAC layer protocol, this includes both Group and Functional addresses. This object is a 64-bit version of <code>ifOutMulticastPkts</code> . |
| ifOutFlowControlPkts | The total number of flow control <code>pause</code> packets transmitted out of the interface. |
| ifOutDiscards | The number of outbound packets which were chosen to be discarded even though no errors had been detected to prevent their being transmitted. One possible reason for discarding such a packet could be to free up buffer space. |
| ifOutErrors | For packet-oriented interfaces, the number of outbound packets that could not be transmitted because of errors. For character-oriented or fixed-length interfaces, the number of outbound transmission units that could not be transmitted because of errors. |
| VLAN Discards | Discarded because the packet was tagged with a VLAN to which this port is not a member. |
| Filter Discards | Dropped by the Content Aware Engine (user-configured filter). |
| Policy Discards | Dropped due to policy setting. For example, due to a user-configured static entry. |

Table 90. Interface Statistics for Port (continued)

| Statistics | Description |
|-----------------------|---|
| Non-Forwarding State | Discarded because the ingress port is not in the forwarding state. |
| IBP/CBP Discards | Discarded because of Ingress Back Pressure (flow control), or because the Common Buffer Pool is full (for example, insufficient packet buffering). |
| HOL-blocking Discards | Discarded because of the Head Of Line (HOL) blocking mechanism. Low-priority packets are placed in a separate queue and can be discarded while applications or the TCP protocol determine whether a retransmission is necessary. HOL blocking forces transmission to stop until the overloaded egress port buffer can receive data again. |
| MMU Discards | Discarded because of the Memory Management Unit. |
| Cell Error Discards | |
| MMU Aging Discards | |
| Other Discards | Discarded packets not included in any category. |
| Empty Egress Portmap | Dropped due to an egress port bitmap of zero condition (no ports in the egress mask). This counter increments whenever the switching decision found that there was no port to send out. |

Interface Protocol Statistics

Use the following command to display the interface protocol statistics of the selected port:

```
show interface port <port alias or number> ip-counters
```

Command mode: All

| | |
|----------------------------------|-----|
| GEA IP statistics for port INT1: | |
| ipInReceives | : 0 |
| ipInHeaderError: | 0 |
| ipInDiscards | : 0 |

Table 91. Interface Protocol Statistics

| Statistics | Description |
|------------------|--|
| ipInReceives | The total number of input datagrams received from interfaces, including those received in error. |
| ipInHeaderErrors | The number of input datagrams discarded because the IP address in their IP header's destination field was not a valid address to be received at this entity (the switch). |
| ipInDiscards | The number of input IP datagrams for which no problems were encountered to prevent their continued processing, but which were discarded (for example, for lack of buffer space). Note that this counter does not include any datagrams discarded while awaiting re-assembly. |

Link Statistics

Use the following command to display the link statistics of the selected port:

```
show interface port <port alias or number> link-counters
```

Command mode: All

| | |
|--------------------------------|---|
| Link statistics for port INT1: | |
| linkStateChange: | 1 |

Table 92. Link Statistics

| Statistics | Description |
|-----------------|---|
| linkStateChange | The total number of link state changes. |

RMON Statistics

Use the following command to display the Remote Monitoring (RMON) statistics of the selected port:

```
show interface port <port alias or number> rmon-counters
```

Command mode: All.

| | |
|---------------------------------|----|
| RMON statistics for port EXT2: | |
| etherStatsDropEvents: | NA |
| etherStatsOctets: | 0 |
| etherStatsPkts: | 0 |
| etherStatsBroadcastPkts: | 0 |
| etherStatsMulticastPkts: | 0 |
| etherStatsCRCAlignErrors: | 0 |
| etherStatsUndersizePkts: | 0 |
| etherStatsOversizePkts: | 0 |
| etherStatsFragments: | NA |
| etherStatsJabbers: | 0 |
| etherStatsCollisions: | 0 |
| etherStatsPkts64Octets: | 0 |
| etherStatsPkts65to127Octets: | 0 |
| etherStatsPkts128to255Octets: | 0 |
| etherStatsPkts256to511Octets: | 0 |
| etherStatsPkts512to1023Octets: | 0 |
| etherStatsPkts1024to1518Octets: | 0 |

Table 93. RMON Statistics of a Port

| Statistics | Description |
|--------------------------|--|
| etherStatsDropEvents | The total number of packets received that were dropped because of system resource constraints. |
| etherStatsOctets | The total number of octets of data (including those in bad packets) received on the network (excluding framing bits but including FCS octets). |
| etherStatsPkts | The total number of packets (including bad packets, broadcast packets, and multicast packets) received. |
| etherStatsBroadcastPkts | The total number of good packets received that were directed to the broadcast address. |
| etherStatsMulticastPkts | The total number of good packets received that were directed to a multicast address. |
| etherStatsCRCAlignErrors | The total number of packets received that had a length (excluding framing bits, but including FCS octets) of between 64 and 1518 octets, inclusive, but had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error). |

Table 93. RMON Statistics of a Port (continued)

| Statistics | Description |
|---------------------------------|--|
| etherStatsUndersizePkts | The total number of packets received that were less than 64 octets long (excluding framing bits but including FCS octets) and were otherwise well formed. |
| etherStatsOversizePkts | The total number of packets received that were longer than 1518 octets (excluding framing bits but including FCS octets) and were otherwise well formed. |
| etherStatsFragments | The total number of packets received that were less than 64 octets in length (excluding framing bits but including FCS octets) and had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error). |
| etherStatsJabbers | The total number of packets received that were longer than 1518 octets (excluding framing bits, but including FCS octets), and had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error). Jabber is defined as the condition where any packet exceeds 20 ms. The allowed range to detect jabber is between 20 ms and 150 ms. |
| etherStatsCollisions | The best estimate of the total number of collisions on this Ethernet segment. |
| etherStatsPkts64Octets | The total number of packets (including bad packets) received that were less than or equal to 64 octets in length (excluding framing bits but including FCS octets). |
| etherStatsPkts65to127 Octets | The total number of packets (including bad packets) received that were greater than 64 octets in length (excluding framing bits but including FCS octets). |
| etherStatsPkts128to255 Octets | The total number of packets (including bad packets) received that were greater than 127 octets in length (excluding framing bits but including FCS octets). |
| etherStatsPkts256to511 Octets | The total number of packets (including bad packets) received that were greater than 255 octets in length (excluding framing bits but including FCS octets). |
| etherStatsPkts512to1023 Octets | The total number of packets (including bad packets) received that were greater than 511 octets in length (excluding framing bits but including FCS octets). |
| etherStatsPkts1024to1518 Octets | The total number of packets (including bad packets) received that were greater than 1023 octets in length (excluding framing bits but including FCS octets). |

QoS Queue Rate-Based Statistics

Use the following command to display the rate-based QoS queue statistics of the selected port:

```
show interface port <port alias or number> egress-queue-rate
```

Command mode: All.

```

QoS Rate for port INTA14:
QoS Queue 0:
  Tx Packets:                5
  Dropped Packets:          0
  Tx Bytes:                  363
  Dropped Bytes:            0
QoS Queue 1:
  Tx Packets:                0
  Dropped Packets:          0
  Tx Bytes:                  0
  Dropped Bytes:            0
QoS Queue 2:
  Tx Packets:                0
  Dropped Packets:          0
  Tx Bytes:                  0
  Dropped Bytes:            0
QoS Queue 3:
  Tx Packets:                0
  Dropped Packets:          0
  Tx Bytes:                  0
  Dropped Bytes:            0
QoS Queue 4:
  Tx Packets:                0
  Dropped Packets:          0
  Tx Bytes:                  0
  Dropped Bytes:            0
QoS Queue 5:
  Tx Packets:                0
  Dropped Packets:          0
  Tx Bytes:                  0
  Dropped Bytes:            0
QoS Queue 6:
  Tx Packets:                0
  Dropped Packets:          0
  Tx Bytes:                  0
  Dropped Bytes:            0
QoS Queue 7:
  Tx Packets:                0
  Dropped Packets:          0
  Tx Bytes:                  0
  Dropped Bytes:            0

```

Table 94. QoS Queue Rate-Based Statistics of a Port

| Statistics | Description |
|-----------------|---|
| Tx Packets | Number of successfully transmitted packets per second for the QoS queue |
| Dropped Packets | Number of dropped packets per second for the QoS queue |

Table 94. QoS Queue Rate-Based Statistics of a Port (continued)

| Statistics | Description |
|---------------|---|
| Tx Bytes | Number of successfully transmitted bytes per second for the QoS queue |
| Dropped Bytes | Number of dropped bytes per second for the QoS queue |

Trunk Group Statistics

Table 95. Trunk Group Statistics Commands

| Command Syntax and Usage |
|--|
| <pre>show interface portchannel <trunk group number> interface counters</pre> <p>Displays interface statistics for the trunk group.</p> <p>Command mode: All</p> |
| <pre>clear interface portchannel <trunk group number> counters</pre> <p>Clears all the statistics on the specified trunk group.</p> <p>Command mode: All except User EXEC</p> |

Layer 2 Statistics

Table 96. Layer 2 Statistics Commands

| Command Syntax and Usage |
|--|
| <pre>show interface port <port alias or number> lacp counters</pre> <p>Displays Link Aggregation Control Protocol (LACP) statistics. See page 164 for sample output.</p> <p>Command mode: All</p> |
| <pre>clear interface port <port alias or number> lacp counters</pre> <p>Clears Link Aggregation Control Protocol (LACP) statistics.</p> <p>Command mode: All except User EXEC</p> |
| <pre>show hotlinks counters</pre> <p>Displays Hot Links statistics. See page 165 for sample output.</p> <p>Command mode: All except User EXEC</p> |
| <pre>clear hotlinks</pre> <p>Clears all Hot Links statistics.</p> <p>Command mode: All except User EXEC</p> |
| <pre>show interface port <port alias or number> lldp counters</pre> <p>Displays LLDP statistics. See page 166 for sample output.</p> <p>Command mode: All except User EXEC</p> |
| <pre>show oam counters</pre> <p>Displays OAM statistics. See page 167 for sample output.</p> <p>Command mode: All except User EXEC</p> |

LACP Statistics

Use the following command to display Link Aggregation Control Protocol (LACP) statistics:

```
show interface port <port alias or number> lacp counters
```

Command mode: All

```
Port EXT1:
-----
Valid LACPDUs received:      - 870
Valid Marker PDUs received: - 0
Valid Marker Rsp PDUs received: - 0
Unknown version/TLV type:   - 0
Illegal subtype received:   - 0
LACPDUs transmitted:       - 6031
Marker PDUs transmitted:    - 0
Marker Rsp PDUs transmitted: - 0
```

Link Aggregation Control Protocol (LACP) statistics are described in the following table:

Table 97. LACP Statistics

| Statistic | Description |
|--------------------------------|--|
| Valid LACPDUs received | Total number of valid LACP data units received. |
| Valid Marker PDUs received | Total number of valid LACP marker data units received. |
| Valid Marker Rsp PDUs received | Total number of valid LACP marker response data units received. |
| Unknown version/TLV type | Total number of LACP data units with an unknown version or type, length, and value (TLV) received. |
| Illegal subtype received | Total number of LACP data units with an illegal subtype received. |
| LACPDUs transmitted | Total number of LACP data units transmitted. |
| Marker PDUs transmitted | Total number of LACP marker data units transmitted. |
| Marker Rsp PDUs transmitted | Total number of LACP marker response data units transmitted. |

Hotlinks Statistics

Use the following command to display Hot Links statistics:

```
show hotlinks counters
```

Command mode: All

```
Hot Links Trigger Stats:

Trigger 1 statistics:
  Trigger Name: Trigger 1
  Master active:           0
  Backup active:          0
  FDB update:             0  failed: 0
```

The following table describes the Hotlinks statistics:

Table 98. Hotlinks Statistics

| Statistic | Description |
|---------------|--|
| Master active | Total number of times the Master interface transitioned to the Active state. |
| Backup active | Total number of times the Backup interface transitioned to the Active state. |
| FDB update | Total number of FDB update requests sent. |
| failed | Total number of FDB update requests that failed. |

LLDP Port Statistics

Use the following command to display LLDP statistics:

```
show interface port <port alias or number> lldp counters
```

Command mode: All

| | |
|---------------------------|-----|
| LLDP Port INT1 Statistics | |
| ----- | |
| Frames Transmitted | : 0 |
| Frames Received | : 0 |
| Frames Received in Errors | : 0 |
| Frames Discarded | : 0 |
| TLVs Unrecognized | : 0 |
| Neighbors Aged Out | : 0 |
| ... | |

The following table describes the LLDP port statistics:

Table 99. LLDP Port Statistics

| Statistic | Description |
|---------------------------|---|
| Frames Transmitted | Total number of LLDP frames transmitted. |
| Frames Received | Total number of LLDP frames received. |
| Frames Received in Errors | Total number of LLDP frames that had errors. |
| Frames Discarded | Total number of LLDP frames discarded. |
| TLVs Unrecognized | Total number of unrecognized TLV (Type, Length, and Value) fields received. |
| Neighbors Aged Out | Total number of neighbor devices that have had their LLDP information aged out. |

OAM Statistics

Use the following command to display OAM statistics:

```
show oam counters
```

Command mode: All

```
OAM statistics on port INT1
-----
Information OAMPDU Tx :      0
Information OAMPDU Rx :      0
Unsupported OAMPDU Tx :      0
Unsupported OAMPDU Rx :      0

Local faults
-----
    0 Link fault records
    0 Critical events
    0 Dying gasps

Remote faults
-----
    0 Link fault records
    0 Critical events
    0 Dying gasps
```

OAM statistics include the following:

- Total number of OAM Protocol Data Units (OAMPDU) transmitted and received.
- Total number of unsupported OAM Protocol Data Units (OAMPDU) transmitted and received.
- Local faults detected
- Remote faults detected

vLAG Statistics

The following table describes the vLAG statistics commands:

Table 100. vLAG Statistics Options

| Command Syntax and Usage |
|--|
| <pre>show vlag isl-statistics</pre> <p>Displays vLAG ISL statistics for the selected port. See page 168 for sample output.</p> |
| <pre>clear vlag statistics</pre> <p>Clears all vLAG statistics.</p> |
| <pre>show vlag statistics</pre> <p>Displays all vLAG statistics. See page 168 for sample output.</p> |

vLAG ISL Statistics

Use the following command to display vLAG statistics:

```
show vlag isl-statistics
```

Command mode: All

| | In Counter | Out Counter |
|----------|------------|-------------|
| Octets: | 2755820 | 2288 |
| Packets: | 21044 | 26 |

ISL statistics include the total number of octets received/transmitted, and the total number of packets received/transmitted over the Inter-Switch Link (ISL).

vLAG Statistics

Use the following command to display vLAG statistics:

```
show vlag statistics
```

Command mode: All

| | | | |
|------------------------------|---|------------------------|---|
| vLAG PDU sent: | | | |
| Role Election: | 0 | System Info: | 0 |
| Peer Instance Enable: | 0 | Peer Instance Disable: | 0 |
| FDB Dynamic Add: | 0 | FDB Dynamic Del: | 0 |
| FDB Inactive Add: | 0 | FDB Inactive Del: | 0 |
| Health Check: | 0 | ISL Hello: | 0 |
| Other: | 0 | Unknown: | 0 |
| vLAG PDU received: | | | |
| Role Election: | 0 | System Info: | 0 |
| Peer Instance Enable: | 0 | Peer Instance Disable: | 0 |
| FDB Dynamic Add: | 0 | FDB Dynamic Del: | 0 |
| FDB Inactive Add: | 0 | FDB Inactive Del: | 0 |
| Health Check: | 0 | ISL Hello: | 0 |
| Other: | 0 | Unknown: | 0 |
| vLAG IGMP packets forwarded: | | | |
| IGMP Reports: | 0 | | |
| IGMP Leaves: | 0 | | |

The following table describes the vLAG statistics:

Table 101. vLAG Statistics

| Statistic | Description |
|-----------------------|--|
| Role Election | Total number of vLAG PDUs sent for role elections. |
| System Info | Total number of vLAG PDUs sent for getting system information. |
| Peer Instance Enable | Total number of vLAG PDUs sent for enabling peer instance. |
| Peer Instance Disable | Total number of vLAG PDUs sent for disabling peer instance. |

Table 101. vLAG Statistics (continued)

| Statistic | Description |
|------------------|--|
| FDB Dynamic Add | Total number of vLAG PDUs sent for addition of FDB dynamic entry. |
| FDB Dynamic Del | Total number of vLAG PDUs sent for deletion of FDB dynamic entry. |
| FDB Inactive Add | Total number of vLAG PDUs sent for addition of FDB inactive entry. |
| FDB Inactive Del | Total number of vLAG PDUs sent for deletion of FDB inactive entry. |
| Health Check | Total number of vLAG PDUs sent for health checks. |
| ISL Hello | Total number of vLAG PDUs sent for ISL hello. |
| Other | Total number of vLAG PDUs sent for other reasons. |
| Unknown | Total number of vLAG PDUs sent for unknown operations. |
| | vLAG IGMP packets forwarded |
| IGMP Reports | Total number of IGMP Reports forwarded over vLAG. |
| IGMP Leaves | Total number of IGMP Leave messages forwarded over vLAG. |

Layer 3 Statistics

Table 102. Layer 3 Statistics Commands

| Command Syntax and Usage |
|---|
| <pre>show ip counters</pre> <p>Displays IP statistics. See page 173 for sample output.</p> <p>Command mode: All</p> |
| <pre>clear ip counters</pre> <p>Clears IPv4 statistics. Use this command with caution as it deletes all the IPv4 statistics.</p> <p>Command mode: All except User EXEC</p> |
| <pre>show ip route counters</pre> <p>Displays route statistics. See page 181 for sample output.</p> <p>Command mode: All</p> |
| <pre>show ip arp counters</pre> <p>Displays Address Resolution Protocol (ARP) statistics. See page 182 for sample output.</p> <p>Command mode: All</p> |
| <pre>show ip dns counters</pre> <p>Displays Domain Name System (DNS) statistics. See page 183 for sample output.</p> <p>Command mode: All</p> |
| <pre>show ip icmp counters</pre> <p>Displays ICMP statistics. See page 184 for sample output.</p> <p>Command mode: All</p> |
| <pre>show ip tcp counters</pre> <p>Displays TCP statistics. See page 186 for sample output.</p> <p>Command mode: All</p> |
| <pre>show ip udp counters</pre> <p>Displays UDP statistics. See page 187 for sample output.</p> <p>Command mode: All</p> |
| <pre>show ip ospf counters</pre> <p>Displays OSPF statistics. See page 194 for sample output.</p> <p>Command mode: All</p> |
| <pre>show ipv6 ospf counters</pre> <p>Displays OSPFv3 statistics. See page 198 for sample output.</p> <p>Command mode: All</p> |

Table 102. Layer 3 Statistics Commands (continued)

| Command Syntax and Usage | |
|---|--|
| show ip igmp counters | Displays IGMP statistics. See page 188 for sample output. Command mode: All |
| show ip igmp vlan <vlan number> counter | Displays IGMP statistics for a specific VLAN. See page 188 for sample output. Command mode: All |
| show layer3 igmp-groups | Displays the total number of IGMP groups that are registered on the switch. Command mode: All |
| show layer3 ipmc-groups | Displays the total number of current IP multicast groups that are registered on the switch. Command mode: All |
| show ipv6 mld counters | Displays Multicast Listener Discovery (MLD) statistics. Command mode: All |
| show ip vrrp counters | When virtual routers are configured, you can display the protocol statistics for VRRP. See page 201 for sample output. Command mode: All |
| show ip pim counters | Displays PIM statistics for all configured PIM interfaces. See page 202 for sample output. Command mode: All |
| show ip pim mroute count | Displays statistics of various multicast entry types. Command mode: All |
| show ip pim interface <interface number> counters | Displays PIM statistics for the selected interface. Command mode: All |
| show ip rip counters | Displays Routing Information Protocol (RIP) statistics. See page 203 for sample output. Command mode: All |
| clear ip arp counters | Clears Address Resolution Protocol (ARP) statistics. Command mode: All except User EXEC |

Table 102. Layer 3 Statistics Commands (continued)

| Command Syntax and Usage |
|--|
| <pre>clear ip dns counters</pre> <p>Clears Domain Name System (DNS) statistics. Command mode: All except User EXEC</p> |
| <pre>clear ip icmp counters</pre> <p>Clears Internet Control Message Protocol (ICMP) statistics. Command mode: All except User EXEC</p> |
| <pre>clear ip tcp counters</pre> <p>Clears Transmission Control Protocol (TCP) statistics. Command mode: All except User EXEC</p> |
| <pre>clear ip udp counters</pre> <p>Clears User Datagram Protocol (UDP) statistics. Command mode: All except User EXEC</p> |
| <pre>clear ip igmp [<VLAN number>] counters</pre> <p>Clears IGMP statistics for all VLANs or for a specific VLAN. Command mode: All</p> |
| <pre>clear ip vrrp counters</pre> <p>Clears VRRP statistics. Command mode: All</p> |
| <pre>clear ip counters</pre> <p>Clears IP statistics. Use this command with caution as it will delete all the IP statistics. Command mode: All</p> |
| <pre>clear ip rip counters</pre> <p>Clears Routing Information Protocol (RIP) statistics. Command mode: All except User EXEC</p> |
| <pre>clear ip ospf counters</pre> <p>Clears Open Shortest Path First (OSPF) statistics. Command mode: All except User EXEC</p> |
| <pre>show layer3 counters</pre> <p>Dumps all Layer 3 statistics. Use this command to gather data for tuning and debugging switch performance. If you want to capture dump data to a file, set your communication software on your workstation to capture session data prior to issuing the dump command. Command mode: All</p> |

IPv4 Statistics

The following command displays IPv4 statistics:

```
show ip counters
```

Command mode: All

Use the following command to clear IPv4 statistics:

```
clear ip counters
```

| | | | |
|--------------------|---------|------------------|---------|
| IP statistics: | | | |
| ipInReceives: | 3115873 | ipInHdrErrors: | 1 |
| ipInAddrErrors: | 35447 | ipForwDatagrams: | 0 |
| ipInUnknownProtos: | 500504 | ipInDiscards: | 0 |
| ipInDelivers: | 2334166 | ipOutRequests: | 1010542 |
| ipOutDiscards: | 4 | ipOutNoRoutes: | 4 |
| ipReasmReqds: | 0 | ipReasmOKs: | 0 |
| ipReasmFails: | 0 | ipFragOKs: | 0 |
| ipFragFails: | 0 | ipFragCreates: | 0 |
| ipRoutingDiscards: | 0 | ipDefaultTTL: | 255 |
| ipReasmTimeout: | 5 | | |

Table 103. IP Statistics

| Statistic | Description |
|-----------------|---|
| ipInReceives | The total number of input datagrams received from interfaces, including those received in error. |
| ipInHdrErrors | The number of input datagrams discarded due to errors in their IP headers, including bad checksums, version number mismatch, other format errors, time-to-live exceeded, errors discovered in processing their IP options, and so forth. |
| ipInAddrErrors | The number of input datagrams discarded because the IP address in their IP header's destination field was not a valid address to be received at this entity (the switch). This count includes invalid addresses (for example, 0.0.0.0) and addresses of unsupported Classes (for example, Class E). For entities which are not IP Gateways and therefore do not forward datagrams, this counter includes datagrams discarded because the destination address was not a local address. |
| ipForwDatagrams | The number of input datagrams for which this entity (the switch) was not their final IP destination, as a result of which an attempt was made to find a route to forward them to that final destination. In entities which do not act as IP Gateways, this counter will include only those packets, which were Source-Routed via this entity (the switch), and the Source-Route option processing was successful. |

Table 103. IP Statistics (continued)

| Statistic | Description |
|-------------------|--|
| ipInUnknownProtos | The number of locally addressed datagrams received successfully but discarded because of an unknown or unsupported protocol. |
| ipInDiscards | The number of input IP datagrams for which no problems were encountered to prevent their continued processing, but which were discarded (for example, for lack of buffer space). Note that this counter does not include any datagrams discarded while awaiting re-assembly. |
| ipInDelivers | The total number of input datagrams successfully delivered to IP user-protocols (including ICMP). |
| ipOutRequests | The total number of IP datagrams which local IP user-protocols (including ICMP) supplied to IP in requests for transmission. Note that this counter does not include any datagrams counted in ipForwDatagrams. |
| ipOutDiscards | The number of output IP datagrams for which no problem was encountered to prevent their transmission to their destination, but which were discarded (for example, for lack of buffer space). Note that this counter would include datagrams counted in ipForwDatagrams if any such packets met this (discretionary) discard criterion. |
| ipOutNoRoutes | The number of IP datagrams discarded because no route could be found to transmit them to their destination. Note that this counter includes any packets counted in ipForwDatagrams, which meet this <i>no-route</i> criterion. Note that this includes any datagrams which a host cannot route because all of its default gateways are down. |
| ipReasmReqds | The number of IP fragments received which needed to be reassembled at this entity (the switch). |
| ipReasmOKs | The number of IP datagrams successfully re- assembled. |
| ipReasmFails | The number of failures detected by the IP re- assembly algorithm (for whatever reason: timed out, errors, and so forth). Note that this is not necessarily a count of discarded IP fragments since some algorithms (notably the algorithm in RFC 815) can lose track of the number of fragments by combining them as they are received. |
| ipFragOKs | The number of IP datagrams that have been successfully fragmented at this entity (the switch). |
| ipFragFails | The number of IP datagrams that have been discarded because they needed to be fragmented at this entity (the switch) but could not be, for example, because their Don't Fragment flag was set. |

Table 103. IP Statistics (continued)

| Statistic | Description |
|-------------------|---|
| ipFragCreates | The number of IP datagram fragments that have been generated as a result of fragmentation at this entity (the switch). |
| ipRoutingDiscards | The number of routing entries, which were chosen to be discarded even though they are valid. One possible reason for discarding such an entry could be to free-up buffer space for other routing entries. |
| ipDefaultTTL | The default value inserted into the <code>Time-To-Live (TTL)</code> field of the IP header of datagrams originated at this entity (the switch), whenever a TTL value is not supplied by the transport layer protocol. |
| ipReasmTimeout | The maximum number of seconds, which received fragments are held while they are awaiting reassembly at this entity (the switch). |

IPv6 Statistics

The following command displays IPv6 statistics:

```
show ipv6 counters
```

Command mode: All

Use the following command to clear IPv6 statistics:

```
clear ipv6 counters
```

```
IPv6 Statistics
*****
144 Rcvd          0   HdrErrors      0   TooBigErrors
0   AddrErrors   0   FwdDgrams     0   UnknownProtos
0   Discards     144 Delivers      130 OutRequests
0   OutDiscards  0   OutNoRoutes   0   ReasmReqds
0   ReasmOKs    0   ReasmFails    0
0   FragOKs     0   FragFails    0   FragCreates
7   RcvdMcastPkt 2   SentMcastPkts 0   TruncatedPkts
0   RcvdRedirects 0   SentRedirects

ICMP Statistics
*****
Received :
33 ICMPPkts      0 ICMPErrPkt      0 DestUnreach  0 TimeExcds
0   ParmProbs    0 PktTooBigMsg    9 ICMEchoReq   10 ICMEchoReps
0   RouterSols   0 RouterAdv      5 NeighSols    9 NeighAdv
0   Redirects    0 AdminProhib    0 ICMPBadCode

Sent
19 ICMPMsgs      0 ICMPErrMsgs    0 DstUnReach   0 TimeExcds
0   ParmProbs    0 PktTooBig      10 EchoReq     9 EchoReply
0   RouterSols   0 RouterAdv      11 NeighSols   5 NeighborAdv
0   RedirectMsgs 0 AdminProhibMsgs

UDP statistics
*****
Received :
0 UDPDgrams     0 UDPNoPorts     0 UDPErrPkts

Sent :
0 UDPDgrams
```

Table 104 describes the IPv6 statistics.

Table 104. IPv6 Statistics

| Statistic | Description |
|---------------|---|
| Rcvd | Number of datagrams received from interfaces, including those received in error. |
| HdrErrors | Number of datagrams discarded due to errors in their IP headers, including bad checksums, version number mismatch, other format errors, time-to-live exceeded, errors discovered in processing their IP options, and so forth. |
| TooBigErrors | The number of input datagrams that could not be forwarded because their size exceeded the link MTU of outgoing interface. |
| AddrErrors | Number of datagrams discarded because the IP address in their IP header's destination field was not a valid address to be received at this entity (the switch). This count includes invalid addresses. For entities which are not IP Gateways and therefore do not forward datagrams, this counter includes datagrams discarded because the destination address was not a local address. |
| FwdDgrams | Number of input datagrams for which this entity (the switch) was not their final IP destination, as a result of which an attempt was made to find a route to forward them to that final destination. In entities which do not act as IP Gateways, this counter will include only those packets, which were Source-Routed via this entity (the switch), and the Source-Route option processing was successful. |
| UnknownProtos | Number of locally addressed datagrams received successfully but discarded because of an unknown or unsupported protocol. |
| Discards | Number of IP datagrams for which no problems were encountered to prevent their continued processing, but which were discarded (for example, for lack of buffer space). Note that this counter does not include any datagrams discarded while awaiting re-assembly. |
| Delivers | Number of datagrams successfully delivered to IP user-protocols (including ICMP). |
| OutRequests | Number of IP datagrams which local IP user-protocols (including ICMP) supplied to IP in requests for transmission. |
| OutDiscards | Number of output IP datagrams for which no problem was encountered to prevent their transmission to their destination, but which were discarded (for example, for lack of buffer space). |
| OutNoRoutes | Number of IP datagrams discarded because no route could be found to transmit them to their destination. Note that this includes any datagrams which a host cannot route because all of its default gateways are down. |

Table 104. IPv6 Statistics (continued)

| Statistic | Description |
|---------------|---|
| ReasmReqds | Number of IP fragments received which needed to be reassembled at this entity (the switch). |
| ReasmOKs | Number of IP datagrams successfully re- assembled. |
| ReasmFails | Number of failures detected by the IP re- assembly algorithm (for whatever reason: timed out, errors, and so forth). Note that this is not necessarily a count of discarded IP fragments since some algorithms (notably the algorithm in RFC 815) can lose track of the number of fragments by combining them as they are received. |
| FragOKs | Number of IP datagrams that have been successfully fragmented at this entity (the switch). |
| FragFails | Number of IP datagrams that have been discarded because they needed to be fragmented at this entity (the switch) but could not be, for example, because their Don't Fragment flag was set. |
| FragCreates | Number of IP datagram fragments that have been generated as a result of fragmentation at this entity (the switch). |
| RcvdMCastPkt | The number of multicast packets received by the interface. |
| SentMcastPkts | The number of multicast packets transmitted by the interface. |
| TruncatedPkts | The number of input datagrams discarded because datagram frame didn't carry enough data. |
| RcvdRedirects | The number of Redirect messages received by the interface. |
| SentRedirects | The number of Redirect messages sent. |

The following table describes the IPv6 ICMP statistics.

Table 105. ICMP Statistics

| Statistic | Description |
|-----------------|---|
| Received | |
| ICMPPkts | Number of ICMP messages which the entity (the switch) received. |
| ICMPErrPkt | Number of ICMP messages which the entity (the switch) received but determined as having ICMP-specific errors (bad ICMP checksums, bad length, and so forth). |
| DestUnreach | Number of ICMP Destination Unreachable messages received. |
| TimeExcds | Number of ICMP Time Exceeded messages received. |
| ParmProbs | Number of ICMP Parameter Problem messages received. |
| PktTooBigMsg | The number of ICMP Packet Too Big messages received by the interface. |
| ICMPEchoReq | Number of ICMP Echo (request) messages received. |
| ICMPEchoReps | Number of ICMP Echo Reply messages received. |
| RouterSols | Number of Router Solicitation messages received by the switch. |
| RouterAdv | Number of Router Advertisements received by the switch. |
| NeighSols | Number of Neighbor Solicitations received by the switch. |
| NeighAdv | Number of Neighbor Advertisements received by the switch. |
| Redirects | Number of ICMP Redirect messages received. |
| AdminProhib | The number of ICMP destination unreachable/communication administratively prohibited messages received by the interface. |
| ICMPBadCode | The number of ICMP Parameter Problem messages received by the interface. |
| Sent | |
| ICMPMsgs | Number of ICMP messages which this entity (the switch) attempted to send. |
| ICMPErrMsgs | Number of ICMP messages which this entity (the switch) did not send due to problems discovered within ICMP such as a lack of buffer. This value should not include errors discovered outside the ICMP layer such as the inability of IP to route the resultant datagram. In some implementations there may be no types of errors that contribute to this counter's value. |
| DstUnReach | Number of ICMP Destination Unreachable messages sent. |
| TimeExcds | Number of ICMP Time Exceeded messages sent. |

Table 105. ICMP Statistics (continued)

| Statistic | Description |
|-----------------|--|
| ParmProbs | Number of ICMP Parameter Problem messages sent. |
| PktTooBigs | The number of ICMP Packet Too Big messages sent by the interface. |
| EchoReq | Number of ICMP Echo (request) messages sent. |
| EchoReply | Number of ICMP Echo Reply messages sent. |
| RouterSols | Number of Router Solicitation messages sent by the switch. |
| RouterAdv | Number of Router Advertisements sent by the switch. |
| NeighSols | Number of Neighbor Solicitations sent by the switch. |
| NeighAdv | Number of Neighbor Advertisements sent by the switch. |
| RedirectMsgs | Number of ICMP Redirect messages sent. For a host, this object will always be zero, since hosts do not send redirects. |
| AdminProhibMsgs | Number of ICMP destination unreachable/communication administratively prohibited messages sent. |

Table 106 describes the UDP statistics.

Table 106. UDP Statistics

| Statistic | Description |
|-----------------|---|
| Received | |
| UDPDgrams | Number of UDP datagrams received by the switch. |
| UDPNoPorts | Number of received UDP datagrams for which there was no application at the destination port. |
| UDPErrPkts | Number of received UDP datagrams that could not be delivered for reasons other than the lack of an application at the destination port. |
| Sent | |
| UDPDgrams | Number of UDP datagrams sent from this entity (the switch). |

IPv4 Route Statistics

The following command displays IPv4 route statistics:

```
show ip route counters
```

Command mode: All

```

Route statistics:
-----
Current total outstanding routes      :          1
Highest number ever recorded         :          1
Current static routes                 :           0
Current RIP routes                    :           0
Current OSPF routes                   :           0
Current BGP routes                    :           0
Maximum supported routes              :         2048

ECMP statistics (active in ASIC):
-----
Maximum number of ECMP routes        :         2048
Maximum number of static ECMP routes :          128
Number of routes with ECMP paths     :           0

```

Table 107. Route Statistics

| Statistics | Description |
|--------------------------------------|---|
| Current total outstanding routes | Total number of outstanding routes in the route table. |
| Highest number ever recorded | Highest number of routes ever recorded in the route table. |
| Current static routes | Total number of static routes in the route table. |
| Current RIP routes | Total number of Routing Information Protocol (RIP) routes in the route table. |
| Current OSPF routes | Total number of OSPF routes in the route table. |
| Current BGP routes | Total number of Border Gateway Protocol routes in the route table. |
| Maximum supported routes | Maximum number of routes that are supported. |
| Maximum number of ECMP routes | Maximum number of ECMP routes that are supported. |
| Maximum number of static ECMP routes | Maximum number of static ECMP routes that are supported. |
| Number of routes with ECMP paths | Current number of routes that contain ECMP paths. |

IPv6 Route Statistics

The following command displays IPv6 route statistics:

```
show ipv6 route counters
```

Command mode: All

```
IPv6 Route statistics:
ipv6RoutesCur:          4  ipv6RoutesHighWater:      6
ipv6RoutesMax:          1156

ECMP statistics:
-----
Maximum number of ECMP routes      :      600
Max ECMP paths allowed for one route :      5
```

Table 108. IPv6 Route Statistics

| Statistics | Description |
|--------------------------------------|--|
| ipv6RoutesCur | Total number of outstanding routes in the route table. |
| ipv6RoutesHighWater | Highest number of routes ever recorded in the route table. |
| ipv6RoutesMax | Maximum number of routes that are supported. |
| Maximum number of ECMP routes | Maximum number of ECMP routes supported. |
| Max ECMP paths allowed for one route | Maximum number of ECMP paths supported for each route. |

Use the `clear` option to delete all IPv6 route statistics.

ARP statistics

The following command displays Address Resolution Protocol statistics.

```
show ip arp counters
```

Command mode: All

```
ARP statistics:
arpEntriesCur:          3  arpEntriesHighWater:      4
arpEntriesMax:          4095
```

Table 109. ARP Statistics

| Statistic | Description |
|---------------------|---|
| arpEntriesCur | The total number of outstanding ARP entries in the ARP table. |
| arpEntriesHighWater | The highest number of ARP entries ever recorded in the ARP table. |
| arpEntriesMax | The maximum number of ARP entries that are supported. |

DNS Statistics

The following command displays Domain Name System statistics.

```
show ip dns counters
```

Command mode: All

| | |
|-----------------|---|
| DNS statistics: | |
| dnsInRequests: | 0 |
| dnsOutRequests: | 0 |
| dnsBadRequests: | 0 |

Table 110. DNS Statistics

| Statistics | Description |
|----------------|--|
| dnsInRequests | The total number of DNS response packets that have been received. |
| dnsOutRequests | The total number of DNS response packets that have been transmitted. |
| dnsBadRequests | The total number of DNS request packets received that were dropped. |

ICMP Statistics

The following command displays ICMP statistics:

```
show ip icmp counters
```

Command mode: All

| | | | |
|----------------------|--------|-----------------------|--------|
| ICMP statistics: | | | |
| icmpInMsgs: | 245802 | icmpInErrors: | 1393 |
| icmpInDestUnreachs: | 41 | icmpInTimeExcds: | 0 |
| icmpInParmProbs: | 0 | icmpInSrcQuenchs: | 0 |
| icmpInRedirects: | 0 | icmpInEchos: | 18 |
| icmpInEchoReps: | 244350 | icmpInTimestamps: | 0 |
| icmpInTimestampReps: | 0 | icmpInAddrMasks: | 0 |
| icmpInAddrMaskReps: | 0 | icmpOutMsgs: | 253810 |
| icmpOutErrors: | 0 | icmpOutDestUnreachs: | 15 |
| icmpOutTimeExcds: | 0 | icmpOutParmProbs: | 0 |
| icmpOutSrcQuenchs: | 0 | icmpOutRedirects: | 0 |
| icmpOutEchos: | 253777 | icmpOutEchoReps: | 18 |
| icmpOutTimestamps: | 0 | icmpOutTimestampReps: | 0 |
| icmpOutAddrMasks: | 0 | icmpOutAddrMaskReps: | 0 |

Table 111. ICMP Statistics

| Statistic | Description |
|---------------------|--|
| icmpInMsgs | The total number of ICMP messages which the entity (the switch) received. Note that this counter includes all those counted by <code>icmpInErrors</code> . |
| icmpInErrors | The number of ICMP messages which the entity (the switch) received but determined as having ICMP-specific errors (bad ICMP checksums, bad length, and so forth). |
| icmpInDestUnreachs | The number of ICMP Destination Unreachable messages received. |
| icmpInTimeExcds | The number of ICMP Time Exceeded messages received. |
| icmpInParmProbs | The number of ICMP Parameter Problem messages received. |
| icmpInSrcQuenchs | The number of ICMP Source Quench (buffer almost full, stop sending data) messages received. |
| icmpInRedirects | The number of ICMP Redirect messages received. |
| icmpInEchos | The number of ICMP Echo (request) messages received. |
| icmpInEchoReps | The number of ICMP Echo Reply messages received. |
| icmpInTimestamps | The number of ICMP Timestamp (request) messages received. |
| icmpInTimestampReps | The number of ICMP Timestamp Reply messages received. |

Table 111. ICMP Statistics

| Statistic | Description |
|----------------------|---|
| icmpInAddrMasks | The number of ICMP Address Mask Request messages received. |
| icmpInAddrMaskReps | The number of ICMP Address Mask Reply messages received. |
| icmpOutMsgs | The total number of ICMP messages which this entity (the switch) attempted to send. Note that this counter includes all those counted by <code>icmpOutErrors</code> . |
| icmpOutErrors | The number of ICMP messages which this entity (the switch) did not send due to problems discovered within ICMP such as a lack of buffer. This value should not include errors discovered outside the ICMP layer such as the inability of IP to route the resultant datagram. In some implementations there may be no types of errors that contribute to this counter's value. |
| icmpOutDestUnreachs | The number of ICMP Destination Unreachable messages sent. |
| icmpOutTimeExcds | The number of ICMP Time Exceeded messages sent. |
| icmpOutParmProbs | The number of ICMP Parameter Problem messages sent. |
| icmpOutSrcQuenchs | The number of ICMP Source Quench (buffer almost full, stop sending data) messages sent. |
| icmpOutRedirects | The number of ICMP Redirect messages sent. For a host, this object will always be zero, since hosts do not send redirects. |
| icmpOutEchos | The number of ICMP Echo (request) messages sent. |
| icmpOutEchoReps | The number of ICMP Echo Reply messages sent. |
| icmpOutTimestamps | The number of ICMP Timestamp (request) messages sent. |
| icmpOutTimestampReps | The number of ICMP Timestamp Reply messages sent. |
| icmpOutAddrMasks | The number of ICMP Address Mask Request messages sent. |
| icmpOutAddrMaskReps | The number of ICMP Address Mask Reply messages sent. |

TCP Statistics

The following command displays TCP statistics:

```
show ip tcp counters
```

Command mode: All

| | | | |
|------------------|--------|------------------|------|
| TCP statistics: | | | |
| tcpRtoAlgorithm: | 4 | tcpRtoMin: | 0 |
| tcpRtoMax: | 240000 | tcpMaxConn: | 2048 |
| tcpActiveOpens: | 0 | tcpPassiveOpens: | 16 |
| tcpAttemptFails: | 0 | tcpEstabResets: | 0 |
| tcpInSegs: | 2035 | tcpOutSegs: | 1748 |
| tcpRetransSegs: | 21 | tcpInErrs: | 0 |
| tcpCurrEstab: | 1 | tcpCurrConn: | 5 |
| tcpOutRsts: | 0 | | |

Table 112. TCP Statistics

| Statistic | Description |
|-----------------|---|
| tcpRtoAlgorithm | The algorithm used to determine the <code>timeout</code> value used for retransmitting unacknowledged octets. |
| tcpRtoMin | The minimum value permitted by a TCP implementation for the retransmission <code>timeout</code> , measured in milliseconds. More refined semantics for objects of this type depend upon the algorithm used to determine the retransmission <code>timeout</code> . In particular, when the <code>timeout</code> algorithm is <code>rsre(3)</code> , an object of this type has the semantics of the <code>LBOUND</code> quantity described in RFC 793. |
| tcpRtoMax | The maximum value permitted by a TCP implementation for the retransmission <code>timeout</code> , measured in milliseconds. More refined semantics for objects of this type depend upon the algorithm used to determine the retransmission <code>timeout</code> . In particular, when the <code>timeout</code> algorithm is <code>rsre(3)</code> , an object of this type has the semantics of the <code>UBOUND</code> quantity described in RFC 793. |
| tcpMaxConn | The limit on the total number of TCP connections the entity (the switch) can support. In entities where the maximum number of connections is dynamic, this object should contain the value -1. |
| tcpActiveOpens | The number of times TCP connections have made a direct transition to the <code>SYN-SENT</code> state from the <code>CLOSED</code> state. |
| tcpPassiveOpens | The number of times TCP connections have made a direct transition to the <code>SYN-RCVD</code> state from the <code>LISTEN</code> state. |
| tcpAttemptFails | The number of times TCP connections have made a direct transition to the <code>CLOSED</code> state from either the <code>SYN-SENT</code> state or the <code>SYN-RCVD</code> state, plus the number of times TCP connections have made a direct transition to the <code>LISTEN</code> state from the <code>SYN-RCVD</code> state. |

Table 112. TCP Statistics (continued)

| Statistic | Description |
|----------------|---|
| tcpEstabResets | The number of times TCP connections have made a direct transition to the CLOSED state from either the ESTABLISHED state or the CLOSE-WAIT state. |
| tcpInSegs | The total number of segments received, including those received in error. This count includes segments received on currently established connections. |
| tcpOutSegs | The total number of segments sent, including those on current connections but excluding those containing only retransmitted octets. |
| tcpRetransSegs | The total number of segments retransmitted - that is, the number of TCP segments transmitted containing one or more previously transmitted octets. |
| tcpInErrs | The total number of segments received in error (for example, bad TCP checksums). |
| tcpCurEstab | The total number of outstanding TCP sessions in the ESTABLISHED state. |
| tcpCurConn | The total number of outstanding TCP sessions that are currently opened. |
| tcpOutRsts | The number of TCP segments sent containing the RST flag. |

UDP Statistics

The following command displays UDP statistics:

```
show ip udp counters
```

Command mode: All

| | | | |
|-----------------|----|------------------|---------|
| UDP statistics: | | | |
| udpInDatagrams: | 54 | udpOutDatagrams: | 43 |
| udpInErrors: | 0 | udpNoPorts: | 1578077 |

Table 113. UDP Statistics

| Statistic | Description |
|-----------------|---|
| udpInDatagrams | The total number of UDP datagrams delivered to the switch. |
| udpOutDatagrams | The total number of UDP datagrams sent from this entity (the switch). |
| udpInErrors | The number of received UDP datagrams that could not be delivered for reasons other than the lack of an application at the destination port. |
| udpNoPorts | The total number of received UDP datagrams for which there was no application at the destination port. |

IGMP Statistics

The following command displays statistics about IGMP protocol packets for all VLANs:

```
show ip igmp counter
```

Command mode: All

| IGMP vlan 2 statistics: | | | |
|----------------------------------|----|------------------------------|---|
| ----- | | | |
| rxIgmpValidPkts: | 0 | rxIgmpInvalidPkts: | 0 |
| rxIgmpGenQueries: | 0 | rxIgmpGrpSpecificQueries: | 0 |
| rxIgmpGroupSrcSpecificQueries: | 0 | rxIgmpDiscardPkts: | 0 |
| rxIgmpLeaves: | 0 | rxIgmpReports: | 0 |
| txIgmpReports: | 0 | txIgmpGrpSpecificQueries: | 0 |
| txIgmpLeaves: | 0 | rxIgmpV3CurrentStateRecords: | 0 |
| rxIgmpV3SourceListChangeRecords: | 0 | rxIgmpV3FilterChangeRecords: | 0 |
| txIgmpGenQueries: | 18 | rxPimHellos: | 0 |

The following command displays statistics about IGMP protocol packets for a specific VLAN:

```
show ip igmp vlan <vlan number> counter
```

Command mode: All

| IGMP vlan 147 statistics: | | | |
|----------------------------------|----|------------------------------|---|
| ----- | | | |
| rxIgmpValidPkts: | 0 | rxIgmpInvalidPkts: | 0 |
| rxIgmpGenQueries: | 0 | rxIgmpGrpSpecificQueries: | 0 |
| rxIgmpGroupSrcSpecificQueries: | 0 | rxIgmpDiscardPkts: | 0 |
| rxIgmpLeaves: | 0 | rxIgmpReports: | 0 |
| txIgmpReports: | 0 | txIgmpGrpSpecificQueries: | 0 |
| txIgmpLeaves: | 0 | rxIgmpV3CurrentStateRecords: | 0 |
| rxIgmpV3SourceListChangeRecords: | 0 | rxIgmpV3FilterChangeRecords: | 0 |
| txIgmpGenQueries: | 11 | rxPimHellos: | 0 |

Table 114. IGMP Statistics

| Statistic | Description |
|-------------------------------|--|
| rxIgmpValidPkts | Total number of valid IGMP packets received |
| rxIgmpInvalidPkts | Total number of invalid packets received |
| rxIgmpGenQueries | Total number of General Membership Query packets received |
| rxIgmpGrpSpecificQueries | Total number of Membership Query packets received from specific groups |
| rxIgmpGroupSrcSpecificQueries | Total number of Group Source-Specific Queries (GSSQ) received |
| rxIgmpDiscardPkts | Total number of IGMP packets discarded |
| rxIgmpLeaves | Total number of Leave requests received |

Table 114. IGMP Statistics

| Statistic | Description |
|---------------------------------|---|
| rxIgmPReports | Total number of Membership Reports received |
| txIgmPReports | Total number of Membership reports transmitted |
| txIgmPGrpSpecificQueries | Total number of Membership Query packets transmitted to specific groups |
| txIgmPLeaves | Total number of Leave messages transmitted |
| rxIgmPV3CurrentStateRecords | Total number of Current State records received |
| rxIgmPV3SourceListChangeRecords | Total number of Source List Change records received. |
| rxIgmPV3FilterChangeRecords | Total number of Filter Change records received. |
| txIgmPGenQueries | Total number of General Membership Query packets transmitted |
| rxPimHellos | Total number of PIM hello packets received |

MLD Statistics

Table 115. MLD Statistics Commands

| Command Syntax and Usage |
|--|
| <pre>show ipv6 mld</pre> <p>Displays MLD global statistics. Command mode: All See page 191 for sample output.</p> |
| <pre>show ipv6 mld counters</pre> <p>Displays MLD area statistics. Command mode: All except User EXEC</p> |
| <pre>show ipv6 mld interface</pre> <p>Displays information for all MLD interfaces. Command mode: All</p> |
| <pre>show ipv6 mld interface <interface number></pre> <p>Displays MLD interface statistics for the specified interface. Command mode: All</p> |
| <pre>show ipv6 mld interface [<interface number>] counters</pre> <p>Displays MLD interface statistics. Command mode: All except User EXE</p> |
| <pre>show ipv6 mld interface counters</pre> <p>Displays total number of MLD entries. Command mode: All</p> |
| <pre>clear ipv6 mld counters</pre> <p>Clears MLD counters. Command mode: Privileged EXEC</p> |
| <pre>clear ipv6 mld dynamic</pre> <p>Clears all dynamic MLD tables. Command mode: Privileged EXEC</p> |
| <pre>clear ipv6 mld groups</pre> <p>Clears dynamic MLD registered group tables. Command mode: Privileged EXEC</p> |
| <pre>clear ipv6 mld mrouter</pre> <p>Clears dynamic MLD mrouter group tables. Command mode: Privileged EXEC</p> |

MLD Global Statistics

The MLD global statistics displays information for all MLD packets received on all interfaces

```
show ipv6 mld counters
```

Command mode: All.

```
MLD global statistics:
-----
Total L3 IPv6 (S, G, V) entries: 2
Total MLD groups:                2
Bad Length:                       0
Bad Checksum:                     0
Bad Receive If:                   0
Receive non-local:                 0
Invalid Packets:                   4

MLD packet statistics for interfaces:

MLD interface packet statistics for interface 1:
MLD msg type      Received      Sent      RxErrors
-----
General Query          0          1067         0
MAS Query              0           0           0
MASSQ Query           0           0           0
MLDv1 Report          0           0           0
MLDv1 Done            0           0           0
MLDv2 Report          1069        1084         0
INC CSRs (v2)         1           0           0
EXC CSRs (v2)         2134        1093         0
TO_INC FMCRs (v2)     1           0           0
TO_EXC FMCRs (v2)     0           15          0
ALLOW SLCRs (v2)     0           0           0
BLOCK SLCRs (v2)      0           0           0

MLD interface packet statistics for interface 2:
MLD msg type      Received      Sent      RxErrors
-----
General Query          0          2467         0
MAS Query              0           0           0
MASSQ Query           0           0           0
MLDv1 Report          0           0           0
MLDv1 Done            0           0           0
MLDv2 Report          2           2472         0
INC CSRs (v2)         1           0           0
EXC CSRs (v2)         0          2476         0
TO_INC FMCRs (v2)     0           0           0
TO_EXC FMCRs (v2)     0           8           0
ALLOW SLCRs (v2)     0           0           0
BLOCK SLCRs (v2)      1           0           0
```

The following table describes the fields in the MLD global statistics output.

Table 116. MLD Global Statistics

| Statistic | Description |
|-----------------------|--|
| Bad Length | Number of messages received with length errors. |
| Bad Checksum | Number of messages received with an invalid IP checksum. |
| Bad Receive If | Number of messages received on an interface not enabled for MLD. |
| Receive non-local | Number of messages received from non-local senders. |
| Invalid packets | Number of rejected packets. |
| General Query (v1/v2) | Number of general query packets. |
| MAS Query(v1/v2) | Number of multicast address specific query packets. |
| MASSQ Query (v2) | Number of multicast address and source specific query packets. |
| Listener Report(v1) | Number of packets sent by a multicast listener in response to MLDv1 query. |
| Listener Done(v1/v2) | Number of packets sent by a host when it wants to stop receiving multicast traffic. |
| Listener Report(v2) | Number of packets sent by a multicast listener in response to MLDv2 query. |
| MLDv2 INC mode CSRs | Number of current state records with include filter mode. |
| MLDv2 EXC mode CSRs | Number of current state records with exclude filter mode. |
| MLDv2 TO_INC FMCRs | Number of filter mode change records for which the filter mode has changed to include mode. |
| MLDv2 TO_EXC FMCRs | Number of filter mode change records for which the filter mode has changed to exclude mode. |
| MLDv2 ALLOW SLCRs | Number of source list change records for which the specified sources from where the data is to be received has changed. |
| MLDv2 BLOCK SLCRs | Number of source list change records for which the specified sources from where the data is to be received is to be blocked. |

OSPF Statistics

Table 117. OSPF Statistics Commands

| Command Syntax and Usage |
|---|
| <pre>show ip ospf counters</pre> <p>Displays OSPF statistics.</p> <p>Command mode: All</p> <p>See page 194 for sample output.</p> |
| <pre>show ip ospf area counters</pre> <p>Displays OSPF area statistics.</p> <p>Command mode: All except User EXEC</p> |
| <pre>show ip ospf interface [<interface number>] counters</pre> <p>Displays OSPF interface statistics.</p> <p>Command mode: All except User EXEC</p> |

OSPF Global Statistics

The following command displays statistics about OSPF packets received on all OSPF areas and interfaces:

```
show ip ospf counters
```

Command mode: All

```

OSPF stats
-----
Rx/Tx Stats:          Rx          Tx
-----
Pkts                  0          0
hello                 23         518
database              4          12
ls requests           3          1
ls acks                7          7
ls updates            9          7

Nbr change stats:    Intf change Stats:
hello                2          up                4
start                0          down              2
n2way                2          loop              0
adjoint ok           2          unloop            0
negotiation done     2          wait timer        2
exchange done        2          backup            0
bad requests          0          nbr change        5
bad sequence          0
loading done          2
nlway                 0
rst_ad                0
down                  1

Timers kickoff
hello                514
retransmit           1028
lsa lock              0
lsa ack               0
dbage                 0
summary               0
ase export            0
  
```

Table 118. OSPF General Statistics

| Statistic | Description |
|---------------------|--|
| Rx/Tx Stats: | |
| Rx Pkts | The sum total of all OSPF packets received on all OSPF areas and interfaces. |
| Tx Pkts | The sum total of all OSPF packets transmitted on all OSPF areas and interfaces. |
| Rx Hello | The sum total of all Hello packets received on all OSPF areas and interfaces. |
| Tx Hello | The sum total of all Hello packets transmitted on all OSPF areas and interfaces. |

Table 118. OSPF General Statistics (continued)

| Statistic | Description |
|--------------------------|--|
| Rx Database | The sum total of all Database Description packets received on all OSPF areas and interfaces. |
| Tx Database | The sum total of all Database Description packets transmitted on all OSPF areas and interfaces. |
| Rx Is Requests | The sum total of all Link State Request packets received on all OSPF areas and interfaces. |
| Tx Is Requests | The sum total of all Link State Request packets transmitted on all OSPF areas and interfaces. |
| Rx Is Acks | The sum total of all Link State Acknowledgement packets received on all OSPF areas and interfaces. |
| Tx Is Acks | The sum total of all Link State Acknowledgement packets transmitted on all OSPF areas and interfaces. |
| Rx Is Updates | The sum total of all Link State Update packets received on all OSPF areas and interfaces. |
| Tx Is Updates | The sum total of all Link State Update packets transmitted on all OSPF areas and interfaces. |
| Nbr Change Stats: | |
| hello | The sum total of all Hello packets received from neighbors on all OSPF areas and interfaces. |
| Start | The sum total number of neighbors in this state (that is, an indication that Hello packets must now be sent to the neighbor at intervals of <code>HelloInterval</code> seconds.) across all OSPF areas and interfaces. |
| n2way | The sum total number of bidirectional communication establishment between this router and other neighboring routers. |
| adjoint ok | The sum total number of decisions to be made (again) as to whether an adjacency should be established/maintained with the neighbor across all OSPF areas and interfaces. |
| negotiation done | The sum total number of neighbors in this state wherein the Master/slave relationship has been negotiated, and sequence numbers have been exchanged, across all OSPF areas and interfaces. |
| exchange done | The sum total number of neighbors in this state (that is, in an adjacency's final state) having transmitted a full sequence of Database Description packets across all OSPF areas and interfaces. |
| bad requests | The sum total number of Link State Requests which have been received for a link state advertisement not contained in the database across all interfaces and OSPF areas. |

Table 118. OSPF General Statistics (continued)

| Statistic | Description |
|---------------------------|---|
| bad sequence | The sum total number of Database Description packets which have been received that either: <ol style="list-style-type: none"> Has an unexpected DD sequence number Unexpectedly has the init bit set Has an options field differing from the last Options field received in a Database Description packet. Any of these conditions indicate that some error has occurred during adjacency establishment for all OSPF areas and interfaces. |
| loading done | The sum total number of link state updates received for all out-of-date portions of the database across all OSPF areas and interfaces. |
| n1way | The sum total number of Hello packets received from neighbors, in which this router is not mentioned across all OSPF interfaces and areas. |
| rst_ad | The sum total number of times the Neighbor adjacency has been reset across all OPSF areas and interfaces. |
| down | The total number of Neighboring routers down (that is, in the initial state of a neighbor conversation) across all OSPF areas and interfaces. |
| Intf Change Stats: | |
| up | The sum total number of interfaces up in all OSPF areas. |
| down | The sum total number of interfaces down in all OSPF areas. |
| loop | The sum total of interfaces no longer connected to the attached network across all OSPF areas and interfaces. |
| unloop | The sum total number of interfaces, connected to the attached network in all OSPF areas. |
| wait timer | The sum total number of times the Wait Timer has been fired, indicating the end of the waiting period that is required before electing a (Backup) Designated Router across all OSPF areas and interfaces. |
| backup | The sum total number of Backup Designated Routers on the attached network for all OSPF areas and interfaces. |
| nbr change | The sum total number of changes in the set of bidirectional neighbors associated with any interface across all OSPF areas. |

Table 118. OSPF General Statistics (continued)

| Statistic | Description |
|------------------------|---|
| Timers Kickoff: | |
| hello | The sum total number of times the Hello timer has been fired (which triggers the <code>send</code> of a Hello packet) across all OSPF areas and interfaces. |
| retransmit | The sum total number of times the Retransmit timer has been fired across all OSPF areas and interfaces. |
| lsa lock | The sum total number of times the Link State Advertisement (LSA) lock timer has been fired across all OSPF areas and interfaces. |
| lsa ack | The sum total number of times the LSA <code>Ack</code> timer has been fired across all OSPF areas and interfaces. |
| dbage | The total number of times the data base age (<code>Dbage</code>) has been fired. |
| summary | The total number of times the Summary timer has been fired. |
| ase export | The total number of times the Autonomous System Export (ASE) timer has been fired. |

OSPFv3 Statistics

Table 119. OSPFv3 Statistics Commands

| Command Syntax and Usage |
|---|
| <pre>show ipv6 ospf counters</pre> <p>Displays OSPFv3 statistics.</p> <p>Command mode: All</p> <p>See page 194 for sample output.</p> |
| <pre>show ipv6 ospf area counters</pre> <p>Displays OSPFv3 area statistics.</p> <p>Command mode: All except User EXEC</p> |
| <pre>show ipv6 ospf interface [<interface number>] counters</pre> <p>Displays OSPFv3 interface statistics.</p> <p>Command mode: All except User EXEC</p> |

OSPFv3 Global Statistics

The following command displays statistics about OSPFv3 packets received on all OSPFv3 areas and interfaces:

```
show ipv6 ospf counters
```

Command mode: All

```

OSPFv3 stats
-----
Rx/Tx/Disd Stats:      Rx          Tx          Discarded
-----
Pkts                   9695       95933       0
hello                  9097       8994        0
database                39         51          6
ls requests             16         8           0
ls acks                 172        360         0
ls updates              371        180         0

Nbr change stats:      Intf change Stats:
down                   0          down         5
attempt               0          loop         0
init                  1          waiting      6
n2way                 1          ptop         0
exstart               1          dr           4
exchange done         1          backup       6
loading done          1          dr other     0
full                  1          all events   33
all events            6

Timers kickoff
hello                 8988
wait                  6
poll                  0
nbr probe             0

Number of LSAs
originated            180
rcvd newer originations 355
  
```

The OSPFv3 General Statistics contain the sum total of all OSPF packets received on all OSPFv3 areas and interfaces.

Table 120. OSPFv3 General Statistics

| Statistics | Description |
|---------------------|---|
| Rx/Tx Stats: | |
| Rx Pkts | The sum total of all OSPFv3 packets received on all OSPFv3 interfaces. |
| Tx Pkts | The sum total of all OSPFv3 packets transmitted on all OSPFv3 interfaces. |
| Discarded Pkts | The sum total of all OSPFv3 packets discarded. |
| Rx hello | The sum total of all Hello packets received on all OSPFv3 interfaces. |

Table 120. OSPFv3 General Statistics (continued)

| Statistics | Description |
|--------------------------|--|
| Tx hello | The sum total of all Hello packets transmitted on all OSPFv3 interfaces. |
| Discarded hello | The sum total of all Hello packets discarded, including packets for which no associated interface has been found. |
| Rx database | The sum total of all Database Description packets received on all OSPFv3 interfaces. |
| Tx database | The sum total of all Database Description packets transmitted on all OSPFv3 interfaces. |
| Discarded database | The sum total of all Database Description packets discarded. |
| Rx ls requests | The sum total of all Link State Request packets received on all OSPFv3 interfaces. |
| Tx ls requests | The sum total of all Link State Request packets transmitted on all OSPFv3 interfaces. |
| Discarded ls requests | The sum total of all Link State Request packets discarded. |
| Rx ls acks | The sum total of all Link State Acknowledgement packets received on all OSPFv3 interfaces. |
| Tx ls acks | The sum total of all Link State Acknowledgement packets transmitted on all OSPFv3 interfaces. |
| Discarded ls acks | The sum total of all Link State Acknowledgement packets discarded. |
| Rx ls updates | The sum total of all Link State Update packets received on all OSPFv3 interfaces. |
| Tx ls updates | The sum total of all Link State Update packets transmitted on all OSPFv3 interfaces. |
| Discarded ls updates | The sum total of all Link State Update packets discarded. |
| Nbr Change Stats: | |
| down | The total number of Neighboring routers down (in the initial state of a neighbor conversation) across all OSPFv3 interfaces. |
| attempt | The total number of transitions into attempt state of neighboring routers across all OSPFv3 interfaces. |
| init | The total number of transitions into init state of neighboring routers across all OSPFv3 interfaces. |
| n2way | The total number of bidirectional communication establishment between this router and other neighboring routers. |
| exstart | The total number of transitions into exstart state of neighboring routers across all OSPFv3 interfaces |

Table 120. OSPFv3 General Statistics (continued)

| Statistics | Description |
|---------------------------|--|
| exchange done | The total number of neighbors in this state (that is, in an adjacency's final state) having transmitted a full sequence of Database Description packets, across all OSPFv3 interfaces. |
| loading done | The total number of link state updates received for all out-of-date portions of the database across all OSPFv3 interfaces. |
| full | The total number of transitions into full state of neighboring routers across all OSPFv3 interfaces. |
| all events | The total number of state transitions of neighboring routers across all OSPFv3 interfaces. |
| Intf Change Stats: | |
| down | The total number of transitions into down state of all OSPFv3 interfaces. |
| loop | The total number of transitions into loopback state of all OSPFv3 interfaces. |
| waiting | The total number of transitions into waiting state of all OSPFv3 interfaces. |
| ptop | The total number of transitions into point-to-point state of all OSPFv3 interfaces. |
| dr | The total number of transitions into Designated Router other state of all OSPFv3 interfaces. |
| backup | The total number of transitions into backup state of all OSPFv3 interfaces. |
| all events | The total number of changes associated with any OSPFv3 interface, including changes into internal states. |
| Timers Kickoff: | |
| hello | The total number of times the Hello timer has been fired (which triggers the <code>send</code> of a Hello packet) across all OSPFv3 interfaces. |
| wait | The total number of times the wait timer has been fired (which causes an interface to exit waiting state), across all OPSFv3 interfaces. |
| poll | The total number of times the timer whose firing causes hellos to be sent to inactive NBMA and Demand Circuit neighbors has been fired, across all OPSFv3 interfaces. |
| nbr probe | The total number of times the neighbor probe timer has been fired, across all OPSFv3 interfaces. |
| Number of LSAs: | |
| originated | The number of LSAs originated by this router. |
| rcvd newer originations | The number of LSAs received that have been determined to be newer originations. |

VRRP Statistics

Virtual Router Redundancy Protocol (VRRP) support on the EN4093 and EN4093R provides redundancy between routers in a LAN. This is accomplished by configuring the same virtual router IP address and ID number on each participating VRRP-capable routing device. One of the virtual routers is then elected as the master, based on a number of priority criteria, and assumes control of the shared virtual router IP address. If the master fails, one of the backup virtual routers will assume routing authority and take control of the virtual router IP address.

When virtual routers are configured, you can display the protocol statistics for VRRP. The following command displays VRRP statistics:

```
show ip vrrp counters
```

Command mode: All

| | | | |
|------------------|---|------------------|---|
| VRRP statistics: | | | |
| vrrpInAdvers: | 0 | vrrpBadAdvers: | 0 |
| vrrpOutAdvers: | 0 | | |
| vrrpBadVersion: | 0 | vrrpBadVrid: | 0 |
| vrrpBadAddress: | 0 | vrrpBadData: | 0 |
| vrrpBadPassword: | 0 | vrrpBadInterval: | 0 |

Table 121. VRRP Statistics

| Statistics | Description |
|-----------------|--|
| vrrpInAdvers | The total number of valid VRRP advertisements that have been received. |
| vrrpBadAdvers | The total number of VRRP advertisements received that were dropped. |
| vrrpOutAdvers | The total number of VRRP advertisements that have been sent. |
| vrrpBadVersion | The total number of VRRP advertisements received that had a bad version number. |
| vrrpBadVrid | The total number of VRRP advertisements received that had a bad virtual router ID. |
| vrrpBadAddress | The total number of VRRP advertisements received that had a bad address. |
| vrrpBadData | The total number of VRRP advertisements received that had bad data. |
| vrrpBadPassword | The total number of VRRP advertisements received that had a bad password. |
| vrrpBadInterval | The total number of VRRP advertisements received that had a bad interval. |

PIM Statistics

The following command displays Protocol Independent Multicast (PIM) statistics:

```
show ip pim counters
```

Command mode: All

| | |
|------------------|-------------|
| Hello Tx/Rx | : 2595/2596 |
| Join/Prune Tx/Rx | : 0/0 |
| Assert Tx/Rx | : 0/0 |
| Register Tx/Rx | : 0/0 |
| Null-Reg Tx/Rx | : 0/0 |
| RegStop Tx/Rx | : 0/0 |
| CandRPAdv Tx/Rx | : 973/0 |
| BSR Tx/Rx | : 0/1298 |
| Graft Tx/Rx | : 0/0 |
| Graft Ack Tx/Rx | : 0/0 |
| Mcast data Tx/Rx | : 0/0 |
| MDP drop Tx/Rx | : 0/0 |
| CTL drop Tx/Rx | : 0/0 |
| Bad pkts | : 0 |

Table 122. PIM Statistics

| Statistics | Description |
|------------------|---|
| Hello Tx/Rx | Number of Hello messages transmitted or received |
| Join/Prune Tx/Rx | Number of Join/Prune messages transmitted or received |
| Assert Tx/Rx | Number of Assert messages transmitted or received |
| Register Tx/Rx | Number of Register messages transmitted or received |
| Null-Reg Tx/Rx | Number of NULL-register messages received |
| RegStop Tx/Rx | Number of Register Stop messages transmitted or received |
| CandRPAdv Tx/Rx | Number of Candidate RP Advertisements transmitted or received |
| BSR Tx/Rx | Number of Bootstrap Router (BSR) messages transmitted or received |
| Graft Tx/Rx | Number of Graft messages transmitted or received |
| Graft Ack Tx/Rx | Number of Graft Acknowledgements transmitted or received |
| Mcast data Tx/Rx | Number of multicast datagrams transmitted or received |
| MDP drop Tx/Rx | Number of Multicast data packet Tx/Rx dropped |
| CTL drop Tx/Rx | Number of PIM control packet Tx/Rx dropped |
| Bad pkts | Number of bad PIM packets received |

Routing Information Protocol Statistics

The following command displays RIP statistics:

```
show ip rip counters
```

Command mode: All

```
RIP ALL STATS INFORMATION:  
RIP packets received = 12  
RIP packets sent = 75  
RIP request received = 0  
RIP response received = 12  
RIP request sent = 3  
RIP response sent = 72  
RIP route timeout = 0  
RIP bad size packet received = 0  
RIP bad version received = 0  
RIP bad zeros received = 0  
RIP bad src port received = 0  
RIP bad src IP received = 0  
RIP packets from self received = 0
```

OpenFlow Statistics

Table 123. OpenFlow Statistics Commands

| Command Syntax and Usage |
|---|
| <pre>show openflow statistics</pre> <p>Displays OpenFlow traffic statistics for each OpenFlow instance.</p> <p>Command mode: All</p> |
| <pre>show openflow instance <I-2> statistics</pre> <p>Displays OpenFlow traffic statistics for the specified instance ID.</p> <p>Command mode: All</p> |
| <pre>clear openflow statistics</pre> <p>Clears OpenFlow data for all instances.</p> <p>Command mode: Privileged EXEC</p> |
| <pre>clear openflow instance <I-2> statistics</pre> <p>Clears OpenFlow data for the specified instance ID.</p> <p>Command mode: Privileged EXEC</p> |

Use the following command to display OpenFlow traffic statistics for each OpenFlow instance:

```
show openflow statistics
```

Command mode: All

```

Openflow statistics for instance 1
Flow Count
    Basic Flows:      0      (ACL Based: 0, Unicast FDB Based: 0, Multicast FDB
Based: 0)
    Emergency Flows: 0      (ACL Based: 0, Unicast FDB Based: 0, Multicast FDB
Based: 0)

Buffering Count:
    Openflow Packets Buffered   : 0
    Openflow Packets Timed out  : 0
    Openflow Packets Retrieved  : 0
    Openflow Packets Retrieve attempts : 0

Message Count
Hello-Sent: 0              Hello-Received: 0
Echo-Request-Sent: 0      Echo-Request-Received: 0
Echo-Reply-Sent: 0        Echo-Reply-Received: 0
Vendor: 0

Vendor Flow-Mod:
    Add: 0
    Modify: 0
    Modify-Strict: 0
    Delete: 0
    Delete-Strict: 0
Feature-Request: 0        Feature-Reply: 0
Get-Config-Request: 0    Get-Config-Reply: 0
Set-Config: 0

Packet-In
    No-Match: 0
    Action: 0

Flow-Removed:
    Idle-Timeout: 0
    Hard-Timeout: 0
    Delete: 0

Vendor-Flow-Removed:
    Idle-Timeout: 0
    Hard-Timeout: 0
    Delete: 0

Port-Status:
    Add: 0
    Delete: 0
    Modify: 0

Packet-Out: 0
Flow-Mod:
    Add: 0
    Modify: 0
    Modify-Strict: 0
    Delete: 0
    Delete-Strict: 0

Port-Mod: 0
...

```

```

...
Statistics-Request:
  Desc: 0
  Flow: 0
  Aggregate: 0
  Table: 0
  Port: 0
  Vendor: 0
    stats: 0
    stats-strict: 0
Statistics-Reply:
  Desc: 0
  Flow: 0
  Aggregate: 0
  Table: 0
  Port: 0
  Vendor: 0
    stats: 0
    stats-strict: 0
Barrier-Request: 0
Barrier-Reply: 0
Error Messages
Hello Failed Sent:
  Incompatible: 0
Hello Failed Recv:
  Incompatible: 0
Bad Request:
  Bad-Version: 0
  Bad-Type: 0
  Bad-Stat: 0
  Bad-Vendor: 0
  Bad-Subtype: 0
  Bad-Len: 0
  Buffer-Empty: 0
  Buffer-Unknown: 0
Bad Action:
  Bad-Type: 0
  Bad-Len: 0
  Bad-Out-Port: 0
  Bad-Argument: 0
  Too-many: 0
Flow-Mod-Failed:
  All-Table-Full: 0
  Overlap: 0
  Permission-Error: 0
  Emergency-Timeout: 0
  Bad-Command: 0
  Unsupported: 0
Port-Mod-Failed:
  Bad-Port: 0
  Bad-hw-addr: 0
-----
Openflow instance 2 is currently disabled

```


Table 124. OpenFlow Table Statistics

| Parameter | Description |
|------------------------------------|--|
| Flow Count | |
| Basic Flows | Count of flows stored in the basic flow table, sorted by type: ACL, unicast FDB and multicast FDB. |
| Emergency Flows | Count of flows stored in the emergency flow table, sorted by type: ACL, unicast FDB and multicast FDB. |
| Buffering Count | |
| Openflow Packets Buffered | Count of packets buffered. |
| Openflow Packets Timed out | Count of buffered packets dropped due to time out. |
| Openflow Packets Retrieved | Count of packets retrieved. |
| Openflow Packets Retrieve attempts | Count of attempts made to retrieve the buffer. |
| Message Count | Count of messages exchanged between Controller and switch. |
| Hello-Sent | Count of <code>Hello</code> messages sent from the switch to Controller. |
| Hello-Received | Count of <code>Hello</code> messages received in the Controller from the switch. |
| Echo-Request-Sent | Count of <code>Echo Request</code> messages sent from switch to Controller. |
| Echo-Request-Received | Count of <code>Echo Request</code> messages received in switch from Controller. |
| Echo-Reply-Sent | Count of <code>Echo Reply</code> messages received in switch from Controller. |
| Echo-Reply-Received | Count of <code>Echo Reply</code> messages received in switch from Controller. |
| Vendor | Count of <code>Vendor</code> messages received in switch from controller. |
| Vendor Flow-Mod | |
| Add | Count of vendor-defined <code>add_flow_mod</code> messages received in the switch. |
| Modify | Count of vendor-defined <code>modify_flow_mod</code> messages received in the switch. |
| Modify-Strict | Count of vendor-defined <code>modify_strict_flow_mod</code> messages received in the switch. |

| Parameter | Description |
|----------------------------|---|
| Delete | Count of vendor-defined <code>delete flow_mod</code> messages received in the switch. |
| Delete-Strict | Count of vendor-defined <code>delete-strict flow_mod</code> messages received in the switch. |
| Feature-Request | Count of <code>Feature Request</code> messages received from the Controller to the switch. |
| Feature-Reply | Count of <code>Feature Reply</code> messages sent from the switch to the Controller. |
| Get-Config-Request | Count of <code>Get Config Request</code> messages received from the Controller to the switch. |
| Get-Config-Reply | Count of <code>Get Config Reply</code> messages sent from the switch to the Controller. |
| Set-Config | Count of <code>Set Config</code> messages received from the Controller. |
| Packet-In | |
| No-Match | Count of <code>Packet-In</code> messages sent to Controller due to no matching flows. |
| Action | Count of <code>Packet-In</code> messages sent to Controller due to action explicitly asking to forward to Controller. |
| Flow-Removed | |
| Idle-Timeout | Count of flow entries removed due to idle-timeout expiration. |
| Hard-Timeout | Count of flow entries removed due to hard-timeout expiration. |
| Delete | Count of flow entries removed due to explicit deletion. |
| Vendor-Flow-Removed | |
| Idle-Timeout | Count of vendor-defined flow entries removed due to idle-timeout expiration. |
| Hard-Timeout | Count of vendor-defined flow entries removed due to hard-timeout expiration. |
| Delete | Count of vendor-defined flow entries removed due to explicit deletion. |
| Port-Status | |
| Add | Count of <code>port-status</code> messages sent triggered by adding a port to OpenFlow. |
| Delete | Count of <code>port-status</code> messages sent triggered by removing a port from OpenFlow. |

| Parameter | Description |
|---------------------------|--|
| Modify | Count of <code>port-status</code> messages sent triggered by a modification of a port belonging to OpenFlow (for example, up/down status). |
| Packet-Out | Count of <code>packet-out</code> messages received from the Controller. |
| Flow-Mod | |
| Add | Count of <code>add_flow_mod</code> messages received in the switch. |
| Modify | Count of <code>modify_flow_mod</code> messages received in the switch. |
| Modify-Strict | Count of <code>modify_strict_flow_mod</code> messages received in the switch. |
| Delete | Count of <code>delete_flow_mod</code> messages received in the switch. |
| Delete-Strict | Count of <code>delete_strict_flow_mod</code> messages received in the switch. |
| Port-Mod | Count of <code>port_mod</code> messages received in the switch from the Controller. |
| Statistics-Request | |
| Desc | Count of Description statistics requests received from the Controller. |
| Flow | Count of Flow statistics requests received from the Controller. |
| Aggregate | Count of Aggregate statistics requests received from the Controller. |
| Table | Count of Table statistics requests received from the Controller. |
| Port | Count of Port statistics requests received from the Controller. |
| Vendor | |
| stats | Count of Vendor statistics requests received from the Controller. |
| stats-strict | Count of Vendor strict statistics requests received from the Controller. |
| Statistics-Reply | |
| Desc | Count of Description statistics requests sent to the Controller. |
| Flow | Count of Flow statistics requests sent to the Controller. |

| Parameter | Description |
|--------------------------|---|
| Aggregate | Count of Aggregate statistics requests sent to the Controller. |
| Table | Count of Table statistics requests sent to the Controller. |
| Port | Count of Port statistics requests sent to the Controller. |
| Vendor | |
| stats | Count of Vendor statistics requests sent to the Controller. |
| stats-strict | Count of Vendor strict statistics requests sent to the Controller. |
| Barrier-Request | Count of <code>barrier-request</code> messages received from the Controller. |
| Barrier-Reply | Count of <code>barrier-reply</code> messages sent to the Controller. |
| Error Messages | Count of error messages handled - sending/receiving error messages. |
| Hello Failed Sent | |
| Incompatible | Count of error messages sent by the switch if the version in the <code>Hello</code> message is incompatible with the version in the Controller. |
| Hello Failed Recv | |
| Incompatible | Count of error messages received in the switch if the version in the <code>Hello</code> message is incompatible with the version in the Controller. |
| Bad Request | |
| Bad-Version | Count of error messages sent due to <code>bad-version</code> in the request header. |
| Bad-Type | Count of error messages sent due to <code>bad-type</code> in the request header. |
| Bad-Stat | Count of error messages sent due to a specific statistics request that is not supported. |
| Bad-Vendor | Count of error messages sent due to vendor-specific message that is not supported. |
| Bad-Subtype | Count of error messages sent due to message subtype that is not supported. |
| Bad-Len | Count of error messages sent due to wrong request length for type of message received in the request header. |
| Buffer-Empty | Count of error messages sent when the specified buffer in the request does not exist. |

| Parameter | Description |
|------------------------|--|
| Buffer-Unknown | Count of error messages sent when the specified buffer in the request does not exist. |
| Bad Action | |
| Bad-Type | Count of error messages sent due to unknown action type specified in <code>flow_mod</code> message. |
| Bad-Len | Count of error messages sent due to wrong action length for type of message received in the <code>flow_mod</code> message. |
| Bad-Out-Port | Count of error message sent due to invalid port in the action field specified <code>flow_mod</code> message. |
| Bad-Argument | Count of error message sent due to bad action argument in <code>flow_mod</code> message that is not supported. |
| Too-Many | Count of error message sent due to too many actions received in the <code>flow_mod</code> message that cannot be handled. |
| Flow-Mod-Failed | |
| All-Table-Full | Count of error messages due to table full when adding or updating <code>flow_mod</code> message. |
| Overlap | Count of error messages sent due to an attempt to add overlapping <code>flow_mod</code> messages. |
| Permission-Error | Count of error messages due to permissions not available to perform action received in the <code>flow_mod</code> message <code>Port_Mod_Failed</code> . |
| Emergency-Timeout | Count of error messages sent due to invalid emergency-timeout in the <code>flow-mod</code> message. |
| Bad-Command | Count of error messages sent due to unknown command. |
| Unsupported | Count of error messages sent due to unsupported action list. |
| Port-Mod-Failed | |
| Bad-Port | Count of error messages sent due to invalid port in <code>port_mod</code> message. |
| Bad-hw-addr | Count of error messages sent due to wrong hardware address specified in <code>port_mod</code> message. |

Management Processor Statistics

Table 125. Management Processor Statistics Commands

| Command Syntax and Usage |
|--|
| <pre>show mp thread</pre> <p>Displays STEM thread statistics. This command is used by Technical Support personnel.</p> <p>Command mode: All</p> |
| <pre>show mp packet counters</pre> <p>Displays packet statistics, to check for leads and load. To view a sample output and a description of the statistics, see page 213.</p> <p>Command mode: All</p> |
| <pre>show mp tcp-block</pre> <p>Displays all TCP control blocks that are in use. To view a sample output and a description of the statistics, see page 225.</p> <p>Command mode: All</p> |
| <pre>show mp udp-block</pre> <p>Displays all UDP control blocks that are in use. To view a sample output, see page 226.</p> <p>Command mode: All</p> |
| <pre>show processes cpu</pre> <p>Displays CPU utilization for periods of up to 1, 4, and 64 seconds. To view a sample output and a description of the stats, see page 226.</p> <p>Command mode: All</p> |
| <pre>show processes cpu history</pre> <p>Displays history of CPU utilization. To view a sample output, see page 229.</p> <p>Command mode: All</p> |

Packet Statistics

Table 126. Packet Statistics Commands

| Command Syntax and Usage |
|--|
| <pre>show mp packet counters</pre> <p>Displays packet statistics, to check for leads and load. To view a sample output and a description of the stats, see page 213.</p> <p>Command mode: All</p> |
| <pre>clear mp packet logs</pre> <p>Clears all CPU packet statistics and logs.</p> <p>Command mode: All</p> |

MP Packet Statistics

The following command displays MP packet statistics:

```
show mp packet counters
```

Command mode: All except User EXEC

```
CPU packet statistics at 8:21:54 Tue Jan 8, 2013
```

| Packet rate: | Incoming | Outgoing |
|--------------|----------|----------|
| ----- | ----- | ----- |
| 1-second: | 8 | 7 |
| 4-seconds: | 7 | 5 |
| 64-seconds: | 4 | 3 |

| Packet counters: | Received | Sent |
|------------------|----------|--------|
| ----- | ----- | ---- |
| Total packets: | 109056 | 148761 |
| Since bootup: | 109056 | 148768 |
| BPDUs: | 6415 | 19214 |
| Cisco packets: | 0 | 0 |
| ARP Requests: | 15 | 10061 |
| ARP Replies: | 8545 | 14 |
| LACP packets: | 3414 | 3420 |
| IPv4 packets: | 60130 | 116101 |
| ICMP Requests: | 0 | 21 |
| ICMP Replies: | 21 | 0 |
| IGMP packets: | 0 | 0 |
| PIM packets: | 0 | 0 |
| VRRP packets: | 0 | 0 |
| TCP packets: | 60088 | 116113 |
| FTP | 0 | 0 |
| HTTP | 0 | 0 |
| SSH | 3 | 3 |
| TACACS | 0 | 0 |
| TELNET | 60095 | 116145 |
| TCP other | 0 | 0 |
| UDP packets: | 24 | 9 |
| DHCP | 0 | 0 |
| NTP | 0 | 0 |
| RADIUS | 0 | 0 |
| SNMP | 0 | 0 |
| TFTP | 0 | 0 |
| UDP other | 24 | 8 |
| RIP packets: | 0 | 1 |
| OSPF packets: | 0 | 0 |
| BGP packets: | 0 | 0 |
| IPv6 packets: | 0 | 0 |
| LLDP PDUs: | 3987 | 6876 |
| FCoE FIP PDUs: | 0 | 0 |
| ECP PDUs: | 0 | 0 |
| Other: | 26549 | 0 |

...

...

Packet Buffer Statistics:

```
-----  
allocs:      265803  
frees:      265806  
failures:    0  
dropped:    0
```

small packet buffers:

```
-----  
current:      1  
max:          1024  
threshold:    128  
hi-watermark: 3  
hi-water time: 3:39:12 Tue Jan 8, 2013
```

medium packet buffers:

```
-----  
current:      0  
max:          2048  
threshold:    50  
hi-watermark: 1  
hi-water time: 3:37:12 Tue Jan 8, 2013
```

jumbo packet buffers:

```
-----  
current:      0  
max:          16  
hi-watermark: 0
```

pkt_hdr statistics:

```
-----  
current      :      0  
max          :     3072  
hi-watermark :     180
```

Router(config)#

Problem 11:

page 239/612

output information have error, suggest use the form below.

Router(config)#show mp tcp-block

All TCP allocated control blocks:

```
145c1418: 0.0.0.0          0 <=>  
          0.0.0.0          179 listen  
1458cf48: 0:0:0:0:0:0:0:0      0 <=>  
          0:0:0:0:0:0:0:0      80 listen  
1458cdf8: 0.0.0.0          0 <=>  
          0.0.0.0          80 listen  
145d3610: 192.168.0.4        4130 <=>  
          10.38.5.151          23 established  
145a7658: 0:0:0:0:0:0:0:0      0 <=>  
          0:0:0:0:0:0:0:0      23 listen  
145a74d8: 0.0.0.0          0 <=>  
          0.0.0.0          23 listen
```

Table 127. Packet Statistics

| Statistics | Description |
|-------------------------|--|
| Packet Rate | |
| 1-second | The rate of incoming and outgoing packets over 1 second. |
| 4-seconds | The rate of incoming and outgoing packets over 4 seconds. |
| 64-seconds | The rate of incoming and outgoing packets over 64 seconds. |
| Packets Counters | |
| Total packets | Total number of packets received |
| Since bootup | Total number of packets received and sent since the last switch reboot. |
| BPDUs | Total number of spanning-tree Bridge Protocol Data Units received. |
| Cisco packets | Total number of UniDirectional Link Detection (UDLD) packets and Cisco Discovery Protocol (CDP) packets received. |
| ARP packets | Total number of Address Resolution Protocol packets received. |
| IPv4 packets | Total number of IPv4 packets received and sent. Includes the following packet types: <ul style="list-style-type: none"> – IGMP – PIM – ICMP requests – ICMP replies |
| TCP packets | Total number of TCP packets received and sent. Includes the following packet types: <ul style="list-style-type: none"> – FTP – HTTP – SSH – TACACS+ – Telnet – Other |
| UDP packets | Total number of UDP packets received and sent. Includes the following packet types: <ul style="list-style-type: none"> – DHCP – NTP – RADIUS – SNMP – TFTP – Other |
| RIP packets | Total number of Routing Information Protocol packets received and sent. |

Table 127. Packet Statistics (continued)

| Statistics | Description |
|---------------------------------|---|
| OSPF packets | Total number of Open Shortest Path First packets received and sent. |
| BGP packets | Total number of Border Gateway Protocol packets received and sent. |
| IPv6 packets | Total number of IPv6 packets received. |
| LLDP PDUs | Total number of Link Layer Discovery Protocol data units received. |
| ECP PDUs | Total number of Edge Control Protocol data units received and sent. |
| MgmtSock Packets | Total number of packets received and transmitted through the management port. |
| Other | Total number of other packets received. |
| Packet Buffer Statistics | |
| allocs | Total number of packet allocations from the packet buffer pool by the TCP/IP protocol stack. |
| frees | Total number of times the packet buffers are freed (released) to the packet buffer pool by the TCP/IP protocol stack. |
| failures | Total number of packet allocation failures from the packet buffer pool by the TCP/IP protocol stack. |
| dropped | Total number of packets dropped by the packet buffer pool. |
| small packet buffers | |
| current | Total number of packet allocations with size less than 128 bytes from the packet buffer pool by the TCP/IP protocol stack. |
| max | Maximum number of small packet allocations supported. |
| threshold | Threshold value for small packet allocations, beyond which only high-priority small packets are allowed. |
| hi-watermark | The highest number of packet allocation with size less than 128 bytes from the packet buffer pool by the TCP/IP protocol stack. |
| hi-water time | Time stamp that indicates when the hi-watermark was reached. |

Table 127. Packet Statistics (continued)

| Statistics | Description |
|------------------------------|---|
| medium packet buffers | |
| current | Total number of packet allocations with size between 128 to 1536 bytes from the packet buffer pool by the TCP/IP protocol stack. |
| max | Maximum number of medium packet allocations supported. |
| threshold | Threshold value for medium packet allocations, beyond which only high-priority medium packets are allowed. |
| hi-watermark | The highest number of packet allocation with size between 128 to 1536 bytes from the packet buffer pool by the TCP/IP protocol stack. |
| hi-water time | Time stamp that indicates when the hi-watermark was reached. |
| jumbo packet buffers | |
| current | Total number of packet allocations with more than 1536 bytes from the packet buffer pool by the TCP/IP protocol stack. |
| max | Maximum number of jumbo packet allocations supported. |
| hi-watermark | The highest number of packet allocation with more than 1536 bytes from the packet buffer pool by the TCP/IP protocol stack. |
| pkt_hdr statistics | |
| current | Total number of packet allocations with more than 1536 bytes from the packet buffer pool by the TCP/IP protocol stack. |
| max | Maximum number of packet allocations with more than 1536 bytes from the packet buffer pool by the TCP/IP protocol stack. |
| hi-watermark | The highest number of packet allocation with more than 1536 bytes from the packet buffer pool by the TCP/IP protocol stack. |

Packet Statistics Log

These commands allow you to display a log of all packets received by CPU. The following table describes the Packet Statistics Log options.

Table 128. Packet Statistics Log Options

| Command Syntax and Usage |
|--|
| <pre>show mp packet log all</pre> <p>Displays all packet logs received by and sent from the CPU. To view a sample output and a description of the log entries, see "Packet Log example" on page 219.</p> |
| <pre>show mp packet log rx</pre> <p>Displays all packets logs received by the CPU.</p> |
| <pre>show mp packet log tx</pre> <p>Displays all packet logs sent from the CPU.</p> |

Packet Log example

```
358. Type: BPDU, sent 1:01:11 Tue Mar 20, 2012
    Port EXT2, VLAN 201, Length 57, Reason 0x0, Flags 0x0
    Dst MAC: 01:80:c2:00:00:00, Src MAC: 08:17:f4:a7:57:2c

357. Type: ICMP ECHO Req, sent 1:01:09 Tue Mar 20, 2012
    Port MGT1, VLAN 4095, Length 16, Reason 0x0, Flags 0x0 FromMgmtSock
    Src IP: 9.43.98.125, Dst IP: 9.43.98.254
```

Each packet log entry includes the following information:

- Entry ID
- Packet type
- Date and time
- Port number
- VLAN number
- Packet length
- Reason code
- Flags
- Source and destination address

Packet Statistics Last Packet

These commands allow you to display a specified number (*N*) of the most recent packet logs received by or sent from the CPU. The following table describes the Packet Statistics Last Packet options.

Table 129. Last Packet Options

| Command Syntax and Usage |
|---|
| <pre>show mp packet last both <I-1000></pre> <p>Displays a specified number of recent packet logs received by and sent from the CPU. To view a sample output and a description, see “Packet Log example” on page 219.</p> |
| <pre>show mp packet last rx <I-1000></pre> <p>Displays a specified number of recent packet logs received by the CPU.</p> |
| <pre>show mp packet last tx <I-1000></pre> <p>Displays a specified number of recent packet logs sent from the CPU.</p> |

Packet Statistics Dump

The following table describes the Packet Statistics Dump options.

Table 130. Packet Statistics Dump Options

| Command Syntax and Usage |
|--|
| <pre>show mp packet dump all</pre> <p>Displays all packet statistics and logs received by and sent from the CPU.</p> |
| <pre>show mp packet dump rx</pre> <p>Displays all packet statistics and logs received by the CPU.</p> |
| <pre>show mp packet dump tx</pre> <p>Displays all packet statistics and logs sent from the CPU.</p> |

Logged Packet Statistics

The following command displays logged packets that have been received or sent, based on the specified filter:

```
show mp packet parse rx|tx < parsing_option >
```

The filter options are described in [Table 131](#).

Table 131. Packet Log Parsing Options

| Command Syntax and Usage |
|--|
| <pre>show mp packet parse rx tx arp</pre> <p>Displays only ARP packets logged.</p> <p>Command mode: All</p> |
| <pre>show mp packet parse rx tx rarp</pre> <p>Displays only Reverse-ARP packets.</p> <p>Command mode: All</p> |
| <pre>show mp packet parse rx tx bpdu</pre> <p>Displays only BPDUs logged</p> <p>Command mode: All</p> |
| <pre>show mp packet parse rx tx cisco</pre> <p>Displays only Cisco packets (BPDU/CDP/UDLD) logged.</p> <p>Command mode: All</p> |
| <pre>show mp packet parse rx tx lacp</pre> <p>Displays only LACP PDUs logged.</p> <p>Command mode: All</p> |
| <pre>show mp packet parse rx tx fcoe</pre> <p>Displays only FCoE FIP PDUs logged.</p> <p>Command mode: All</p> |
| <pre>show mp packet parse rx tx ipv4</pre> <p>Displays only IPv4 packets logged.</p> <p>Command mode: All</p> |
| <pre>show mp packet parse rx tx igmp</pre> <p>Displays only IGMP packets logged.</p> <p>Command mode: All</p> |
| <pre>show mp packet parse rx tx pim</pre> <p>Displays only PIM packets logged.</p> <p>Command mode: All</p> |
| <pre>show mp packet parse rx tx icmp</pre> <p>Displays only ICMP packets logged.</p> <p>Command mode: All</p> |

Table 131. Packet Log Parsing Options (continued)

| Command Syntax and Usage |
|--|
| <pre>show mp packet parse rx tx tcp</pre> <p>Displays only TCP packets logged.</p> <p>Command mode: All</p> |
| <pre>show mp packet parse rx tx ftp</pre> <p>Displays only FTP packets logged.</p> <p>Command mode: All</p> |
| <pre>show mp packet parse rx tx http</pre> <p>Displays only HTTP packets logged.</p> <p>Command mode: All</p> |
| <pre>show mp packet parse rx tx ssh</pre> <p>Displays only SSH packets logged.</p> <p>Command mode: All</p> |
| <pre>show mp packet parse rx tx tacacs</pre> <p>Displays only TACACS packets logged.</p> <p>Command mode: All</p> |
| <pre>show mp packet parse rx tx telnet</pre> <p>Displays only TELNET packets logged.</p> <p>Command mode: All</p> |
| <pre>show mp packet parse rx tx tcpother</pre> <p>Displays only TCP other-port packets logged.</p> <p>Command mode: All</p> |
| <pre>show mp packet parse rx tx udp</pre> <p>Displays only UDP packets logged.</p> <p>Command mode: All</p> |
| <pre>show mp packet parse rx tx dhcp</pre> <p>Displays only DHCP packets logged.</p> <p>Command mode: All</p> |
| <pre>show mp packet parse rx tx ntp</pre> <p>Displays only NTP packets logged.</p> <p>Command mode: All</p> |
| <pre>show mp packet parse rx tx radius</pre> <p>Displays only RADIUS packets logged.</p> <p>Command mode: All</p> |
| <pre>show mp packet parse rx tx snmp</pre> <p>Displays only SNMP packets logged.</p> <p>Command mode: All</p> |

Table 131. Packet Log Parsing Options (continued)

| Command Syntax and Usage |
|---|
| <pre>show mp packet parse rx tx tftp</pre> <p>Displays only TFTP packets logged.</p> <p>Command mode: All</p> |
| <pre>show mp packet parse rx tx udpother</pre> <p>Displays only UDP other-port packets logged.</p> <p>Command mode: All</p> |
| <pre>show mp packet parse rx tx ipv6</pre> <p>Displays only IPv6 packets logged.</p> <p>Command mode: All</p> |
| <pre>show mp packet parse rx tx rip</pre> <p>Displays only RIP packets logged.</p> <p>Command mode: All</p> |
| <pre>show mp packet parse rx tx ospf</pre> <p>Displays only OSPF packets logged.</p> <p>Command mode: All</p> |
| <pre>show mp packet parse rx tx bgp</pre> <p>Displays only BGP packets logged.</p> <p>Command mode: All</p> |
| <pre>show mp packet parse rx tx lldp</pre> <p>Displays only LLDP PDUs logged.</p> <p>Command mode: All</p> |
| <pre>show mp packet parse rx tx vlan <VLAN_number></pre> <p>Displays only logged packets with the specified VLAN.</p> <p>Command mode: All</p> |
| <pre>show mp packet parse rx tx port <port_number></pre> <p>Displays only logged packets with the specified port.</p> <p>Command mode: All</p> |
| <pre>show mp packet parse rx tx mac <MAC_address></pre> <p>Displays only logged packets with the specified MAC address.</p> <p>Command mode: All</p> |
| <pre>show mp packet parse rx tx ip-addr <IPv4_address></pre> <p>Displays only logged packets with the specified IPv4 address.</p> <p>Command mode: All</p> |

Table 131. Packet Log Parsing Options (continued)

| Command Syntax and Usage |
|--|
| <pre>show mp packet parse rx tx other</pre> <p>Displays logs of all packets not explicitly selectable.</p> <p>Command mode: All</p> |
| <pre>show mp packet parse rx tx raw</pre> <p>Displays raw packet buffer in addition to headers.</p> <p>Command mode: All</p> |

TCP Statistics

The following command displays TCP statistics:

```
show mp tcp-block
```

Command mode: All

```

Data Ports:
-----
All TCP allocated control blocks:
14835bd8:  0.0.0.0                0 <=>
           172.31.38.107          80 listen MGT up
147c6eb8:  0:0:0:0:0:0:0:0              0 <=>
           0:0:0:0:0:0:0:0          80 listen
147c6d68:  0.0.0.0                0 <=>
           0.0.0.0                80 listen
14823918:  172.31.37.42             55866 <=>
           172.31.38.107          23 established 0 ??
11af2394:  0.0.0.0                0 <=>
           172.31.38.107          23 listen MGT up
147e6808:  0.0.0.0                0 <=>
           0.0.0.0                23 listen
147e66b8:  0:0:0:0:0:0:0:0              0 <=>
           0:0:0:0:0:0:0:0          23 listen
147e6568:  0.0.0.0                0 <=>
           0.0.0.0                23 listen

Mgmt Ports:
-----
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp      0      0 172.31.38.107:http     *:*                     LISTEN
tcp      0      0 172.31.38.107:telnet  *:*                     LISTEN
tcp      0      0 *:11000                 *:*                     LISTEN
tcp      0  1274 172.31.38.107:telnet  172.31.37.42:55866    ESTABLISHED

```

Table 132. MP Specified TCP Statistics

| Statistics | Description |
|----------------|------------------------|
| 14835bd8 | Memory |
| 0.0.0.0 | Destination IP address |
| 0 | Destination port |
| 172.31.38.107 | Source IP |
| 80 | Source port |
| listen MGT1 up | State |

UDP Statistics

The following command displays UDP statistics:

```
show mp udp-block
```

Command mode: All except User EXEC

```

Data Ports:
-----
All UDP allocated control blocks:
  68: listen
 161: listen
 500: listen
 546: listen

Mgmt Ports:
-----
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
udp      0      0 9.43.95.121:snmp       *.*
0.0.0.0          0 <=> 9.43.95.121          161 accept MGT1 up
  
```

CPU Statistics

The following commands display CPU utilization statistics:

```
show mp cpu
```

Command mode: All

| CPU utilization | Highest | Thread | Time |
|-------------------|---------|--------|-------------------------------------|
| cpuUtil1Second: | 3% | 83% | 58 (I2C) 12:02:14 Fri Oct 14, 2011 |
| cpuUtil4Seconds: | 5% | | |
| cpuUtil64Seconds: | 5% | | |

Table 133. CPU Statistics

| Statistics | Description |
|------------------|--|
| cpuUtil1Second | The use of MP CPU over 1 second. It shows the percentage, highest rate, thread, and time the highest utilization occurred. |
| cpuUtil4Seconds | The use of MP CPU over 4 seconds. It shows the percentage. |
| cpuUtil64Seconds | The use of MP CPU over 64 seconds. It shows the percentage. |
| Highest | The highest percent of CPU use. |

Table 133. CPU Statistics

| Statistics | Description |
|------------|---|
| Thread | The thread ID and name of the thread that caused the highest CPU use. |
| Time | The time when the highest CPU use was reached. |

show processes cpu

Command mode: All

```

-----
CPU Utilization at  8:25:55 Tue Jan  8, 2013

Total CPU Utilization: For 1 second: 2.92%
                      For 5 second: 3.38%
                      For 1 minute: 7.88%
                      For 5 minute: 8.93%

Highest CPU Utilization: thread  2 (STP ) at  6:44:56 Tue Jan  8, 2013

-----
Thread  Thread      Utilization      Status
  ID    Name         1sec    5sec    1Min    5Min
-----
  1     STEM      0.00%   0.00%   0.00%   0.00%   idle
  2     STP        0.00%   0.05%   0.10%   0.10%   idle
  3     MFDB       0.00%   0.00%   5.06%   5.22%   idle
  4     TND        0.00%   0.00%   0.00%   0.00%   idle
  5     CONS       0.00%   0.00%   0.00%   0.15%   suspended
  6     TNET       0.11%   0.58%   0.17%   0.27%   running
  7     TNET       0.00%   0.00%   0.00%   0.00%   idle
  8     TNET       0.00%   0.00%   0.00%   0.00%   idle
  9     TNET       0.00%   0.00%   0.00%   0.00%   idle
 10     LOG        0.00%   0.00%   0.00%   0.00%   idle
 11     TRAP       0.00%   0.00%   0.00%   0.00%   idle
 13     NTP        0.00%   0.00%   0.00%   0.00%   idle
 14     IP         0.04%   0.04%   0.06%   0.06%   idle
 17     IP         0.01%   0.08%   0.04%   0.04%   idle
 18     RIP        0.00%   0.00%   0.00%   0.00%   idle
 19     AGR        0.00%   0.00%   0.00%   0.00%   idle
 20     EPI       0.16%   0.27%   0.12%   0.10%   runnable
 22     PORT       0.00%   0.00%   0.00%   0.00%   idle
 24     BGP       0.18%   0.04%   0.00%   0.00%   idle
 32     SCAN       0.00%   0.00%   0.00%   0.00%   idle
 34     OSPF      0.20%   0.04%   0.02%   0.01%   idle
 36     SNMP       0.00%   0.00%   0.00%   0.00%   idle
 37     SNMP       0.00%   0.00%   0.00%   0.00%   idle
 38     SNMP       0.00%   0.00%   0.00%   0.00%   idle
 40     SSHD      0.00%   0.00%   0.00%   0.00%   idle
...
 120    VDPT      0.00%   0.00%   0.00%   0.00%   idle
 124    HIST      0.00%   0.00%   0.00%   0.00%   runnable
 128    NORM      0.00%   0.00%   0.00%   0.00%   idle
 129    NORM      0.00%   0.00%   0.00%   0.00%   idle
 130    DONE      0.00%   0.00%   0.00%   0.00%   idle
-----

```

Table 134. CPU Statistics

| Statistics | Description |
|-------------------|--|
| Thread ID | The thread ID number. |
| Thread Name | The name of the thread. |
| 1sec | The percent of CPU use over 1 second. |
| 5sec | The percent of CPU use over 5 seconds. |
| 1Min | The percent of CPU use over 1 minute. |
| 5Min | The percent of CPU use over 5 minutes. |
| Status | The status of the process. |

CPU Statistics History

The following command display a history of CPU use statistics:

```
show processes cpu history
```

Command mode: All

```
-----  
CPU Utilization History  
-----  
 17 (IP ) 98% at 22:17:24 Mon Feb 20, 2012  
 59 (LACP) 9% at 22:17:33 Mon Feb 20, 2012  
110 (ETMR) 12% at 22:17:34 Mon Feb 20, 2012  
110 (ETMR) 12% at 22:17:36 Mon Feb 20, 2012  
110 (ETMR) 12% at 22:17:40 Mon Feb 20, 2012  
110 (ETMR) 12% at 22:17:45 Mon Feb 20, 2012  
110 (ETMR) 17% at 22:17:47 Mon Feb 20, 2012  
110 (ETMR) 18% at 22:17:49 Mon Feb 20, 2012  
110 (ETMR) 25% at 22:20:28 Mon Feb 20, 2012  
110 (ETMR) 26% at 22:39:08 Mon Feb 20, 2012  
 37 (SNMP) 28% at 22:46:20 Mon Feb 20, 2012  
 94 (PROX) 57% at 23:29:36 Mon Feb 20, 2012  
 94 (PROX) 63% at 23:29:37 Mon Feb 20, 2012  
 94 (PROX) 63% at 23:29:39 Mon Feb 20, 2012  
 58 (I2C ) 64% at 16:21:54 Tue Feb 21, 2012  
 5 (CONS) 86% at 18:41:54 Tue Feb 21, 2012  
 58 (I2C ) 88% at 18:41:55 Tue Feb 21, 2012  
 58 (I2C ) 88% at 21:29:41 Sat Feb 25, 2012  
 58 (I2C ) 98% at 12:04:59 Tue Feb 28, 2012  
 58 (I2C ) 100% at 11:31:32 Sat Mar 10, 2012  
-----
```

Access Control List Statistics

The following commands display and change ACL statistics.

Table 135. ACL Statistics Commands

| Command Syntax and Usage |
|---|
| <pre>show access-control list <ACL number> counters</pre> <p>Displays the Access Control List Statistics for a specific ACL.</p> <p>Command mode: All</p> |
| <pre>show access-control list6 <ACL number> counters</pre> <p>Displays the IPv6 ACL statistics for a specific ACL.</p> <p>Command mode: All</p> |
| <pre>show access-control macl <MACL number> counters</pre> <p>Displays the ACL statistics for a specific management ACL (MACL).</p> <p>Command mode: All</p> |
| <pre>show access-control counters</pre> <p>Displays all ACL statistics.</p> <p>Command mode: All</p> |
| <pre>clear access-control list {<ACL number> all} counters</pre> <p>Clears ACL statistics.</p> <p>Command mode: Privileged EXEC</p> |
| <pre>clear access-control list6 {<ACL number> all}</pre> <p>Clears IPv6 ACL statistics.</p> <p>Command mode: Privileged EXEC</p> |
| <pre>show access-control meter <meter number> counters</pre> <p>Displays ACL meter statistics.</p> <p>Command mode: All</p> |
| <pre>clear access-control meter <meter number> counters</pre> <p>Clears ACL meter statistics.</p> <p>Command mode: Privileged EXEC</p> |

ACL Statistics

The following command displays ACL statistics.

```
show access-control counters
```

Command mode: All

| | |
|-----------------|----------|
| Hits for ACL 1: | 26057515 |
| Hits for ACL 2: | 26057497 |

VMAP Statistics

The following command displays VLAN Map statistics.

```
show access-control vmap {<vmap number>} counters
```

Command mode: All

| | |
|------------------|-------|
| Hits for VMAP 1: | 57515 |
|------------------|-------|

Fibre Channel over Ethernet Statistics

The following command displays Fibre Channel over Ethernet (FCoE) statistics:

```
show fcoe counters
```

Command mode: All

| | | | |
|------------------|----|--------------|----|
| FCOE statistics: | | | |
| FCFAdded: | 5 | FCFRemoved: | 1 |
| FCOEAdded: | 81 | FCOERemoved: | 24 |

Fibre Channel over Ethernet (FCoE) statistics are described in the following table:

Table 136. FCoE Statistics (/stats/fcoe)

| Statistic | Description |
|-------------|--|
| FCFAdded | Total number of FCoE Forwarders (FCF) added. |
| FCFRemoved | Total number of FCoE Forwarders (FCF) removed. |
| FCOEAdded | Total number of FCoE connections added. |
| FCOERemoved | Total number of FCoE connections removed. |

The total can accumulate over several FCoE sessions, until the statistics are cleared.

The following command clears Fibre Channel over Ethernet (FCoE) statistics:

```
clear fcoe counters
```

Command mode: All

ACL Meter Statistics

This option displays ACL meter statistics.

```
show access-control meter <meter number> counters
```

Command mode: All

```
Out of profile hits for Meter 1, Port EXT1: 0  
Out of profile hits for Meter 2, Port EXT1: 0
```

SNMP Statistics

The following command displays SNMP statistics:

```
show snmp-server counters
```

Command mode: All except User EXEC

| | | | |
|----------------------|--------|----------------------|--------|
| SNMP statistics: | | | |
| snmpInPkts: | 150097 | snmpInBadVersions: | 0 |
| snmpInBadC'tyNames: | 0 | snmpInBadC'tyUses: | 0 |
| snmpInASNParseErrs: | 0 | snmpEnableAuthTraps: | 0 |
| snmpOutPkts: | 150097 | snmpInBadTypes: | 0 |
| snmpInTooBig: | 0 | snmpInNoSuchNames: | 0 |
| snmpInBadValues: | 0 | snmpInReadOnlys: | 0 |
| snmpInGenErrs: | 0 | snmpInTotalReqVars: | 798464 |
| snmpInTotalSetVars: | 2731 | snmpInGetRequests: | 17593 |
| snmpInGetNexts: | 131389 | snmpInSetRequests: | 615 |
| snmpInGetResponses: | 0 | snmpInTraps: | 0 |
| snmpOutTooBig: | 0 | snmpOutNoSuchNames: | 1 |
| snmpOutBadValues: | 0 | snmpOutReadOnlys: | 0 |
| snmpOutGenErrs: | 1 | snmpOutGetRequests: | 0 |
| snmpOutGetNexts: | 0 | snmpOutSetRequests: | 0 |
| snmpOutGetResponses: | 150093 | snmpOutTraps: | 4 |
| snmpSilentDrops: | 0 | snmpProxyDrops: | 0 |

Table 137. SNMP Statistics

| Statistic | Description |
|--------------------|---|
| snmpInPkts | The total number of Messages delivered to the SNMP entity from the transport service. |
| snmpInBadVersions | The total number of SNMP Messages, which were delivered to the SNMP protocol entity and were for an unsupported SNMP version. |
| snmpInBadC'tyNames | The total number of SNMP Messages delivered to the SNMP entity which used an SNMP community name not known to the said entity (the switch). |
| snmpInBadC'tyUses | The total number of SNMP Messages delivered to the SNMP protocol entity which represented an SNMP operation which was not allowed by the SNMP community named in the Message. |

Table 137. SNMP Statistics (continued)

| Statistic | Description |
|---------------------|---|
| snmpInASNParseErrs | <p>The total number of ASN.1 or BER errors encountered by the SNMP protocol entity when decoding SNMP Messages received.</p> <p>Note: OSI's method of specifying abstract objects is called ASN.1 (Abstract Syntax Notation One, defined in X.208), and one set of rules for representing such objects as strings of ones and zeros is called the BER (Basic Encoding Rules, defined in X.209). ASN.1 is a flexible notation that allows one to define a variety of data types, from simple types such as integers and bit strings to structured types such as sets and sequences. BER describes how to represent or encode values of each ASN.1 type as a string of eight-bit octets.</p> |
| snmpEnableAuthTraps | An object to enable or disable the authentication traps generated by this entity (the switch). |
| snmpOutPkts | The total number of SNMP Messages which were passed from the SNMP protocol entity to the transport service. |
| snmpInBadTypes | The total number of SNMP Messages which failed ASN parsing. |
| snmpInTooBig | The total number of SNMP Protocol Data Units (PDUs) which were delivered to the SNMP protocol entity and for which the value of the error-status field is <i>too big</i> . |
| snmpInNoSuchNames | The total number of SNMP Protocol Data Units (PDUs) which were delivered to the SNMP protocol entity and for which the value of the error-status field is <i>noSuchName</i> . |
| snmpInBadValues | The total number of SNMP Protocol Data Units (PDUs) which were delivered to the SNMP protocol entity and for which the value of the error-status field is <i>badValue</i> . |
| snmpInReadOnly | The total number of valid SNMP Protocol Data Units (PDUs), which were delivered to the SNMP protocol entity and for which the value of the error-status field is <i>'read-Only'</i> . It should be noted that it is a protocol error to generate an SNMP PDU, which contains the value <i>'read-Only'</i> in the error-status field. As such, this object is provided as a means of detecting incorrect implementations of the SNMP. |
| snmpInGenErrs | The total number of SNMP Protocol Data Units (PDUs), which were delivered to the SNMP protocol entity and for which the value of the error-status field is <i>genErr</i> . |

Table 137. SNMP Statistics (continued)

| Statistic | Description |
|--------------------|---|
| snmpInTotalReqVars | The total number of MIB objects which have been retrieved successfully by the SNMP protocol entity as a result of receiving valid SNMP Get-Request and Get-Next Protocol Data Units (PDUs). |
| snmpInTotalSetVars | The total number of MIB objects, which have been altered successfully by the SNMP protocol entity as a result of receiving valid SNMP Set-Request Protocol Data Units (PDUs). |
| snmpInGetRequests | The total number of SNMP Get-Request Protocol Data Units (PDUs), which have been accepted and processed by the SNMP protocol entity. |
| snmpInGetNexts | The total number of SNMP Get-Next Protocol Data Units (PDUs), which have been accepted and processed by the SNMP protocol entity. |
| snmpInSetRequests | The total number of SNMP Set-Request Protocol Data Units (PDUs), which have been accepted and processed by the SNMP protocol entity. |
| snmpInGetResponses | The total number of SNMP Get-Response Protocol Data Units (PDUs), which have been accepted and processed by the SNMP protocol entity. |
| snmpInTraps | The total number of SNMP Trap Protocol Data Units (PDUs), which have been accepted and processed by the SNMP protocol entity. |
| snmpOutTooBig | The total number of SNMP Protocol Data Units (PDUs), which were generated by the SNMP protocol entity and for which the value of the error-status field is <i>too big</i> . |
| snmpOutNoSuchNames | The total number of SNMP Protocol Data Units (PDUs), which were generated by the SNMP protocol entity and for which the value of the error-status is <i>noSuchName</i> . |
| snmpOutBadValues | The total number of SNMP Protocol Data Units (PDUs), which were generated by the SNMP protocol entity and for which the value of the error-status field is <i>badValue</i> . |
| snmpOutReadOnly | Not in use. |
| snmpOutGenErrs | The total number of SNMP Protocol Data Units (PDUs), which were generated by the SNMP protocol entity and for which the value of the error-status field is <i>genErr</i> . |
| snmpOutGetRequests | The total number of SNMP Get-Request Protocol Data Units (PDUs), which have been generated by the SNMP protocol entity. |

Table 137. SNMP Statistics (continued)

| Statistic | Description |
|---------------------|--|
| snmpOutGetNexts | The total number of SNMP Get-Next Protocol Data Units (PDUs), which have been generated by the SNMP protocol entity. |
| snmpOutSetRequests | The total number of SNMP Set-Request Protocol Data Units (PDUs), which have been generated by the SNMP protocol entity. |
| snmpOutGetResponses | The total number of SNMP Get-Response Protocol Data Units (PDUs), which have been generated by the SNMP protocol entity. |
| snmpOutTraps | The total number of SNMP Trap Protocol Data Units (PDUs), which have been generated by the SNMP protocol entity. |
| snmpSilentDrops | The total number of <code>GetRequest</code> -PDUs, <code>GetNextRequest</code> -PDUs, <code>GetBulkRequest</code> -PDUs, <code>SetRequest</code> -PDUs, and <code>InformRequest</code> -PDUs delivered to the SNMPv2 entity which were silently dropped because the size of a reply containing an alternate Response-PDU with an empty variable bindings field was greater than either a local constraint or the maximum message size associated with the originator of the request. |
| snmpProxyDrops | The total number of <code>GetRequest</code> -PDUs, <code>GetNextRequest</code> -PDUs, <code>GetBulkRequest</code> -PDUs, <code>SetRequest</code> -PDUs, and <code>InformRequest</code> -PDUs delivered to the SNMP entity which were silently dropped because the transmission of the message to a proxy target failed in a manner such that no Response-PDU could be returned. |

NTP Statistics

Networking OS uses NTP (Network Timing Protocol) version 3 to synchronize the switch's internal clock with an atomic time calibrated NTP server. With NTP enabled, the switch can accurately update its internal clock to be consistent with other devices on the network and generates accurate syslogs.

The following command displays NTP statistics:

```
show ntp counters
```

Command mode: All

| | |
|--|----|
| NTP statistics: | |
| Primary Server: | |
| Requests Sent: | 17 |
| Responses Received: | 17 |
| Updates: | 1 |
| Secondary Server: | |
| Requests Sent: | 0 |
| Responses Received: | 0 |
| Updates: | 0 |
| Last update based on response from primary/secondary server. | |
| Last update time: 18:04:16 Tue Jul 13, 2010 | |
| Current system time: 18:55:49 Tue Jul 13, 2010 | |

Table 138. NTP Statistics

| Field | Description |
|---|---|
| Primary Server | <ul style="list-style-type: none">• Requests Sent: The total number of NTP requests the switch sent to the primary NTP server to synchronize time.• Responses Received: The total number of NTP responses received from the primary NTP server.• Updates: The total number of times the switch updated its time based on the NTP responses received from the primary NTP server. |
| Secondary Server | <ul style="list-style-type: none">• Requests Sent: The total number of NTP requests the switch sent to the secondary NTP server to synchronize time.• Responses Received: The total number of NTP responses received from the secondary NTP server.• Updates: The total number of times the switch updated its time based on the NTP responses received from the secondary NTP server. |
| Last update based on response from primary server | Last update of time on the switch based on either primary or secondary NTP response received. |

Table 138. NTP Statistics (continued)

| Field | Description |
|---------------------|--|
| Last update time | The time stamp showing the time when the switch was last updated. |
| Current system time | The switch system time when the following command was issued: show ntp counters |

The following command displays information about NTP associated peers:

```
show ntp associations
```

Command mode: All

| | | | | |
|---------------------|--------------|----|---------|-----------|
| address | ref clock | st | when(s) | offset(s) |
| *12.200.151.18 | 198.72.72.10 | 3 | 35316 | -2 |
| *synced, #unsynched | | | | |

Table 139. NTP Associations

| Field | Description |
|-----------|--|
| address | Peer address |
| ref clock | Peer reference clock address |
| st | Peer stratum |
| when(s) | Time in seconds since the latest NTP packet was received from the peer |
| offset(s) | Offset in seconds between the peer clock and local clock |

PTP Statistics

Table 140. Precision Time Protocol Statistics Commands

| |
|---|
| Command Syntax and Usage |
| <pre>show ptp counters</pre> <p>Displays Precision Time Protocol statistics.</p> <p>Command mode: All</p> |
| <pre>show interface port <port alias or number> ptp-counters</pre> <p>Displays Precision Time Protocol statistics for the port.</p> <p>Command mode: All</p> |
| <pre>clear ptp counters</pre> <p>Resets PTP packet counters.</p> <p>Command mode: Privileged EXEC</p> |

Use the following command to display Precision Time Protocol traffic statistics:

```
show ptp counters
```

Command mode: All

| | |
|-----------------------------------|---|
| Precision time protocol counters: | |
| +-----+ | |
| Received Announce messages: | 0 |
| Received Sync messages: | 0 |
| Received Follow-Up messages: | 0 |
| Received Delay-Request messages: | 0 |
| Received Delay-Response messages: | 0 |
| +-----+ | |
| Sent Announce messages: | 0 |
| Sent Sync messages: | 0 |
| Sent Follow-Up messages: | 0 |
| Sent Delay-Request messages: | 0 |
| Sent Delay-Response messages: | 0 |
| +-----+ | |

PTP statistics include the following:

- total number of Announce messages transmitted and received.
- total number of Sync transmitted and received.
- total number of Follow_Up messages transmitted and received
- total number of Delay_Req messages transmitted and received
- total number of Delay_Resp messages transmitted and received

SLP Statistics

Table 141. SLP Statistics Commands

| Command Syntax and Usage |
|--|
| <pre>show ip slp counter</pre> <p>Displays SLP packet counters.</p> <p>Command mode: All</p> |
| <pre>clear ip slp counter</pre> <p>Clears SLP packet counters.</p> <p>Command mode: Privileged EXEC</p> |

Use the following command to display SLP packet counters:

```
show ip slp counter
```

Command mode: All

```
SLP Send Counters:
  SLP DAAdvert           : 0
  SLP SrvRqst           : 0
  SLP SrvRply           : 0
  SLP SrvAck            : 0
  SLP AttrRqst          : 0
  SLP AttrRply          : 0
  SLP SrvTypeRqst       : 0
  SLP SrvReg            : 0
  SLP SrvDeReg          : 0
  SLP SrvTypeRply       : 0
  SLP SAAdvert          : 0
  SLP Unknown           : 0

SLP Receive Counters:
  SLP DAAdvert           : 0
  SLP SrvRqst           : 0
  SLP SrvRply           : 0
  SLP SrvAck            : 0
  SLP AttrRqst          : 0
  SLP AttrRply          : 0
  SLP SrvTypeRqst       : 0
  SLP SrvReg            : 0
  SLP SrvDeReg          : 0
  SLP SrvTypeRply       : 0
  SLP SAAdvert          : 0
  SLP Dropped            : 0
    Incorect pkt/dest    : 0
    Scopes mismatch      : 0
    Others                : 0
```

Statistics Dump

The following command dumps switch statistics:

```
show counters
```

Use the dump command to dump all switch statistics (40K or more, depending on your configuration). This data can be used to tune or debug switch performance.

If you want to capture dump data to a file, set your communication software on your workstation to capture session data prior to issuing the dump command.

Chapter 4. Configuration Commands

This chapter discusses how to use the Command Line Interface (CLI) for making, viewing, and saving switch configuration changes. Many of the commands, although not new, display more or different information than in the previous version. Important differences are called out in the text.

Table 142. General Configuration Commands

| Command Syntax and Usage |
|---|
| <pre>show running-config</pre> <p>Dumps current configuration to a script file.</p> <p>Command mode: Privileged EXEC</p> <p>For details, see page 500.</p> |
| <pre>show running-config diff</pre> <p>Displays running configuration changes that have been applied but not saved to flash memory.</p> <p>Command mode: Privileged EXEC</p> |
| <pre>copy running-config backup-config</pre> <p>Copy the current (running) configuration from switch memory to the backup-config partition.</p> <p>Command mode: Privileged EXEC</p> <p>For details, see page 501.</p> |
| <pre>copy running-config startup-config</pre> <p>Copy the current (running) configuration from switch memory to the startup-config partition.</p> <p>Command mode: Privileged EXEC</p> |
| <pre>copy running-config {ftp tftp sftp} [data-port extm-port mgt-port]</pre> <p>Backs up current configuration to a file on the selected FTP/TFTP/SFTP server. Select a management port, or press Enter to use the default (management) port.</p> <p>Command mode: Privileged EXEC</p> |

Table 142. General Configuration Commands

| Command Syntax and Usage |
|--|
| <pre>copy {ftp tftp sftp} running-config [data-port extm-port mgt-port]</pre> <p>Restores current configuration from a FTP/TFTP/SFTP server. Select a management port, or press Enter to use the default (management) port.</p> <p>Command mode: Privileged EXEC</p> <p>For details, see page 502.</p> |
| <pre>copy {tftp sftp} {ca-cert host-key host-cert}</pre> <p>Import interface used by NIST certified test laboratories for USGv6 (NIST SP 500-267) certification purposes. Required for RSA digital signature authentication verification during IKEv2 interoperability testing. Uses TFTP or SFTP to import:</p> <ul style="list-style-type: none">– ca-cert: Certificate Authority root certificate– host-key: host private key– host-cert: host public key <p>Command mode: Privileged EXEC</p> |

Viewing and Saving Changes

As you use the configuration commands to set switch parameters, the changes you make take effect immediately. You do not need to apply them. Configuration changes are lost the next time the switch boots, unless you save the changes.

You can view all running configuration changes that have been applied but not saved to flash memory using the `show running-config diff` command in Privileged EXEC mode.

Note: Some operations can override the settings of the Configuration commands. Therefore, settings you view using the Configuration commands (for example, port status) might differ from run-time information that you view using the Information commands. The Information commands display current run-time information of switch parameters.

Saving the Configuration

You must save configuration settings to flash memory, so the EN4093 and EN4093R reloads the settings after a reset.

Note: If you do not save the changes, they will be lost the next time the system is rebooted.

To save the new configuration, enter the following command:

```
Router# copy running-config startup-config
```

When you save configuration changes, the changes are saved to the *active* configuration block. For instructions on selecting the configuration to run at the next system reset, see [“Selecting a Configuration Block” on page 525](#).

System Configuration

These commands provide configuration of switch management parameters such as user and administrator privilege mode passwords, Web-based management settings, and management access lists.

Table 143. System Configuration Commands

| Command Syntax and Usage |
|---|
| <pre>system date <yyy> <mm> <dd></pre> <p>Prompts the user for the system date. The date retains its value when the switch is reset.</p> <p>Command mode: Global configuration</p> |
| <pre>system time <hh>:<mm>:<ss></pre> <p>Configures the system time using a 24-hour clock format. The time retains its value when the switch is reset.</p> <p>Command mode: Global configuration</p> |
| <pre>system timezone</pre> <p>Configures the time zone where the switch resides. You are prompted to select your location (continent, country, region) by the timezone wizard. Once a region is selected, the switch updates the time to reflect local changes to Daylight Saving Time, etc.</p> <p>Command mode: Global configuration</p> |
| <pre>[no] system daylight</pre> <p>Disables or enables daylight saving time in the system clock. When enabled, the switch will add an extra hour to the system clock so that it is consistent with the local clock. By default, this option is disabled.</p> <p>Command mode: Global configuration</p> |
| <pre>terminal-length <0-300></pre> <p>Configures the number of lines per screen displayed in the CLI for the current session. A value of 0 disables paging. By default, it is set to the corresponding <code>line vty length</code> or <code>line console length</code> value in effect at login.</p> <p>Command mode: All</p> |
| <pre>line console length <0-300></pre> <p>Configures the number of lines per screen displayed in the CLI by default for console sessions. Setting it to 0 disables paging. The default value is 28.</p> <p>Command mode: Global configuration</p> |
| <pre>no line console</pre> <p>Sets <code>line console length</code> to the default value of 28.</p> <p>Command mode: Global configuration</p> |
| <pre>line vty length <0-300></pre> <p>Sets the default number of lines per screen displayed for Telnet and SSH sessions. A value of 0 disables paging. The default value is 28.</p> <p>Command mode: Global configuration</p> |

Table 143. System Configuration Commands (continued)

| Command Syntax and Usage | |
|--|--|
| <code>no line vty</code> | <p>Sets <code>line vty length</code> to the default value of 28.</p> <p>Command mode: Global configuration</p> |
| <code>system idle <0-60></code> | <p>Sets the idle timeout for CLI sessions in minutes. The default value is 10 minutes. A value of 0 disables system idle.</p> <p>Command mode: Global configuration</p> |
| <code>system linkscan {fast normal slow}</code> | <p>Configures the link scan interval used to poll the status of ports.</p> <p>Command mode: Global configuration</p> |
| <code>system notice <maximum 1024 character multi-line login notice> <'.' to end></code> | <p>Displays a login notice immediately before the “Enter password:” prompt. This notice can contain up to 1024 characters and new lines.</p> <p>Command mode: Global configuration</p> |
| <code>[no] banner <1-80 characters></code> | <p>Configures a login banner of up to 80 characters. When a user or administrator logs into the switch, the login banner is displayed. It is also displayed as part of the output from the <code>show sys-info</code> command.</p> <p>Command mode: Global configuration</p> |
| <code>[no] hostname <character string></code> | <p>Enables or disables displaying of the host name (system administrator’s name) in the Command Line Interface (CLI).</p> <p>Command mode: Global configuration</p> |
| <code>[no] system dhcp [extm mgt]</code> | <p>Enables or disables Dynamic Host Control Protocol for setting the IP address on the selected interface. When enabled, the IP address obtained from the DHCP server overrides the static IP address. The default setting is <code>enabled</code>.</p> <p>Command mode: Global configuration</p> |
| <code>[no] system reset-control</code> | <p>Enables or disables the reset control flag. When enabled, the switch continues to function after a crash of the main processor, using the last known Layer 2/3 information.</p> <p>Command mode: Global configuration</p> |

Table 143. System Configuration Commands (continued)

| Command Syntax and Usage |
|--|
| <code>[no] system packet-logging</code> Enables or disables logging of packets that come to the CPU. The default setting is enabled. Command mode: Global configuration |
| <code>show system</code> Displays the current system parameters. Command mode: All |

System Error Disable and Recovery Configuration

The Error Disable and Recovery feature allows the switch to automatically disable a port if an error condition is detected on the port. The port remains in the error-disabled state until it is re-enabled manually, or re-enabled automatically by the switch after a timeout period has elapsed. The error-disabled state of a port does not persist across a system reboot.

Table 144. Error Disable Configuration Commands

| Command Syntax and Usage |
|---|
| <pre>errdisable timeout <30 - 86400></pre> <p>Configures the error-recovery timeout, in seconds. After the timer expires, the switch attempts to re-enable the port. The default value is 300.</p> <p>Note: When you change the timeout value, all current error-recovery timers are reset.</p> <p>Command mode: Global configuration</p> |
| <pre>errdisable recovery</pre> <p>Globally enables automatic error-recovery for error-disabled ports. The default setting is disabled.</p> <p>Note: Each port must have error-recovery enabled to participate in automatic error recovery.</p> <p>Command mode: Global configuration</p> |
| <pre>no errdisable recovery</pre> <p>Globally disables error-recovery for error-disabled ports; <code>errdisable recovery</code> is disabled globally by default.</p> <p>Command mode: All</p> |
| <pre>show errdisable</pre> <p>Displays the current system Error Disable configuration.</p> <p>Command mode: All</p> |

System Host Log Configuration

Table 145. Host Log Configuration Commands

| Command Syntax and Usage | |
|---|--|
| [no] logging host <1-2> address <IP address> [data-port extm-port mgt-port] | Sets the IPv4 address of the first or second syslog host. Command mode: Global configuration |
| [no] logging host <1-2> address6 <IP address> [data-port extm-port mgt-port] | Sets the IPv6 address of the first or second syslog host. Command mode: Global configuration |
| logging host <1-2> severity <0-7> | This option sets the severity level of the first or second syslog host displayed. The default is 7, which means log all severity levels. Command mode: Global configuration |
| logging host <1-2> facility <0-7> | This option sets the facility level of the first or second syslog host displayed. The default is 0. Command mode: Global configuration |
| logging source-interface <1-5> | Sets the loopback interface number for syslogs. Command mode: Global configuration |
| logging console | Enables delivering syslog messages to the console. It is enabled by default. Command mode: Global configuration |
| no logging console | Disables delivering syslog messages to the console. When necessary, disabling <code>console</code> ensures the switch is not affected by syslog messages. It is enabled by default. Command mode: Global configuration |

Table 145. Host Log Configuration Commands

| Command Syntax and Usage | |
|---|---|
| <pre>[no] logging synchronous [level <0-7> all]</pre> | <p>Enables or disables synchronous logging for unsolicited messages. When enabled, if unsolicited messages occur while solicited output display is in progress, the unsolicited messages are buffered and then output separately from the solicited messages. The buffer can store up to 20 unsolicited messages, after which unsolicited messages are discarded. When disabled, unsolicited and solicited messages are logged together.</p> <p>The <code>level</code> parameter sets a minimum severity level (lower or equal numeric values) for unsolicited messages to be displayed asynchronously; <code>all</code> displays all unsolicited messages asynchronously, regardless of severity level. The default setting is 2.</p> <p>Command mode: Global configuration</p> |
| <pre>logging console severity <0-7></pre> | <p>Sets the severity level of system log messages to display via the console, Telnet, and SSH. The system displays only messages with the selected severity level and above. For example, if you set the console severity to 2, only messages with severity level of 1 and 2 are displayed. The default is 7, which means log all severity levels.</p> <p>Command mode: Global configuration</p> |
| <pre>no logging console severity</pre> | <p>Disables delivering syslog messages to the console based on severity.</p> <p>Command mode: Global configuration</p> |
| <pre>[no] logging buffer severity <0-7></pre> | <p>Sets the severity level of system log messages that are written to flash buffer. The system saves only messages with the selected severity level and above. For example, if you set the buffer severity to 2, only messages with severity level of 1 and 2 are saved.</p> <p>Command mode: Global configuration</p> |
| <pre>[no] logging log [<feature>]</pre> | <p>Displays a list of features for which syslog messages can be generated. You can choose to enable/disable specific features (such as <code>vlangs</code>, <code>stg</code>, or <code>ssh</code>), or enable/disable syslog on all available features.</p> <p>Command mode: Global configuration</p> |
| <pre>show logging [severity <severity level>] [reverse]</pre> | <p>Displays the current syslog settings, followed by the most recent 2000 syslog messages, as displayed by the <code>show logging messages</code> command. For details, see page 27.</p> <p>The <code>reverse</code> option displays the output in reverse order, from the newest entry to the oldest.</p> <p>Command mode: All</p> |

SSH Server Configuration

For the EN4093 and EN4093R 10Gb Scalable Switch, these commands enable Secure Shell access from any SSH client.

Table 146. SSH Server Configuration Commands

| Command Syntax and Usage |
|---|
| <pre>ssh scp-password</pre> <p>Set the administration password for SCP access. Command mode: Global configuration</p> |
| <pre>ssh generate-host-key</pre> <p>Generate the RSA host key. Command mode: Global configuration</p> |
| <pre>ssh port <TCP port number></pre> <p>Sets the SSH server port number. Command mode: Global configuration</p> |
| <pre>ssh scp-enable</pre> <p>Enables the SCP apply and save. Command mode: Global configuration</p> |
| <pre>no ssh scp-enable</pre> <p>Disables the SCP apply and save. Command mode: Global configuration</p> |
| <pre>ssh enable</pre> <p>Enables the SSH server. Command mode: Global configuration</p> |
| <pre>no ssh enable</pre> <p>Disables the SSH server. Command mode: Global configuration</p> |
| <pre>show ssh</pre> <p>Displays the current SSH server configuration. Command mode: All</p> |

RADIUS Server Configuration

Table 147. RADIUS Server Configuration Commands

| Command Syntax and Usage | |
|---|---|
| [no] radius-server primary-host <IP address> | <p>Sets the primary RADIUS server address.</p> <p>Command mode: Global configuration</p> |
| [no] radius-server secondary-host <IP address> | <p>Sets the secondary RADIUS server address.</p> <p>Command mode: Global configuration</p> |
| radius-server primary-host <IP address> key <1-32 characters> | <p>This is the primary shared secret between the switch and the RADIUS server(s).</p> <p>Command mode: Global configuration</p> |
| radius-server secondary-host <IP address> key <1-32 characters> | <p>This is the secondary shared secret between the switch and the RADIUS server(s).</p> <p>Command mode: Global configuration</p> |
| [default] radius-server port <UDP port number> | <p>Enter the number of the UDP port to be configured, between 1500 - 3000. The default is 1645.</p> <p>Command mode: Global configuration</p> |
| radius-server retransmit <1-3> | <p>Sets the number of failed authentication requests before switching to a different RADIUS server. The default is 3 requests.</p> <p>Command mode: Global configuration</p> |
| radius-server timeout <1-10> | <p>Sets the amount of time, in seconds, before a RADIUS server authentication attempt is considered to have failed. The default is 3 seconds.</p> <p>Command mode: Global configuration</p> |
| ip radius source-interface loopback <1-5> | <p>Sets the RADIUS source loopback interface.</p> <p>Command mode: Global configuration</p> |
| [no] radius-server backdoor | <p>Enables or disables the RADIUS backdoor for Telnet/SSH/HTTP/HTTPS. The default value is disabled.</p> <p>To obtain the RADIUS backdoor password for your switch, contact your Service and Support line.</p> <p>Command mode: Global configuration</p> |

Table 147. RADIUS Server Configuration Commands

| Command Syntax and Usage |
|--|
| <pre>radius-server enable</pre> <p>Enables the RADIUS server.</p> <p>Command mode: Global configuration</p> |
| <pre>no radius-server enable</pre> <p>Disables the RADIUS server.</p> <p>Command mode: Global configuration</p> |
| <pre>show radius-server</pre> <p>Displays the current RADIUS server parameters.</p> <p>Command mode: All</p> |

TACACS+ Server Configuration

TACACS (Terminal Access Controller Access Control system) is an authentication protocol that allows a remote access server to forward a user's logon password to an authentication server to determine whether access can be allowed to a given system. TACACS is not an encryption protocol, and therefore less secure than TACACS+ and Remote Authentication Dial-In User Service (RADIUS) protocols. Both TACACS and TACACS+ are described in RFC 1492.

TACACS+ protocol is more reliable than RADIUS, as TACACS+ uses the Transmission Control Protocol (TCP) whereas RADIUS uses the User Datagram Protocol (UDP). Also, RADIUS combines authentication and authorization in a user profile, whereas TACACS+ separates the two operations.

TACACS+ offers the following advantages over RADIUS as the authentication device:

- TACACS+ is TCP-based, so it facilitates connection-oriented traffic.
- It supports full-packet encryption, as opposed to password-only in authentication requests.
- It supports de-coupled authentication, authorization, and accounting.

Table 148. TACACS+ Server Configuration Commands

| Command Syntax and Usage | |
|---|---|
| [no] tacacs primary-host <IP address> | Defines the primary TACACS+ server address. Command mode: Global configuration |
| [no] tacacs secondary-host <IP address> | Defines the secondary TACACS+ server address. Command mode: Global configuration |
| [no] tacacs primary-host <IP address> key <1-32 characters> | This is the primary shared secret between the switch and the TACACS+ server(s). Command mode: Global configuration |
| [no] tacacs secondary-host <IP address> key <1-32 characters> | This is the secondary shared secret between the switch and the TACACS+ server(s). Command mode: Global configuration |
| [default] tacacs port <TCP port number> | Enter the number of the TCP port to be configured, between 1 and 65000. The default is 49. Command mode: Global configuration |
| tacacs retransmit <1-3> | Sets the number of failed authentication requests before switching to a different TACACS+ server. The default is 3 requests. Command mode: Global configuration |

Table 148. TACACS+ Server Configuration Commands (continued)

| Command Syntax and Usage | |
|--|---|
| <code>tacacs attempts <1-10></code> | <p>Sets the number of failed login attempts before disconnecting the user. The default is 2 attempts.</p> <p>Command mode: Global configuration</p> |
| <code>tacacs timeout <4-15></code> | <p>Sets the amount of time, in seconds, before a TACACS+ server authentication attempt is considered to have failed. The default is 5 seconds.</p> <p>Command mode: Global configuration</p> |
| <code>ip tacacs source-interface loopback <1-5></code> | <p>Sets the TACACS+ source loopback interface.</p> <p>Command mode: Global configuration</p> |
| <code>[no] tacacs user-mapping {<0-15> user oper admin}</code> | <p>Maps a TACACS+ authorization level to a switch user level. Enter a TACACS+ authorization level (0-15), followed by the corresponding switch user level.</p> <p>Command mode: Global configuration</p> |
| <code>[no] tacacs backdoor</code> | <p>Enables or disables the TACACS+ back door for Telnet, SSH/SCP, or HTTP/HTTPS.</p> <p>Enabling this feature allows you to bypass the TACACS+ servers. It is recommended that you use Secure Backdoor to ensure the switch is secured, because Secure Backdoor disallows access through the back door when the TACACS+ servers are responding.</p> <p>The default setting is disabled.</p> <p>To obtain the TACACS+ backdoor password for your EN4093 and EN4093R, contact your Service and Support line.</p> <p>Command mode: Global configuration</p> |
| <code>[no] tacacs secure-backdoor</code> | <p>Enables or disables TACACS+ secure back door access through Telnet, SSH/SCP, or HTTP/HTTPS only when the TACACS+ servers are not responding.</p> <p>This feature is recommended to permit access to the switch when the TACACS+ servers become unresponsive. If no back door is enabled, the only way to gain access when TACACS+ servers are unresponsive is to use the back door via the console port.</p> <p>The default is disabled.</p> <p>Command mode: Global configuration</p> |
| <code>[no] tacacs privilege-mapping</code> | <p>Enables or disables TACACS+ privilege-level mapping.</p> <p>The default value is disabled.</p> <p>Command mode: Global configuration</p> |

Table 148. TACACS+ Server Configuration Commands (continued)

| Command Syntax and Usage | |
|--|---|
| [no] tacacs-server password-change | <p>Enables or disables TACACS+ password change. The default value is disabled.</p> <p>Command mode: Global configuration</p> |
| primary-password | <p>Configures the password for the primary TACACS+ server. The CLI will prompt you for input.</p> <p>Command mode: Global configuration</p> |
| secondary-password | <p>Configures the password for the secondary TACACS+ server. The CLI will prompt you for input.</p> <p>Command mode: Global configuration</p> |
| [no] tacacs-server command-authorization | <p>Enables or disables TACACS+ command authorization.</p> <p>Command mode: Global configuration</p> |
| [no] tacacs-server command-logging | <p>Enables or disables TACACS+ command logging.</p> <p>Command mode: Global configuration</p> |
| [no] tacacs-server directed-request [restricted no-truncate] | <p>Enables or disables TACACS+ directed request, which uses a specified TACACS+ server for authentication, authorization, accounting. When enabled, When directed-request is enabled, each user must add a configured TACACS+ server hostname to the username (for example, username@hostname) during login.</p> <p>This command allows the following options:</p> <ul style="list-style-type: none"> – Restricted: Only the username is sent to the specified TACACS+ server. – No-truncate: The entire login string is sent to the TACACS+ server. <p>Command mode: Global configuration</p> |
| [no] tacacs-server enable | <p>Enables or disables the TACACS+ server. By default, the server is disabled.</p> <p>Command mode: Global configuration</p> |
| [no] tacacs-server accounting-enable | <p>Enables or disables TACACS+ accounting.</p> <p>Command mode: Global configuration</p> |
| show tacacs-server | <p>Displays current TACACS+ configuration parameters.</p> <p>Command mode: All</p> |

LDAP Server Configuration

LDAP (Lightweight Directory Access Protocol) is an authentication protocol that allows a remote access server to forward a user's logon password to an authentication server to determine whether access can be allowed to a given system.

Table 149. LDAP Server Configuration Commands

| Command Syntax and Usage | |
|---|--|
| <code>[no] ldap-server primary-host <IP address></code> | <p>Sets the primary LDAP server address.</p> <p>Command mode: Global configuration</p> |
| <code>[no] ldap-server secondary-host <IP address></code> | <p>Sets the secondary LDAP server address.</p> <p>Command mode: Global configuration</p> |
| <code>[default] ldap-server port <UDP port number></code> | <p>Enter the number of the UDP port to be configured, between 1 - 65000. The default is 389.</p> <p>Command mode: Global configuration</p> |
| <code>ldap-server retransmit <1-3></code> | <p>Sets the number of failed authentication requests before switching to a different LDAP server. The default is 3 requests.</p> <p>Command mode: Global configuration</p> |
| <code>ldap-server timeout <4-15></code> | <p>Sets the amount of time, in seconds, before a LDAP server authentication attempt is considered to have failed. The default is 5 seconds.</p> <p>Command mode: Global configuration</p> |
| <code>ldap-server domain [<1-128 characters> none]</code> | <p>Sets the domain name for the LDAP server. Enter the full path for your organization. For example:</p> <p><code>ou=people,dc=mydomain,dc=com</code></p> <p>Command mode: Global configuration</p> |
| <code>[no] ldap-server backdoor</code> | <p>Enables or disables the LDAP back door for Telnet, SSH/SCP, or HTTP/HTTPS. The default setting is disabled.</p> <p>To obtain the LDAP back door password for your EN4093 and EN4093R, contact your Service and Support line.</p> <p>Command mode: Global configuration</p> |

Table 149. LDAP Server Configuration Commands (continued)

| Command Syntax and Usage | |
|------------------------------------|--|
| <code>ldap-server enable</code> | Enables the LDAP server. Command mode: Global configuration |
| <code>no ldap-server enable</code> | Disables the LDAP server. Command mode: Global configuration |
| <code>show ldap-server</code> | Displays the current LDAP server parameters. Command mode: All |

NTP Server Configuration

These commands allow you to synchronize the switch clock to a Network Time Protocol (NTP) server. By default, this option is disabled.

Table 150. NTP Server Configuration Commands

| Command Syntax and Usage |
|---|
| <pre>[no] ntp primary-server <IP address>[data-port extm-port mgt-port]</pre> <p>Prompts for the IP addresses of the primary NTP server to which you want to synchronize the switch clock. Select the port to use for data transfer:</p> <ul style="list-style-type: none">– internal management port (mgt)– data port (data)– external management port (extm) <p>Command mode: Global configuration</p> |
| <pre>[no] ntp secondary-server <IP address>[data-port extm-port mgt-port]</pre> <p>Prompts for the IP addresses of the secondary NTP server to which you want to synchronize the switch clock. Select the port to use for data transfer:</p> <ul style="list-style-type: none">– internal management port (mgt)– data port (data)– external management port (extm) <p>Command mode: Global configuration</p> |
| <pre>[no] ntp ipv6 primary-server <IPv6 address>[data-port extm-port mgt-port]</pre> <p>Prompts for the IPv6 addresses of the primary NTP server to which you want to synchronize the switch clock. Select the port to use for data transfer:</p> <ul style="list-style-type: none">– internal management port (mgt)– data port (data)– external management port (extm) <p>Note: To delete the IPv6 primary server, use the following command: no ntp primary-server <IP address></p> <p>Command mode: Global configuration</p> |
| <pre>[no] ntp ipv6 secondary-server <IPv6 address>[data-port extm-port mgt-port]</pre> <p>Prompts for the IPv6 addresses of the secondary NTP server to which you want to synchronize the switch clock. Select the port to use for data transfer:</p> <ul style="list-style-type: none">– internal management port (mgt)– data port (data)– external management port (extm) <p>Note: To delete the IPv6 secondary server, use the following command: no ntp secondary-server <IP address></p> <p>Command mode: Global configuration</p> |

Table 150. NTP Server Configuration Commands

| Command Syntax and Usage | |
|-----------------------------|--|
| [no] ntp sync-logs | <p>Enables or disables informational logs for NTP synchronization failures. Default setting is enabled.</p> <p>Command mode: Global configuration</p> |
| ntp offset <0-86400> | <p>Configures the minimum offset in seconds between the switch clock and the NTP server that triggers a system log message.</p> <p>The default value is 300.</p> <p>Command mode: Global configuration</p> |
| no ntp offset | <p>Resets the NTP offset to the default 300 seconds value.</p> <p>Command mode: Global configuration</p> |
| ntp interval <5-44640> | <p>Specifies the interval, that is, how often, in minutes, to re-synchronize the switch clock with the NTP server.</p> <p>The default value is 1440.</p> <p>Command mode: Global configuration</p> |
| ntp source loopback <1-5> | <p>Sets the NTP source loopback interface.</p> <p>Command mode: Global configuration</p> |
| [no] ntp authenticate | <p>Enables or disables NTP authentication. The default setting is disabled. When authentication is enabled, the switch transmits NTP packets with the MAC address appended.</p> <p>Command mode: Global configuration</p> |
| ntp primary-key <1-65534> | <p>Adds the NTP primary server key, which specifies which MD5 key is used by the primary server.</p> <p>Command mode: Global configuration</p> |
| ntp secondary-key <1-65534> | <p>Adds the NTP secondary server key, which specifies which MD5 key is used by the secondary server.</p> <p>Command mode: Global configuration</p> |
| ntp trusted-key <1-65534> 0 | <p>Adds an MD5 key code to the list of trusted keys. Enter 0 (zero) to remove the selected key code.</p> <p>Command mode: Global configuration</p> |

Table 150. NTP Server Configuration Commands

| Command Syntax and Usage |
|--|
| <pre>ntp enable</pre> <p>Enables the NTP synchronization service. Command mode: Global configuration</p> |
| <pre>no ntp enable</pre> <p>Disables the NTP synchronization service. Command mode: Global configuration</p> |
| <pre>show ntp</pre> <p>Displays the current NTP service settings. Command mode: All</p> |

NTP MD5 Key Commands

Table 151. NTP MD5 KEy Configuration Options

| Command Syntax and Usage |
|---|
| <pre>ntp message-digest-key <1-65534> md5-key <1-16 characters></pre> <p>Configures the selected MD5 key code. Command mode: Global configuration</p> |
| <pre>no ntp message-digest-key <1-65534></pre> <p>Deletes the selected MD5 key code. Command mode: Global configuration</p> |

System SNMP Configuration

Networking OS supports SNMP-based network management. In SNMP model of network management, a management station (client/manager) accesses a set of variables known as MIBs (Management Information Base) provided by the managed device (agent). If you are running an SNMP network management station on your network, you can manage the switch using the following standard SNMP MIBs:

- MIB II (RFC 1213)
- Ethernet MIB (RFC 1643)
- Bridge MIB (RFC 1493)

An SNMP agent is a software process on the managed device that listens on UDP port 161 for SNMP messages. Each SNMP message sent to the agent contains a list of management objects to retrieve or to modify.

SNMP parameters that can be modified include:

- System name
- System location
- System contact
- Use of the SNMP system authentication trap function
- Read community string
- Write community string
- Trap community strings

Table 152. System SNMP Commands

| Command Syntax and Usage |
|--|
| <pre>snmp-server name <1-64 characters></pre> <p>Configures the name for the system. The name can have a maximum of 64 characters.</p> <p>Command mode: Global configuration</p> |
| <pre>snmp-server location <1-64 characters></pre> <p>Configures the name of the system location. The location can have a maximum of 64 characters.</p> <p>Command mode: Global configuration</p> |
| <pre>snmp-server contact <1-64 characters></pre> <p>Configures the name of the system contact. The contact can have a maximum of 64 characters.</p> <p>Command mode: Global configuration</p> |
| <pre>snmp-server read-community <1-32 characters></pre> <p>Configures the SNMP read community string. The read community string controls SNMP “get” access to the switch. It can have a maximum of 32 characters. The default read community string is <i>public</i>.</p> <p>Command mode: Global configuration</p> |

Table 152. System SNMP Commands

| Command Syntax and Usage | |
|---|--|
| <code>snmp-server write-community <1-32 characters></code> | <p>Configures the SNMP write community string. The write community string controls SNMP “set” and “get” access to the switch. It can have a maximum of 32 characters. The default write community string is <i>private</i>.</p> <p>Command mode: Global configuration</p> |
| <code>[no] snmp-server read-community-additional <1-32 characters></code> | <p>Adds or removes an additional SNMP read community string. Up to 7 additional read community strings are supported.</p> <p>Command mode: Global configuration</p> |
| <code>[no] snmp-server write-community-additional <1-32 characters></code> | <p>Adds or removes an additional SNMP write community string. Up to 7 additional write community strings are supported.</p> <p>Command mode: Global configuration</p> |
| <code>snmp-server trap-source {<interface number> loopback <1-5>}</code> | <p>Configures the source interface for SNMP traps.</p> <p>To send traps through the management ports, specify interface 128.</p> <p>Command mode: Global configuration</p> |
| <code>snmp-server host <trap host IP address> <trap host community string></code> | <p>Adds a trap host server.</p> <p>Command mode: Global configuration</p> |
| <code>no snmp-server host <trap host IP address></code> | <p>Removes the trap host server.</p> <p>Command mode: Global configuration</p> |
| <code>snmp-server timeout <1-30></code> | <p>Sets the timeout value for the SNMP state machine, in minutes.</p> <p>Command mode: Global configuration</p> |
| <code>[no] snmp-server authentication-trap</code> | <p>Enables or disables the use of the system authentication trap facility. The default setting is disabled.</p> <p>Command mode: Global configuration</p> |
| <code>[no] snmp-server link-trap</code> | <p>Enables or disables the sending of SNMP link up and link down traps. The default setting is enabled.</p> <p>Command mode: Global configuration</p> |
| <code>show snmp-server</code> | <p>Displays the current SNMP configuration.</p> <p>Command mode: All</p> |

SNMPv3 Configuration

SNMP version 3 (SNMPv3) is an extensible SNMP Framework that supplements the SNMPv2 Framework by supporting the following:

- a new SNMP message format
- security for messages
- access control
- remote configuration of SNMP parameters

For more details on the SNMPv3 architecture please refer to RFC3411 to RFC3418.

Table 153. SNMPv3 Configuration Commands

| Command Syntax and Usage |
|--|
| <pre>snmp-server user <I-16></pre> <p>This command allows you to create a user security model (USM) entry for an authorized user. You can also configure this entry through SNMP.</p> <p>Command mode: Global configuration</p> <p>To view command options, see page 267.</p> |
| <pre>snmp-server view <I-128></pre> <p>This command allows you to create different MIB views.</p> <p>Command mode: Global configuration</p> <p>To view command options, see page 268.</p> |
| <pre>snmp-server access <I-32></pre> <p>This command allows you to specify access rights. The View-based Access Control Model defines a set of services that an application can use for checking access rights of the user. You need access control when you have to process retrieval or modification request from an SNMP entity.</p> <p>Command mode: Global configuration</p> <p>To view command options, see page 269.</p> |
| <pre>snmp-server group <I-16></pre> <p>A group maps the user name to the access group names and their access rights needed to access SNMP management objects. A group defines the access rights assigned to all names that belong to a particular group.</p> <p>Command mode: Global configuration</p> <p>To view command options, see page 270.</p> |
| <pre>snmp-server community <I-16></pre> <p>The community table contains objects for mapping community strings and version-independent SNMP message parameters.</p> <p>Command mode: Global configuration</p> <p>To view command options, see page 271.</p> |

Table 153. SNMPv3 Configuration Commands (continued)

| |
|--|
| <pre>snmp-server target-address <I-16></pre> <p>This command allows you to configure destination information, consisting of a transport domain and a transport address. This is also termed as transport endpoint. The SNMP MIB provides a mechanism for performing source address validation on incoming requests, and for selecting community strings based on target addresses for outgoing notifications.</p> <p>Command mode: Global configuration</p> <p>To view command options, see page 272.</p> |
| <pre>snmp-server target-parameters <I-16></pre> <p>This command allows you to configure SNMP parameters, consisting of message processing model, security model, security level, and security name information. There may be multiple transport endpoints associated with a particular set of SNMP parameters, or a particular transport endpoint may be associated with several sets of SNMP parameters.</p> <p>Command mode: Global configuration</p> <p>To view command options, see page 273.</p> |
| <pre>snmp-server notify <I-16></pre> <p>A notification application typically monitors a system for particular events or conditions, and generates Notification-Class messages based on these events or conditions.</p> <p>Command mode: Global configuration</p> <p>To view command options, see page 274.</p> |
| <pre>snmp-server version {v1v2v3 v3only}</pre> <p>This command allows you to enable or disable the access to SNMP versions 1, 2 or 3. The default value is v1v2v3.</p> <p>Command mode: Global configuration</p> |
| <pre>show snmp-server v3</pre> <p>Displays the current SNMPv3 configuration.</p> <p>Command mode: All</p> |

User Security Model Configuration

You can make use of a defined set of user identities using this Security Model. An SNMP engine must have the knowledge of applicable attributes of a user.

These commands help you create a user security model entry for an authorized user. You need to provide a security name to create the USM entry.

Table 154. User Security Model Configuration Commands

| Command Syntax and Usage | |
|--|---|
| <pre>snmp-server user <1-16> name <1-32 characters></pre> | <p>This command allows you to configure a string that represents the name of the user. This is the login name that you need in order to access the switch.</p> <p>Command mode: Global configuration</p> |
| <pre>snmp-server user <1-16> authentication-protocol {md5 sha none} authentication-password <password value></pre> | <p>This command allows you to configure the authentication protocol and password.</p> <p>The authentication protocol can be HMAC-MD5-96 or HMAC-SHA-96, or none. The default algorithm is none.</p> <p>When you configure an authentication algorithm, you must provide a password, otherwise you will get an error message during validation. This command allows you to create or change your password for authentication.</p> <p>Command mode: Global configuration</p> |
| <pre>snmp-server user <1-16> privacy-protocol {des none} privacy-password <password value></pre> | <p>This command allows you to configure the type of privacy protocol and the privacy password.</p> <p>The privacy protocol protects messages from disclosure. The options are <i>des</i> (CBC-DES Symmetric Encryption Protocol) or <i>none</i>. If you specify <i>des</i> as the privacy protocol, then make sure that you have selected one of the authentication protocols (MD5 or HMAC-SHA-96). If you select <i>none</i> as the authentication protocol, you will get an error message.</p> <p>You can create or change the privacy password.</p> <p>Command mode: Global configuration</p> |
| <pre>no snmp-server user <1-16></pre> | <p>Deletes the USM user entries.</p> <p>Command mode: Global configuration</p> |
| <pre>show snmp-server v3 user <1-16></pre> | <p>Displays the USM user entries.</p> <p>Command mode: All</p> |

SNMPv3 View Configuration

Note that the first five default `vacmViewTreeFamily` entries cannot be removed, and their names cannot be changed.

Table 155. SNMPv3 View Configuration Commands

| Command Syntax and Usage | |
|---|---|
| <code>snmp-server view <I-128> name <I-32 characters></code> | This command defines the name for a family of view subtrees. Command mode: Global configuration |
| <code>snmp-server view <I-128> tree <I-64 characters></code> | This command defines MIB tree, which when combined with the corresponding mask defines a family of view subtrees. Command mode: Global configuration |
| <code>[no] snmp-server view <I-128> mask <I-32 characters></code> | This command defines the bit mask, which in combination with the corresponding tree defines a family of view subtrees. Command mode: Global configuration |
| <code>snmp-server view <I-128> type {included excluded}</code> | This command indicates whether the corresponding instances of <code>vacmViewTreeFamilySubtree</code> and <code>vacmViewTreeFamilyMask</code> define a family of view subtrees, which is included in or excluded from the MIB view. Command mode: Global configuration |
| <code>no snmp-server view <I-128></code> | Deletes the <code>vacmViewTreeFamily</code> group entry. Command mode: Global configuration |
| <code>show snmp-server v3 view <I-128></code> | Displays the current <code>vacmViewTreeFamily</code> configuration. Command mode: All |

View-based Access Control Model Configuration

The view-based Access Control Model defines a set of services that an application can use for checking access rights of the user. Access control is needed when the user has to process SNMP retrieval or modification request from an SNMP entity.

Table 156. View-based Access Control Model Commands

| Command Syntax and Usage |
|--|
| <pre>snmp-server access <1-32> name <1-32 characters></pre> <p>Defines the name of the group.</p> <p>Command mode: Global configuration</p> |
| <pre>snmp-server access <1-32> prefix <1-32 characters></pre> <p>Defines the name of the context. An SNMP context is a collection of management information that an SNMP entity can access. An SNMP entity has access to many contexts. For more information on naming the management information, see RFC2571, the SNMP Architecture document. The view-based Access Control Model defines a table that lists the locally available contexts by contextName.</p> <p>Command mode: Global configuration</p> |
| <pre>snmp-server access <1-32> security {usm snmpv1 snmpv2}</pre> <p>Allows you to select the security model to be used.</p> <p>Command mode: Global configuration</p> |
| <pre>snmp-server access <1-32> level {noAuthNoPriv authNoPriv authPriv}</pre> <p>Defines the minimum level of security required to gain access rights. The level <code>noAuthNoPriv</code> means that the SNMP message will be sent without authentication and without using a privacy protocol. The level <code>authNoPriv</code> means that the SNMP message will be sent with authentication but without using a privacy protocol. The <code>authPriv</code> means that the SNMP message will be sent both with authentication and using a privacy protocol.</p> <p>Command mode: Global configuration</p> |
| <pre>snmp-server access <1-32> match {exact prefix}</pre> <p>If the value is set to <code>exact</code>, then all the rows whose contextName exactly matches the prefix are selected. If the value is set to <code>prefix</code> then the all the rows where the starting octets of the contextName exactly match the prefix are selected.</p> <p>Command mode: Global configuration</p> |
| <pre>snmp-server access <1-32> read-view <1-32 characters></pre> <p>Defines a read view name that allows you read access to a particular MIB view. If the value is empty or if there is no active MIB view having this value then no access is granted.</p> <p>Command mode: Global configuration</p> |

Table 156. View-based Access Control Model Commands (continued)

| Command Syntax and Usage |
|--|
| <pre>snmp-server access <1-32> write-view <1-32 characters></pre> <p>Defines a write view name that allows you write access to the MIB view. If the value is empty or if there is no active MIB view having this value then no access is granted.</p> <p>Command mode: Global configuration</p> |
| <pre>snmp-server access <1-32> notify-view <1-32 characters></pre> <p>Defines a notify view name that allows you notify access to the MIB view.</p> <p>Command mode: Global configuration</p> |
| <pre>no snmp-server access <1-32></pre> <p>Deletes the View-based Access Control entry.</p> <p>Command mode: Global configuration</p> |
| <pre>show snmp-server v3 access <1-32></pre> <p>Displays the View-based Access Control configuration.</p> <p>Command mode: All</p> |

SNMPv3 Group Configuration

Table 157. SNMPv3 Group Configuration Commands

| Command Syntax and Usage |
|---|
| <pre>snmp-server group <1-16> security {usm snmpv1 snmpv2}</pre> <p>Defines the security model.</p> <p>Command mode: Global configuration</p> |
| <pre>snmp-server group <1-16> user-name <1-32 characters></pre> <p>Sets the user name as defined in the following command on page 267: <pre>snmp-server user <1-16> name <1-32 characters></pre></p> <p>Command mode: Global configuration</p> |
| <pre>snmp-server group <1-16> group-name <1-32 characters></pre> <p>The name for the access group as defined in the following command: <pre>snmp-server access <1-32> name <1-32 characters></pre> on page 267.</p> <p>Command mode: Global configuration</p> |
| <pre>no snmp-server group <1-16></pre> <p>Deletes the vacmSecurityToGroup entry.</p> <p>Command mode: Global configuration</p> |
| <pre>show snmp-server v3 group <1-16></pre> <p>Displays the current vacmSecurityToGroup configuration.</p> <p>Command mode: All</p> |

SNMPv3 Community Table Configuration

These commands are used for configuring the community table entry. The configured entry is stored in the community table list in the SNMP engine. This table is used to configure community strings in the Local Configuration Datastore (LCD) of SNMP engine.

Table 158. SNMPv3 Community Table Configuration Commands

| Command Syntax and Usage |
|---|
| <pre>snmp-server community <1-16> index <1-32 characters></pre> <p>Allows you to configure the unique index value of a row in this table.</p> <p>Command string: Global configuration</p> |
| <pre>snmp-server community <1-16> name <1-32 characters></pre> <p>Defines the user name as defined in the following command on page 267:</p> <pre>snmp-server user <1-16> name <1-32 characters></pre> <p>Command string: Global configuration</p> |
| <pre>snmp-server community <1-16> user-name <1-32 characters></pre> <p>Defines a readable string that represents the corresponding value of an SNMP community name in a security model.</p> <p>Command mode: Global configuration</p> |
| <pre>snmp-server community <1-16> tag <1-255 characters></pre> <p>Allows you to configure a tag. This tag specifies a set of transport endpoints to which a command responder application sends an SNMP trap.</p> <p>Command mode: Global configuration</p> |
| <pre>no snmp-server community <1-16></pre> <p>Deletes the community table entry.</p> <p>Command mode: Global configuration</p> |
| <pre>show snmp-server v3 community <1-16></pre> <p>Displays the community table configuration.</p> <p>Command mode: All</p> |

SNMPv3 Target Address Table Configuration

These commands are used to configure the target transport entry. The configured entry is stored in the target address table list in the SNMP engine. This table of transport addresses is used in the generation of SNMP messages.

Table 159. Target Address Table Configuration Commands

| Command Syntax and Usage |
|--|
| <pre>snmp-server target-address <1-16> address <IP address> name <1-32 characters></pre> <p>Allows you to configure the locally arbitrary, but unique identifier, target address name associated with this entry.</p> <p>Command mode: Global configuration</p> |
| <pre>snmp-server target-address <1-16> name <1-32 characters> address <transport IP address></pre> <p>Configures a transport IPv4 address that can be used in the generation of SNMP traps.</p> <p>Command mode: Global configuration</p> |
| <pre>snmp-server target-address <1-16> port <port number></pre> <p>Allows you to configure a transport address port that can be used in the generation of SNMP traps.</p> <p>Command mode: Global configuration</p> |
| <pre>snmp-server target-address <1-16> taglist <1-255 characters></pre> <p>Allows you to configure a list of tags that are used to select target addresses for a particular operation.</p> <p>Command mode: Global configuration</p> |
| <pre>snmp-server target-address <1-16> parameters-name <1-32 characters></pre> <p>Defines the name as defined in the following command on page 273: <pre>snmp-server target-parameters <1-16> name <1-32 characters></pre></p> <p>Command mode: Global configuration</p> |
| <pre>no snmp-server target-address <1-16></pre> <p>Deletes the Target Address Table entry.</p> <p>Command mode: Global configuration</p> |
| <pre>show snmp-server v3 target-address <1-16></pre> <p>Displays the current Target Address Table configuration.</p> <p>Command mode: All</p> |

SNMPv3 Target Parameters Table Configuration

You can configure the target parameters entry and store it in the target parameters table in the SNMP engine. This table contains parameters that are used to generate a message. The parameters include the message processing model (for example: SNMPv3, SNMPv2c, SNMPv1), the security model (for example: USM), the security name, and the security level (`noAuthNoPriv`, `authNoPriv`, or `authPriv`).

Table 160. Target Parameters Table Configuration Commands

| Command Syntax and Usage |
|---|
| <pre>snmp-server target-parameters <1-16> name <1-32 characters></pre> <p>Allows you to configure the locally arbitrary, but unique, identifier that is associated with this entry.</p> <p>Command mode: Global configuration</p> |
| <pre>snmp-server target-parameters <1-16> message {snmpv1 snmpv2c snmpv3}</pre> <p>Allows you to configure the message processing model that is used to generate SNMP messages.</p> <p>Command mode: Global configuration</p> |
| <pre>snmp-server target-parameters <1-16> security {usm snmpv1 snmpv2}</pre> <p>Allows you to select the security model to be used when generating the SNMP messages.</p> <p>Command mode: Global configuration</p> |
| <pre>snmp-server target-parameters <1-16> user-name <1-32 characters></pre> <p>Defines the name that identifies the user in the USM table (page 267) on whose behalf the SNMP messages are generated using this entry.</p> <p>Command mode: Global configuration</p> |
| <pre>snmp-server target-parameters <1-16> level {noAuthNoPriv authNoPriv authPriv}</pre> <p>Allows you to select the level of security to be used when generating the SNMP messages using this entry. The level <code>noAuthNoPriv</code> means that the SNMP message will be sent without authentication and without using a privacy protocol. The level <code>authNoPriv</code> means that the SNMP message will be sent with authentication but without using a privacy protocol. The <code>authPriv</code> means that the SNMP message will be sent both with authentication and using a privacy protocol.</p> <p>Command mode: Global configuration</p> |
| <pre>no snmp-server target-parameters <1-16></pre> <p>Deletes the <code>targetParamsTable</code> entry.</p> <p>Command mode: Global configuration</p> |
| <pre>show snmp-server v3 target-parameters <1-16></pre> <p>Displays the current <code>targetParamsTable</code> configuration.</p> <p>Command mode: All</p> |

SNMPv3 Notify Table Configuration

SNMPv3 uses Notification Originator to send out traps. A notification typically monitors a system for particular events or conditions, and generates Notification-Class messages based on these events or conditions.

Table 161. Notify Table Commands

| Command Syntax and Usage |
|--|
| <pre>snmp-server notify <1-16> name <1-32 characters></pre> <p>Defines a locally arbitrary, but unique, identifier associated with this SNMP notify entry.</p> <p>Command mode: Global configuration</p> |
| <pre>snmp-server notify <1-16> tag <1-255 characters></pre> <p>Allows you to configure a tag that contains a tag value which is used to select entries in the Target Address Table. Any entry in the <code>snmpTargetAddrTable</code>, that matches the value of this tag, is selected.</p> <p>Command mode: Global configuration</p> |
| <pre>no snmp-server notify <1-16></pre> <p>Deletes the notify table entry.</p> <p>Command mode: Global configuration</p> |
| <pre>show snmp-server v3 notify <1-16></pre> <p>Displays the current notify table configuration.</p> <p>Command mode: All</p> |

System Access Configuration

The following table describes system access configuration commands.

Table 162. System Access Configuration Commands

| Command Syntax and Usage |
|--|
| <pre>access user user-password</pre> <p>Sets the user (<code>user</code>) password. The user has no direct responsibility for switch management. The user view switch status information and statistics, but cannot make any configuration changes.</p> <p>This command will prompt for required information: current admin password, new password (up to 128 characters) and confirmation of the new password.</p> <p>Note: To disable the user account, set the password to null (no password).</p> <p>Command Mode: Global configuration</p> |
| <pre>access user operator-password</pre> <p>Sets the operator (<code>oper</code>) password. The operator manages all functions of the switch. The operator can view all switch information and statistics and can reset ports.</p> <p>This command will prompt for required information: current admin password, new password (up to 128 characters) and confirmation of the new password.</p> <p>Note: To disable the operator account, set the password to null (no password). The default setting is disabled (no password).</p> <p>Command Mode: Global configuration</p> |
| <pre>access user administrator-password</pre> <p>Sets the administrator (<code>admin</code>) password. The administrator has complete access to all menus, information, and configuration commands on the EN4093 and EN4093R, including the ability to change both the user and administrator passwords.</p> <p>This command will prompt for required information: current admin password, new password (up to 128 characters) and confirmation of the new password.</p> <p>Access includes “<code>oper</code>” functions.</p> <p>Note: You cannot disable the administrator password.</p> <p>Command Mode: Global configuration</p> |
| <pre>[no] access http enable</pre> <p>Enables or disables HTTP (Web) access to the Browser-Based Interface. It is enabled by default.</p> <p>Command mode: Global configuration</p> |
| <pre>[default] access http port [<i><port number></i>]</pre> <p>Sets the switch port used for serving switch Web content. The default is HTTP port 80.</p> <p>Command mode: Global configuration</p> |

Table 162. System Access Configuration Commands (continued)

| Command Syntax and Usage | |
|--|--|
| [no] access snmp {read-only read-write} | Disables or provides read-only/write-read SNMP access. Command mode: Global configuration |
| [no] access telnet enable | Enables or disables Telnet access. This command is enabled by default. Command mode: Global configuration |
| [default] access telnet port [<1-65535>] | Sets an optional Telnet server port number for cases where the server listens for Telnet sessions on a non-standard port. Command mode: Global configuration |
| [default] access tftp-port [<1-65535>] | Sets the TFTP port for the switch. The default is port 69. Command mode: Global configuration |
| [no] access tsbbi enable | Enables or disables Telnet/SSH configuration through the Browser-Based Interface (BBI). Command mode: Global configuration |
| [no] access userbbi enable | Enables or disables user configuration access through the Browser-Based Interface (BBI). Command mode: Global configuration |
| show access | Displays the current system access parameters. Command mode: All |

Management Network Configuration

These commands are used to define IP address ranges which are allowed to access the switch for management purposes.

Table 163. Management Network Configuration Commands

| Command Syntax and Usage | |
|---|---|
| <pre>access management-network <mgmt network IPv4 or IPv6 address> <mgmt network mask or prefix length></pre> | <p>Adds a defined network through which switch access is allowed through Telnet, SNMP, RIP, or the Networking OS browser-based interface. A range of IP addresses is produced when used with a network mask address. Specify an IP address and mask address in dotted-decimal notation.</p> <p>Note: If you configure the management network without including the switch interfaces, the configuration causes the Firewall Load Balancing health checks to fail and creates a “Network Down” state on the network.</p> <p>Command mode: Global configuration</p> |
| <pre>no access management-network <mgmt network IPv4 or IPv6 address> <mgmt network mask or prefix length></pre> | <p>Removes a defined network, which consists of a management network address and a management network mask address.</p> <p>Command mode: Global configuration</p> |
| <pre>access management-network <mgmt network IPv4 or IPv6 address> <mgmt network mask or prefix length> {snmp-ro snmp-rw}</pre> | <p>Adds a defined network through which SNMP read-only or SNMP read/write switch access is allowed. Specify an IP address and mask address in dotted-decimal notation.</p> <p>Command mode: Global configuration</p> |
| <pre>no access management-network {snmp-ro snmp-rw}</pre> | <p>Clears the SNMP read-only or SNMP read/write access control list for management purposes.</p> <p>Command mode: Global configuration</p> |
| <pre>show access management-network</pre> | <p>Displays the current management network configuration and SNMP access management IP list.</p> <p>Command mode: All</p> |
| <pre>clear access management-network</pre> | <p>Removes all defined management networks.</p> <p>Command mode: All except User EXEC</p> |

User Access Control Configuration

The following table describes user-access control commands.

Passwords can be a maximum of 128 characters.

Table 164. User Access Control Configuration Commands

| Command Syntax and Usage |
|---|
| <pre>access user <1-10></pre> <p>Configures the User ID.</p> <p>Command mode: Global configuration</p> |
| <pre>access user eject {<user name> <session ID>}</pre> <p>Ejects the specified user from the EN4093 and EN4093R.</p> <p>Command mode: Global configuration</p> |
| <pre>clear line <1-12></pre> <p>Ejects the user with the corresponding session ID from the EN4093 and EN4093R.</p> <p>Command mode: Privileged EXEC</p> |
| <pre>[no] access user administrator-enable</pre> <p>Enables or disables the default administrator account.</p> <p>Command mode: Global configuration</p> |
| <pre>access user user-password <1-128 characters></pre> <p>Sets the user (<code>user</code>) password. The user has no direct responsibility for switch management. He or she can view switch status information and statistics, but cannot make any configuration changes.</p> <p>Command mode: Global configuration</p> |
| <pre>access user operator-password <1-128 characters></pre> <p>Sets the operator (<code>oper</code>) password. The operator manages all functions of the switch. He or she can view all switch information and statistics and can reset ports.</p> <p>Command mode: Global configuration</p> |
| <pre>access user administrator-password <1-128 characters></pre> <p>Sets the administrator (<code>admin</code>) password. The super user administrator has complete access to all information and configuration commands on the EN4093 and EN4093R, including the ability to change both the user and administrator passwords.</p> <p>Access includes “<code>oper</code>” functions.</p> <p>Command mode: Global configuration</p> |
| <pre>show access user</pre> <p>Displays the current user status.</p> <p>Command mode: All</p> |

System User ID Configuration

The following table describes user ID configuration commands.

Table 165. User ID Configuration Commands

| Command Syntax and Usage | |
|---|--|
| <pre>access user <1-10> level {user operator administrator}</pre> | <p>Sets the Class-of-Service to define the user's authority level. Networking OS defines these levels as: User, Operator, and Administrator, with User being the most restricted level.</p> <p>Command mode: Global configuration</p> |
| <pre>access user <1-10> name <1-8 characters></pre> | <p>Defines the user name of maximum eight characters.</p> <p>Command mode: Global configuration</p> |
| <pre>access user <1-10> password</pre> | <p>Sets the user (<code>user</code>) password. This command will prompt for required information: current admin password, new password (up to 128 characters) and confirmation of the new password.</p> <p>Command mode: Global configuration</p> |
| <pre>access user <1-10> enable</pre> | <p>Enables the user ID.</p> <p>Command mode: Global configuration</p> |
| <pre>no access user <1-10> enable</pre> | <p>Disables the user ID.</p> <p>Command mode: Global configuration</p> |
| <pre>no access user <1-10></pre> | <p>Deletes the user ID.</p> <p>Command mode: Global configuration</p> |
| <pre>show access user</pre> | <p>Displays the current user ID configuration.</p> <p>Command mode: All</p> |

Strong Password Configuration

The following table describes strong password configuration commands.

Table 166. Strong Password Configuration Commands

| Command Syntax and Usage |
|---|
| <pre>access user strong-password enable</pre> <p>Enables Strong Password requirement. Command mode: Global configuration</p> |
| <pre>no access user strong-password enable</pre> <p>Disables Strong Password requirement. Command mode: Global configuration</p> |
| <pre>access user strong-password expiry <1-365></pre> <p>Configures the number of days allowed before the password must be changed. The default value is 60 days. Command mode: Global configuration</p> |
| <pre>access user strong-password warning <1-365></pre> <p>Configures the number of days before password expiration, that a warning is issued to users. The default value is 15 days. Command mode: Global configuration</p> |
| <pre>access user strong-password faillog <1-255></pre> <p>Configures the number of failed login attempts allowed before a security notification is logged. The default value is 3 login attempts. Command mode: Global configuration</p> |
| <pre>[no] access user strong-password lockout</pre> <p>Enables or disables account lockout after a specified number of failed login attempts. Default setting is disabled. Command mode: Global configuration</p> |
| <pre>access user strong-password faillock <1-10></pre> <p>Configures the number of failed login attempts that trigger the account lockout. Default value is 6. Command mode: Global configuration</p> |
| <pre>access user strong-password clear local user {lockout fail-attempts} {<username> all}</pre> <p>Enables locked out accounts or resets failed login counters for all users or for a specific user. Command mode: Global configuration</p> |
| <pre>show access user strong-password</pre> <p>Displays the current Strong Password configuration. Command mode: All</p> |

HTTPS Access Configuration

The following table describes HTTPS access configuration commands.

Table 167. HTTPS Access Configuration Commands

| Command Syntax and Usage |
|--|
| <pre>[no] access https enable</pre> <p>Enables or disables BBI access (Web access) using HTTPS.</p> <p>Command mode: Global configuration</p> |
| <pre>[default] access https port [<TCP port number>]</pre> <p>Defines the HTTPS Web server port number. The default port is 443.</p> <p>Command mode: Global configuration</p> |
| <pre>access https generate-certificate</pre> <p>Allows you to generate a certificate to connect to the SSL to be used during the key exchange. A default certificate is created when HTTPS is enabled for the first time. The user can create a new certificate defining the information that they want to be used in the various fields. For example:</p> <ul style="list-style-type: none"> – Country Name (2 letter code): CA – State or Province Name (full name): Ontario – Locality Name (for example, city): Ottawa – Organization Name (for example, company): IBM – Organizational Unit Name (for example, section): Operations – Common Name (for example, user's name): Mr Smith – Email (for example, email address): info@ibm.com <p>You will be asked to confirm if you want to generate the certificate. It will take approximately 30 seconds to generate the certificate. Then the switch will restart SSL agent.</p> <p>Command mode: Global configuration</p> |
| <pre>access https save-certificate</pre> <p>Allows the client, or the Web browser, to accept the certificate and save the certificate to Flash to be used when the switch is rebooted.</p> <p>Command mode: Global configuration</p> |
| <pre>show access</pre> <p>Displays the current SSL Web Access configuration.</p> <p>Command mode: All</p> |

Custom Daylight Saving Time Configuration

Use these commands to configure custom Daylight Saving Time. The DST is defined by two rules, the start rule and end rule. The rules specify the dates when the DST starts and finishes. These dates are represented as specific calendar dates or as relative offsets in a month (for example, 'the second Sunday of September').

Relative offset example:

2070901 = Second Sunday of September, at 1:00 a.m.

Calendar date example:

0070901 = September 7, at 1:00 a.m.

Table 168. Custom DST Configuration Commands

| Command Syntax and Usage |
|---|
| <pre>system custom-dst start-rule <WDDMMhh></pre> <p>Configures the start date for custom DST, as follows:</p> <p>WDDMMhh</p> <p>W = week (0-5, where 0 means use the calendar date) D = day of the week (01-07, where 01 is Monday) MM = month (1-12) hh = hour (0-23)</p> <p>Note: Week 5 is always considered to be the last week of the month.</p> <p>Command mode: Global configuration</p> |
| <pre>system custom-dst end-rule <WDDMMhh></pre> <p>Configures the end date for custom DST, as follows:</p> <p>WDDMMhh</p> <p>W = week (0-5, where 0 means use the calendar date) D = day of the week (01-07, where 01 is Monday) MM = month (1-12) hh = hour (0-23)</p> <p>Note: Week 5 is always considered to be the last week of the month.</p> <p>Command mode: Global configuration</p> |
| <pre>system custom-dst enable</pre> <p>Enables the Custom Daylight Saving Time settings.</p> <p>Command mode: Global configuration</p> |
| <pre>no system custom-dst enable</pre> <p>Disables the Custom Daylight Savings Time settings.</p> <p>Command mode: Global configuration</p> |
| <pre>show custom-dst</pre> <p>Displays the current Custom DST configuration.</p> <p>Command mode: All</p> |

sFlow Configuration

Networking OS supports sFlow version 5. sFlow is a sampling method used for monitoring high speed switched networks. Use these commands to configure the sFlow agent on the switch.

Table 169. sFlow Configuration Commands

| Command Syntax and Usage |
|--|
| <code>sflow enable</code> Enables the sFlow agent. Command mode: Global configuration |
| <code>no sflow enable</code> Disables the sFlow agent. Command mode: Global configuration |
| <code>sflow server <IP address></code> Defines the sFlow server address. Command mode: Global configuration |
| <code>sflow port <1-65535></code> Configures the UDP port for the sFlow server. The default value is 6343. Command mode: Global configuration |
| <code>show sflow</code> Displays sFlow configuration parameters. Command mode: All |

sFlow Port Configuration

Use the following commands to configure the sFlow port on the switch.

Table 170. sFlow Port Configuration Commands

| Command Syntax and Usage |
|--|
| <code>[no] sflow polling <5-60></code> Configures the sFlow polling interval, in seconds. The default setting is disabled. Command mode: Interface port |
| <code>[no] sflow sampling <256-65536></code> Configures the sFlow sampling rate, in packets per sample. The default setting is disabled. Command mode: Interface port |

Port Configuration

Use the Port Configuration commands to configure settings for switch ports (INT_x) and (EXT_x). If you are configuring management ports (MGT1), see [“Management Port Configuration” on page 293](#).

Table 171. Port Configuration Commands

| Command Syntax and Usage |
|--|
| <pre>interface port <port alias or number></pre> <p>Enter Interface port mode.</p> <p>Command mode: Global configuration</p> |
| <pre>dot1p <0-7></pre> <p>Configures the port's 802.1p priority level.</p> <p>Command mode: Interface port</p> |
| <pre>pvid <VLAN number></pre> <p>Sets the default VLAN number which will be used to forward frames which are not VLAN tagged. The default number is 1 for non-management ports.</p> <p>Command mode: Interface port</p> |
| <pre>name <1-64 characters></pre> <p>Sets a name for the port. The assigned port name appears next to the port number on some information and statistics screens. The default is set to None.</p> <p>Command mode: Interface port</p> |
| <pre>unicast-bandwidth <10-100></pre> <p>Configures the allocated bandwidth percentage for unicast traffic on the port. The remaining bandwidth is automatically allocated to multicast traffic. The default value is 50.</p> <p>Command mode: Interface port</p> |
| <pre>unicast-bandwidth global <10-100></pre> <p>Configures the allocated bandwidth percentage for unicast traffic on the egress ports. The remaining bandwidth is automatically allocated to multicast traffic. The default value is 50. This applies to all ports.</p> <p>Command mode: Interface port</p> |
| <pre>[no] bpdu-guard</pre> <p>Enables or disables BPDU guard, to avoid spanning-tree loops on ports with Port Fast Forwarding enabled.</p> <p>Command mode: Interface port</p> |
| <pre>[no] dscp-marking</pre> <p>Enables or disables DSCP re-marking on a port.</p> <p>Command mode: Interface port</p> |

Table 171. Port Configuration Commands (continued)

| Command Syntax and Usage | |
|---|---|
| [no] reflective-relay force | <p>Enables or disables constraint to always keep reflective relay active. Default setting is disabled.</p> <p>Command mode: Interface port</p> |
| [no] rmon | <p>Enables or disables Remote Monitoring for the port. RMON must be enabled for any RMON configurations to function.</p> <p>Command mode: Interface port</p> |
| [no] tagging | <p>Disables or enables VLAN tagging for this port. The default setting is disabled for external ports (EXT_x) and enabled for internal server ports (INT_x).</p> <p>Command mode: Interface port</p> |
| [no] tag-pvid | <p>Disables or enables VLAN tag persistence. When disabled, the VLAN tag is removed from packets whose VLAN tag matches the port PVID. The default setting is disabled for internal server ports (INT_x) and external ports (EXT_x), and enabled for management (MGT_x) ports.</p> <p>Command mode: Interface port</p> |
| [no] tagpvid-ingress | <p>Enables or disables tagging the ingress frames with the port's VLAN ID. When enabled, the PVID tag is inserted into untagged and 802.1Q single-tagged ingress frames as outer VLAN ID. The default setting is disabled.</p> <p>Command mode: Interface port/Interface portchannel</p> |
| [no] flood-blocking | <p>Enables or disables port Flood Blocking. When enabled, unicast and multicast packets with unknown destination MAC addresses are blocked from the port.</p> <p>Command mode: Interface port</p> |
| [no] mac-address-table mac-notification | <p>Enables or disables MAC Address Notification. With MAC Address Notification enabled, the switch generates a syslog message when a MAC address is added or removed from the MAC address table.</p> <p>Command mode: Interface port/Interface portchannel</p> |
| [no] learning | <p>Enables or disables FDB learning on the port.</p> <p>Command mode: Interface port</p> |
| port-channel min-links <1-32> | <p>Set the minimum number of links for this port. If the specified minimum number of ports are not available, the trunk is placed in the down state.</p> <p>Command mode: Interface port</p> |

Table 171. Port Configuration Commands (continued)

| Command Syntax and Usage | |
|--|--|
| [no] broadcast-threshold <0-262143> | Limits the number of broadcast packets per second to the specified value. If disabled, the port forwards all broadcast packets. Command mode: Interface port |
| [no] multicast-threshold <0-262143> | Limits the number of multicast packets per second to the specified value. If disabled, the port forwards all multicast packets. Command mode: Interface port |
| [no] dest-lookup-threshold <0-262143> | Limits the number of unknown unicast packets per second to the specified value. If disabled, the port forwards all unknown unicast packets. Command mode: Interface port |
| no shutdown | Enables the port. Command mode: Interface port |
| shutdown | Disables the port. (To temporarily disable a port without changing its configuration attributes, refer to “Temporarily Disabling a Port” on page 288.) Command mode: Interface port |
| show interface port <port alias or number> | Displays current port parameters. Command mode: All |

Port Error Disable and Recovery Configuration

The Error Disable and Recovery feature allows the switch to automatically disable a port if an error condition is detected on the port. The port remains in the error-disabled state until it is re-enabled manually, or re-enabled automatically by the switch after a timeout period has elapsed. The error-disabled state of a port does not persist across a system reboot.

Table 172. Port Error Disable Commands

| Command Syntax and Usage |
|---|
| <pre>errdisable recovery</pre> <p>Enables automatic error-recovery for the port. The default setting is enabled.</p> <p>Note: Error-recovery must be enabled globally before port-level commands become active.</p> <p>Command mode: Interface port</p> |
| <pre>no errdisable recovery</pre> <p>Enables automatic error-recovery for the port.</p> <p>Command mode: Interface port</p> |
| <pre>show interface port <port alias or number> errdisable</pre> <p>Displays current port Error Disable parameters.</p> <p>Command mode: All</p> |

Port Link Configuration

Use these commands to set flow control for the port link.

Table 173. Port Link Configuration Commands

| Command Syntax and Usage |
|--|
| <pre>speed {10 100 1000 10000 auto}</pre> <p>Sets the link speed. Some options are not valid on all ports. The choices include:</p> <ul style="list-style-type: none"> – 1000 Mbps – 10000 Mps – any (auto negotiate port speed) <p>Command mode: Interface port</p> |
| <pre>duplex {full half any}</pre> <p>Sets the operating mode. The choices include:</p> <ul style="list-style-type: none"> – Any negotiation (default) – Half-duplex – Full-duplex <p>Command mode: Interface port</p> |

Table 173. Port Link Configuration Commands

| Command Syntax and Usage |
|---|
| <pre>flowcontrol {receive send} [on off]</pre> <p>Sets the flow control. The choices include:</p> <ul style="list-style-type: none"> – Receive flow control – Transmit flow control – No flow control <p>Note: For external ports (EXTx) the default setting is no flow control, and for internal ports (INTx) the default setting is both receive and transmit.</p> <p>Command mode: Interface port</p> |
| <pre>[no] auto</pre> <p>Turns auto-negotiation on or off.</p> <p>Command mode: Interface port</p> |
| <pre>show interface port <port alias or number></pre> <p>Displays current port parameters.</p> <p>Command mode: All</p> |

Temporarily Disabling a Port

To temporarily disable a port without changing its stored configuration attributes, enter the following command at any prompt:

```
Router# interface port <port alias or number> shutdown
```

Because this configuration sets a temporary state for the port, you do not need to use a save operation. The port state will revert to its original configuration when the EN4093 and EN4093R 10Gb Scalable Switch is reset. See the [“Operations Commands” on page 503](#) for other operations-level commands.

Unidirectional Link Detection Configuration

UDLD commands are described in the following table.

Table 174. Port UDLD Configuration Commands

| Command Syntax and Usage |
|--|
| <pre>[no] udld</pre> <p>Enables or disables UDLD on the port.</p> <p>Command mode: Interface port</p> |
| <pre>[no] udld aggressive</pre> <p>Configures the UDLD mode for the selected port, as follows:</p> <ul style="list-style-type: none">– Normal: Detect unidirectional links that have mis-connected interfaces. The port is disabled if UDLD determines that the port is mis-connected. Use the “no” form to select normal operation.– Aggressive: In addition to the normal mode, the aggressive mode disables the port if the neighbor stops sending UDLD probes for 7 seconds. <p>Command mode: Interface port</p> |
| <pre>show interface port <port number> udld</pre> <p>Displays current port UDLD parameters.</p> <p>Command mode: All</p> |

Port OAM Configuration

Operation, Administration, and Maintenance (OAM) protocol allows the switch to detect faults on the physical port links. OAM is described in the IEEE 802.3ah standard. OAM Discovery commands are described in the following table.

Table 175. Port OAM Configuration Commands

| Command Syntax and Usage |
|---|
| <pre>oam {active passive}</pre> <p>Configures the OAM discovery mode, as follows:</p> <ul style="list-style-type: none"> – Active: This port link initiates OAM discovery. – Passive: This port allows its peer link to initiate OAM discovery. <p>If OAM determines that the port is in an anomalous condition, the port is disabled.</p> <p>Command mode: Interface port</p> |
| <pre>no oam {active passive}</pre> <p>Disables OAM discovery on the port.</p> <p>Command mode: Interface port</p> |
| <pre>show interface port <port number> oam</pre> <p>Displays current port OAM parameters.</p> <p>Command mode: All</p> |

Port ACL Configuration

The following table describes port ACL configuration commands

Table 176. Port ACL/QoS Configuration Commands

| Command Syntax and Usage |
|---|
| <pre>[no] access-control list <ACL number></pre> <p>Adds or removes the specified ACL. You can add multiple ACLs to a port.</p> <p>Command mode: Interface port</p> |
| <pre>[no] access-control list6 <ACL number></pre> <p>Adds or removes the specified IPv6 ACL. You can add multiple ACLs to a port.</p> <p>Command mode: Interface port</p> |
| <pre>[no] access-control group <ACL group number></pre> <p>Adds or removes the specified ACL group. You can add multiple ACL groups to a port.</p> <p>Command mode: Interface port</p> |
| <pre>show interface port <port alias or number> access-control</pre> <p>Displays current ACL QoS parameters.</p> <p>Command mode: All</p> |

Port Spanning Tree Configuration

Table 177. Port STP Commands

| Command Syntax and Usage |
|--|
| <pre>[no] spanning-tree portfast</pre> <p>Enables or disables this port as an edge port. An edge port is not connected to a bridge, and can begin forwarding traffic as soon as the link is up. Configure server ports as edge ports (enabled).</p> <p>Note: After you configure the port as an edge port, you must disable the port and then re-enable the port for the change to take effect.</p> <p>Command mode: Interface port</p> |
| <pre>[no] spanning-tree link-type p2p shared</pre> <p>Defines the type of link connected to the port, as follows:</p> <ul style="list-style-type: none"> – no: Configures the port to detect the link type, and automatically match its settings. – p2p: Configures the port for Point-To-Point protocol. – shared: Configures the port to connect to a shared medium (usually a hub). <p>The default link type is auto.</p> <p>Command mode: Interface port</p> |
| <pre>show interface port {<port alias or number>}</pre> <p>Displays current port configuration parameters.</p> <p>Command mode: All</p> |

Port Spanning Tree Guard Configuration

Table 178. Port STP Guard Options

| Command Syntax and Usage |
|---|
| <pre>spanning-tree guard loop</pre> <p>Enables STP loop guard. STP loop guard prevents the port from forwarding traffic if no BPDUs are received. The port is placed into a loop-inconsistent blocking state until a BPDU is received.</p> <p>Command mode: Interface port/Interface portchannel</p> |
| <pre>spanning-tree guard root</pre> <p>Enables STP root guard. STP root guard enforces the position of the root bridge. If the bridge receives a superior BPDU, the port is placed into a root-inconsistent state (listening).</p> <p>Command mode: Interface port/Interface portchannel</p> |

Table 178. Port STP Guard Options

| Command Syntax and Usage |
|--|
| <pre>spanning-tree guard none</pre> <p>Disables STP loop guard and root guard.</p> <p>Command mode: Interface port/Interface portchannel</p> |
| <pre>no spanning-tree guard</pre> <p>Sets the Spanning Tree guard parameters to their default values.</p> <p>Command mode: Interface port/Interface portchannel</p> |

Port WRED Configuration

These commands allow you to configure Weighted Random Early Detection (WRED) parameters for a selected port. For global WRED configuration, see [“Weighted Random Early Detection Configuration” on page 300](#).

Table 179. Port WRED Options

| Command Syntax and Usage |
|--|
| <pre>[no] random-detect ecn enable</pre> <p>Enables or disables Explicit Congestion Notification (ECN). When ECN is on, the switch marks the ECN bit of the packet (if applicable) instead of dropping the packet. ECN-aware devices are notified of the congestion and those devices can take corrective actions.</p> <p>Note: ECN functions only on TCP traffic.</p> <p>Command mode: Interface port</p> |
| <pre>random-detect enable</pre> <p>Turns on Random Detection and avoidance.</p> <p>Command mode: Interface port</p> |
| <pre>no random-detect enable</pre> <p>Turns off Random Detection and avoidance.</p> <p>Command mode: Interface port</p> |
| <pre>show interface port <port alias or number> random-detect</pre> <p>Displays current Random Detection and avoidance parameters.</p> <p>Command mode: All</p> |

Port WRED Transmit Queue Configuration

Use this menu to define WRED thresholds for the port's transmit queues. Set each threshold between 1% and 100%. When the average queue size grows beyond the minimum threshold, packets begin to be dropped. When the average queue size reaches the maximum threshold, all packets are dropped. The probability of packet-drop between the thresholds is defined by the drop rate.

Table 180. Port WRED Transmit Queue Options

| Command Syntax and Usage |
|--|
| <pre>[no] random-detect transmit-queue <0-7> tcp <min. threshold (1-100)> <max. threshold (1-100)> <drop rate (1-100)></pre> <p>Configures the WRED thresholds for TCP traffic. Use the <code>no</code> form to clear the WRED threshold value.</p> <p>Command mode: Interface port</p> |
| <pre>[no] random-detect transmit-queue <0-7> non-tcp <min. threshold (1-100)> <max. threshold (1-100)> <drop rate (1-100)></pre> <p>Configures the WRED thresholds for non-TCP traffic. Use the <code>no</code> form to clear the WRED threshold value.</p> <p>Command mode: Interface port</p> |
| <pre>random-detect transmit-queue <0-7> enable</pre> <p>Sets the WRED transmit queue configuration to <code>on</code>.</p> <p>Command mode: Interface port</p> |
| <pre>no random-detect transmit-queue <0-7> enable</pre> <p>Sets the WRED transmit queue configuration to <code>off</code>.</p> <p>Command mode: Interface port</p> |

Management Port Configuration

You can use these commands to set port parameters for management ports (MGT1 and EXTM). Use these commands to set port parameters for the port link. For MGT1, the values for speed, duplex, and flow control are fixed, and cannot be configured.

Table 181. Management Port Configuration Commands

| Command Syntax and Usage |
|---|
| <pre>speed {10 100 1000 auto}</pre> <p>Sets the link speed. The choices include:</p> <ul style="list-style-type: none"> – 10 Mbps – 100 Mbps – 1000 Mbps – Auto — for auto negotiation <p>Command mode: Interface port</p> |

Table 181. Management Port Configuration Commands (continued)

| Command Syntax and Usage |
|---|
| <p><code>duplex {full half any}</code></p> <p>Sets the operating mode. The choices include:</p> <ul style="list-style-type: none"> – Full-duplex – Half-duplex – Any — for auto negotiation (default) <p>Command mode: Interface port</p> |
| <p><code>[no] flowcontrol {receive send both}</code></p> <p>Sets the flow control. The choices include:</p> <ul style="list-style-type: none"> – Receive flow control – Transmit flow control – Both receive and transmit flow control (default) – No flow control <p>Command mode: Interface port</p> |
| <p><code>no shutdown</code></p> <p>Enables the port.</p> <p>Command mode: Interface port</p> |
| <p><code>shutdown</code></p> <p>Disables the port.</p> <p>Command mode: Interface port</p> |
| <p><code>show interface port <port alias or number></code></p> <p>Displays current port parameters.</p> <p>Command mode: All</p> |

Stacking Configuration

A *stack* is a group of switches that work together as a unified system. The network views a stack of switches as a single entity, identified by a single network IP address. The Stacking Configuration menu is used to configure a stack, and to define the Master and Backup interface that represents the stack on the network.

The Stacking Configuration menu is available only after Stacking is enabled and the switch is reset. For more information, see [“Stacking Boot Options” on page 517](#).

Table 182. Stacking Commands

| Command Syntax and Usage |
|--|
| [no] stack name <1-63 characters> Defines a name for the stack. Command mode: Global configuration |
| [no] stack backup <csnum (1-8)> Defines the backup switch in the stack, based on its configured switch number (csnum). Command mode: Global configuration |
| show stack switch-number <csnum (1-8)> Displays the current stacking parameters. Command mode: All |

Stacking Switch Configuration

The following table describes stacking switch configuration commands

Table 183. Stacking Switch Commands

| Command Syntax and Usage |
|---|
| <pre>stack switch-number <csnum (1-8)> bay <1-4></pre> <p>Binds the selected switch to the stack, based on its bay number in the chassis. You also must enter the UUID to specify the chassis in which the switch resides.</p> <p>Command mode: Global configuration</p> |
| <pre>stack switch-number <csnum (1-8)> bind <asnum (1-16)></pre> <p>Binds the selected switch to the stack, based on its assigned switch number (asnum).</p> <p>Command mode: Global configuration</p> |
| <pre>no stack switch-number <csnum (1-8)></pre> <p>Deletes the selected switch from the stack.</p> <p>Command mode: Global configuration</p> |
| <pre>show stack attached-switches</pre> <p>Displays the current stacking switch parameters.</p> <p>Command mode: All</p> |

Quality of Service Configuration

Quality of Service (QoS) commands configure the 802.1p priority value and DiffServ Code Point value of incoming packets. This allows you to differentiate between various types of traffic, and provide different priority levels.

802.1p Configuration

This feature provides the EN4093 and EN4093R the capability to filter IP packets based on the 802.1p bits in the packet's VLAN header. The 802.1p bits specify the priority that you should give to the packets while forwarding them. The packets with a higher (non-zero) priority bits are given forwarding preference over packets with numerically lower priority bits value.

Table 184. 802.1p Configuration Commands

| Command Syntax and Usage |
|--|
| <pre>qos transmit-queue mapping <priority (0-7)> <COSq number></pre> <p>Maps the 802.1p priority of to the Class of Service queue (COSq) priority. Enter the 802.1p priority value (0-7), followed by the Class of Service queue that handles the matching traffic.</p> <p>Command mode: Global configuration</p> |
| <pre>qos transmit-queue weight-cos <COSq number> <weight (0-15)></pre> <p>Configures the weight of the selected Class of Service queue (COSq). Enter the queue number (0-1), followed by the scheduling weight (0-15).</p> <p>Command mode: Global configuration</p> |
| <pre>show qos transmit-queue</pre> <p>Displays the current 802.1p parameters.</p> <p>Command mode: All</p> |
| <pre>qos unicast-bandwidth <10-100></pre> <p>Configures the allocated bandwidth percentage for unicast traffic on the egress ports. The remaining bandwidth is automatically allocated to multicast traffic. The default value is 50. This applies to all ports.</p> <p>Command mode: All</p> |

DSCP Configuration

These commands map the DiffServ Code Point (DSCP) value of incoming packets to a new value or to an 802.1p priority value.

Table 185. DSCP Configuration Commands

| Command Syntax and Usage | |
|--|---|
| <pre>qos dscp dscp-mapping <DSCP (0-63)> <new DSCP (0-63)></pre> | <p>Maps the initial DiffServ Code Point (DSCP) value to a new value. Enter the DSCP value (0-63) of incoming packets, followed by the new value.</p> <p>Command mode: Global configuration</p> |
| <pre>qos dscp dot1p-mapping <DSCP (0-63)> <priority (0-7)></pre> | <p>Maps the DiffServ Code point value to an 802.1p priority value. Enter the DSCP value, followed by the corresponding 802.1p value.</p> <p>Command mode: Global configuration</p> |
| <pre>qos dscp re-marking</pre> | <p>Turns on DSCP re-marking globally.</p> <p>Command mode: Global configuration</p> |
| <pre>no qos dscp re-marking</pre> | <p>Turns off DSCP re-marking globally.</p> <p>Command mode: Global configuration</p> |
| <pre>show qos dscp</pre> | <p>Displays the current DSCP parameters.</p> <p>Command mode: All</p> |

Control Plane Protection

To prevent switch instability if the switch is unable to process a high rate of control-plane traffic, the switch now supports CoPP. CoPP, allows you to assign control-plane traffic protocols to one of 48 queues, and can set bandwidth limits for each queue.

Table 186. CoPP Commands

| Command Syntax and Usage |
|---|
| <p><code>qos protocol-packet-control packet-queue-map <packet queue number (0-47)> <packet type></code></p> <p>Configures a packet type to associate with each packet queue number. Enter a queue number, followed by the packet type. You may map multiple packet types to a single queue. The following packet types are allowed:</p> <ul style="list-style-type: none"> – 802.1x (IEEE 802.1x packets) – application-cri-packets (critical packets of various applications, such as Telnet, SSH) – arp-bcast (ARP broadcast packets) – arp-ucast (ARP unicast reply packets) – bgp (BGP packets) – bpdu (Spanning Tree Protocol packets) – cisco-bpdu (Cisco STP packets) – dest-unknown (packets with destination not yet learned) – dhcp (DHCP packets) – icmp (ICMP packets) – igmp (IGMP packets) – ipv4-miscellaneous (IPv4 packets with IP options and TTL exception) – ipv6-nd (IPv6 Neighbor Discovery packets) – lacp (LACP/Link Aggregation protocol packets) – lldp (LLDP packets) – ospf (OSPF packets) – ospf3 (OSPF3 Packets) – pim (PIM packets) – ptp (PTP packets) – rip (RIP packets) – system (system protocols, such as tftp, ftp, telnet, ssh) – udld (UDLD packets) – vlag (vLAG packets) – vrrp (VRRP packets) <p>Command mode: Global configuration</p> |
| <p><code>qos protocol-packet-control rate-limit-packet-queue <packet queue number (0-47)> <1-10000></code></p> <p>Configures the number of packets per second allowed for each packet queue.</p> <p>Command mode: Global configuration</p> |

Table 186. CoPP Commands

| Command Syntax and Usage |
|--|
| <pre>no qos protocol-packet-control packet-queue-map <packet type></pre> <p>Clears the selected packet type from its associated packet queue.</p> <p>Command mode: Global configuration</p> |
| <pre>no qos protocol-packet-control rate-limit-packet-queue <packet queue number (0-47)></pre> <p>Clears the packet rate configured for the selected packet queue.</p> <p>Command mode: Global configuration</p> |
| <pre>show qos protocol-packet-control information protocol</pre> <p>Displays of mapping of protocol packet types to each packet queue number. The status indicates whether the protocol is running or not running.</p> <p>Command mode: All</p> |
| <pre>show qos protocol-packet-control information queue</pre> <p>Displays the packet rate configured for each packet queue.</p> <p>Command mode: All</p> |

Weighted Random Early Detection Configuration

Weighted Random Early Detection (WRED) provides congestion avoidance by pre-emptively dropping packets before a queue becomes full. EN4093 and EN4093R implementation of WRED defines TCP and non-TCP traffic profiles on a per-port, per COS queue basis. For each port, you can define a transmit-queue profile with thresholds that define packet-drop probability.

These commands allow you to configure global WRED parameters. For port WRED commands, see [“Port WRED Configuration” on page 292](#).

Table 187. WRED Configuration Options

| Command Syntax and Usage |
|--|
| <pre>qos random-detect ecn</pre> <p>Enables or disables Explicit Congestion Notification (ECN). When ECN is on, the switch marks the ECN bit of the packet (if applicable) instead of dropping the packet. ECN-aware devices are notified of the congestion and those devices can take corrective actions.</p> <p>Note: ECN functions only on TCP traffic.</p> <p>Command mode: Global configuration</p> |
| <pre>qos random-detect enable</pre> <p>Turns on Random Detection and avoidance.</p> <p>Command mode: Global configuration</p> |

Table 187. WRED Configuration Options

| Command Syntax and Usage |
|--|
| <pre>no qos random-detect enable</pre> <p>Turns off Random Detection and avoidance.</p> <p>Command mode: Global configuration</p> |
| <pre>show qos random-detect</pre> <p>Displays current Random Detection and avoidance parameters.</p> <p>Command mode: All</p> |

WRED Transmit Queue Configuration

Table 188. WRED Transmit Queue Options

| Command Syntax and Usage |
|--|
| <pre>[no] qos random-detect transmit-queue <0-7> tcp <min. threshold (1-100)> <max. threshold (1-100)> <drop rate (1-100)></pre> <p>Configures the WRED thresholds for TCP traffic. Use the <code>no</code> form to clear the WRED threshold value.</p> <p>Command mode: Global configuration</p> |
| <pre>[no] qos random-detect transmit-queue <0-7> non-tcp <min. threshold (1-100)> <max. threshold (1-100)> <drop rate (1-100)></pre> <p>Configures the WRED thresholds for non-TCP traffic. Use the <code>no</code> form to clear the WRED threshold value.</p> <p>Command mode: Global configuration</p> |
| <pre>qos random-detect transmit-queue <0-7> enable</pre> <p>Sets the WRED transmit queue configuration to <code>on</code>.</p> <p>Command mode: Global configuration</p> |
| <pre>no qos random-detect transmit-queue <0-7> enable</pre> <p>Sets the WRED transmit queue configuration to <code>off</code>.</p> <p>Command mode: Global configuration</p> |

Access Control Configuration

Use these commands to create Access Control Lists and ACL Groups. ACLs define matching criteria used for IP filtering and Quality of Service functions.

For information about assigning ACLs to ports, see [“Port ACL Configuration” on page 290](#).

Table 189. General ACL Configuration Commands

| Command Syntax and Usage |
|--|
| <pre>[no] access-control list <1-640></pre> <p>Configures an Access Control List.</p> <p>Command mode: Global configuration</p> <p>To view command options, see page 303.</p> |
| <pre>[no] access-control group <1-640></pre> <p>Configures an ACL Group.</p> <p>Command mode: Global configuration</p> <p>To view command options, see page 317.</p> |
| <pre>show access-control</pre> <p>Displays the current ACL parameters.</p> <p>Command mode: All</p> |

Access Control List Configuration

These commands allow you to define filtering criteria for each Access Control List (ACL).

Table 190. ACL Configuration Commands

| Command Syntax and Usage |
|--|
| <pre>[no] access-control list <1-640> egress-port port <port alias or number></pre> <p>Configures the ACL to function on egress packets.</p> <p>Command mode: Global configuration</p> |
| <pre>access-control list <1-640> action {permit deny set-priority <0-7>}</pre> <p>Configures a filter action for packets that match the ACL definitions. You can choose to permit (pass) or deny (drop) packets, or set the 802.1p priority level (0-7).</p> <p>Command mode: Global configuration</p> |
| <pre>[no] access-control list <1-640> statistics</pre> <p>Enables or disables the statistics collection for the Access Control List.</p> <p>Command mode: Global configuration</p> |
| <pre>default access-control list <1-640></pre> <p>Resets the ACL parameters to their default values.</p> <p>Command mode: Global configuration</p> |
| <pre>show access-control list <1-640></pre> <p>Displays the current ACL parameters.</p> <p>Command mode: All</p> |
| <pre>[no] access-control list6 <1-128></pre> <p>Configures an IPv6 Access Control List. To view command options, see page 307.</p> <p>Command mode: Global configuration</p> |

Ethernet Filtering Configuration

These commands allow you to define Ethernet matching criteria for an ACL.

Table 191. Ethernet Filtering Configuration Commands

| Command Syntax and Usage |
|---|
| <pre>[no] access-control list <I-640> ethernet source-mac-address <MAC address> <MAC mask></pre> <p>Defines the source MAC address for this ACL.</p> <p>Command mode: Global configuration</p> |
| <pre>[no] access-control list <I-640> ethernet destination-mac-address <MAC address> <MAC mask></pre> <p>Defines the destination MAC address for this ACL.</p> <p>Command mode: Global configuration</p> |
| <pre>[no] access-control list <I-640> ethernet vlan <VLAN ID> <VLAN mask></pre> <p>Defines a VLAN number and mask for this ACL.</p> <p>Command mode: Global configuration</p> |
| <pre>[no] access-control list <I-640> ethernet ethernet-type {arp ip ipv6 mpls rarp any <other (0x600-0xFFFF)>}</pre> <p>Defines the Ethernet type for this ACL.</p> <p>Command mode: Global configuration</p> |
| <pre>[no] access-control list <I-640> ethernet priority <0-7></pre> <p>Defines the Ethernet priority value for the ACL.</p> <p>Command mode: Global configuration</p> |
| <pre>default access-control list <I-640> ethernet</pre> <p>Resets Ethernet parameters for the ACL to their default values.</p> <p>Command mode: Global configuration</p> |
| <pre>no access-control list <I-640> ethernet</pre> <p>Removes Ethernet parameters for the ACL.</p> <p>Command mode: Global configuration</p> |
| <pre>show access-control list <I-640> ethernet</pre> <p>Displays the current Ethernet parameters for the ACL.</p> <p>Command mode: All</p> |

IPv4 Filtering Configuration

These commands allow you to define IPv4 matching criteria for an ACL.

Table 192. IP version 4 Filtering Configuration Commands

| Command Syntax and Usage | | | | | | | | | | | | | | | |
|---|---|--------|------|---|------|---|------|---|-----|----|-----|----|------|-----|------|
| [no] access-control list <1-640> ipv4 source-ip-address <IP address> <IP mask> | <p>Defines a source IP address for the ACL. If defined, traffic with this source IP address will match this ACL. Specify an IP address in dotted decimal notation.</p> <p>Command mode: Global configuration</p> | | | | | | | | | | | | | | |
| [no] access-control list <1-640> ipv4 destination-ip-address <IP address> <IP mask> | <p>Defines a destination IP address for the ACL. If defined, traffic with this destination IP address will match this ACL.</p> <p>Command mode: Global configuration</p> | | | | | | | | | | | | | | |
| [no] access-control list <1-640> ipv4 protocol <0-255> | <p>Defines an IP protocol for the ACL. If defined, traffic from the specified protocol matches this filter. Specify the protocol number. Listed below are some of the well-known protocols.</p> <table border="1"> <thead> <tr> <th>Number</th> <th>Name</th> </tr> </thead> <tbody> <tr> <td>1</td> <td>icmp</td> </tr> <tr> <td>2</td> <td>igmp</td> </tr> <tr> <td>6</td> <td>tcp</td> </tr> <tr> <td>17</td> <td>udp</td> </tr> <tr> <td>89</td> <td>ospf</td> </tr> <tr> <td>112</td> <td>vrrp</td> </tr> </tbody> </table> <p>Command mode: Global configuration</p> | Number | Name | 1 | icmp | 2 | igmp | 6 | tcp | 17 | udp | 89 | ospf | 112 | vrrp |
| Number | Name | | | | | | | | | | | | | | |
| 1 | icmp | | | | | | | | | | | | | | |
| 2 | igmp | | | | | | | | | | | | | | |
| 6 | tcp | | | | | | | | | | | | | | |
| 17 | udp | | | | | | | | | | | | | | |
| 89 | ospf | | | | | | | | | | | | | | |
| 112 | vrrp | | | | | | | | | | | | | | |
| [no] access-control list <1-640> ipv4 type-of-service <0-255> | <p>Defines a Type of Service (ToS) value for the ACL. For more information on ToS, refer to RFC 1340 and 1349.</p> <p>Command mode: Global configuration</p> | | | | | | | | | | | | | | |
| default access-control list <1-640> ipv4 | <p>Resets the IPv4 parameters for the ACL to their default values.</p> <p>Command mode: Global configuration</p> | | | | | | | | | | | | | | |
| show access-control list <1-640> ipv4 | <p>Displays the current IPv4 parameters.</p> <p>Command mode: All</p> | | | | | | | | | | | | | | |

TCP/UDP Filtering Configuration

These commands allow you to define TCP/UDP matching criteria for an ACL.

Table 193. TCP/UDP Filtering Configuration Commands

| Command Syntax and Usage | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
|--|---|--------|------|----|----------|----|-----|----|-----|----|--------|----|------|----|------|----|------|----|-------|----|--------|----|------|----|--------|----|--------|----|------|
| <pre>[no] access-control list <1-640> tcp-udp source-port <1-65535> <mask (0xFFFF)></pre> | <p>Defines a source port for the ACL. If defined, traffic with the specified TCP or UDP source port will match this ACL. Specify the port number. Listed below are some of the well-known ports:</p> <table border="1"> <thead> <tr> <th>Number</th> <th>Name</th> </tr> </thead> <tbody> <tr><td>20</td><td>ftp-data</td></tr> <tr><td>21</td><td>ftp</td></tr> <tr><td>22</td><td>ssh</td></tr> <tr><td>23</td><td>telnet</td></tr> <tr><td>25</td><td>smtp</td></tr> <tr><td>37</td><td>time</td></tr> <tr><td>42</td><td>name</td></tr> <tr><td>43</td><td>whois</td></tr> <tr><td>53</td><td>domain</td></tr> <tr><td>69</td><td>tftp</td></tr> <tr><td>70</td><td>gopher</td></tr> <tr><td>79</td><td>finger</td></tr> <tr><td>80</td><td>http</td></tr> </tbody> </table> <p>Command mode: Global configuration</p> | Number | Name | 20 | ftp-data | 21 | ftp | 22 | ssh | 23 | telnet | 25 | smtp | 37 | time | 42 | name | 43 | whois | 53 | domain | 69 | tftp | 70 | gopher | 79 | finger | 80 | http |
| Number | Name | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 20 | ftp-data | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 21 | ftp | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 22 | ssh | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 23 | telnet | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 25 | smtp | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 37 | time | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 42 | name | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 43 | whois | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 53 | domain | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 69 | tftp | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 70 | gopher | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 79 | finger | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 80 | http | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| <pre>[no] access-control list <1-640> tcp-udp destination-port <1-65535> <mask (0xFFFF)></pre> | <p>Defines a destination port for the ACL. If defined, traffic with the specified TCP or UDP destination port will match this ACL. Specify the port number, just as with <code>sport</code> above.</p> <p>Command mode: Global configuration</p> | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| <pre>[no] access-control list <1-640> tcp-udp flags <value (0x0-0x3f)> <mask (0x0-0x3f)></pre> | <p>Defines a TCP/UDP flag for the ACL.</p> <p>Command mode: Global configuration</p> | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| <pre>default access-control list <1-640> tcp-udp</pre> | <p>Resets the TCP/UDP parameters for the ACL to their default values.</p> <p>Command mode: Global configuration</p> | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| <pre>show access-control list <1-640> tcp-udp</pre> | <p>Displays the current TCP/UDP Filtering parameters.</p> <p>Command mode: All</p> | | | | | | | | | | | | | | | | | | | | | | | | | | | | |

Packet Format Filtering Configuration

These commands allow you to define Packet Format matching criteria for an ACL.

Table 194. Packet Format Filtering Configuration Commands

| Command Syntax and Usage |
|--|
| <pre>[no] access-control list <1-640> packet-format ethernet {ethertype2 snap llc}</pre> <p>Defines the Ethernet format for the ACL.</p> <p>Command mode: Global configuration</p> |
| <pre>[no] access-control list <1-640> packet-format tagging {any none tagged}</pre> <p>Defines the tagging format for the ACL.</p> <p>Command mode: Global configuration</p> |
| <pre>[no] access-control list <1-640> packet-format ip {ipv4 ipv6}</pre> <p>Defines the IP format for the ACL.</p> <p>Command mode: Global configuration</p> |
| <pre>default access-control list <1-640> packet-format</pre> <p>Resets Packet Format parameters for the ACL to their default values.</p> <p>Command mode: Global configuration</p> |
| <pre>show access-control list <1-640> packet-format</pre> <p>Displays the current Packet Format parameters for the ACL.</p> <p>Command mode: All</p> |

ACL IPv6 Configuration

These commands allow you to define filtering criteria for each IPv6 Access Control List (ACL).

Table 195. IPv6 ACL Options

| Command Syntax and Usage |
|--|
| <pre>[no] access-control list6 <1-128> egress-port port <port alias or number></pre> <p>Configures the ACL to function on egress packets.</p> <p>Command mode: Global configuration</p> |
| <pre>access-control list6 <1-128> action {permit deny set-priority <0-7>}</pre> <p>Configures a filter action for packets that match the ACL definitions. You can choose to permit (pass) or deny (drop) packets, or set the 802.1p priority level (0-7).</p> <p>Command mode: Global configuration</p> |
| <pre>[no] access-control list6 <1-128> statistics</pre> <p>Enables or disables the statistics collection for the Access Control List.</p> <p>Command mode: Global configuration</p> |

Table 195. IPv6 ACL Options

| Command Syntax and Usage |
|--|
| <pre>default access-control list6 <1-128></pre> <p>Resets the ACL parameters to their default values. Command mode: Global configuration</p> |
| <pre>show access-control list <1-128></pre> <p>Displays the current ACL parameters. Command mode: All</p> |

IPv6 Filtering Configuration

These commands allow you to define IPv6 matching criteria for an ACL.

Table 196. IP version 6 Filtering Options

| Command Syntax and Usage |
|---|
| <pre>[no] access-control list6 <1-128> ipv6 source-address <IPv6 address> <prefix length (1-128)></pre> <p>Defines a source IPv6 address for the ACL. If defined, traffic with this source address will match this ACL. Command mode: Global configuration</p> |
| <pre>[no] access-control list6 <1-128> ipv6 destination-address <IPv6 address> <prefix length (1-128)></pre> <p>Defines a destination IPv6 address for the ACL. If defined, traffic with this destination address will match this ACL. Command mode: Global configuration</p> |
| <pre>[no] access-control list6 <1-128> ipv6 next-header <0-255></pre> <p>Defines the next header value for the ACL. If defined, traffic with this next header value will match this ACL. Command mode: Global configuration</p> |
| <pre>[no] access-control list6 <1-128> ipv6 flow-label <0-1048575></pre> <p>Defines the flow label for the ACL. If defined, traffic with this flow label will match this ACL. Command mode: Global configuration</p> |
| <pre>[no] access-control list6 <1-128> ipv6 traffic-class <0-255></pre> <p>Defines the traffic class for the ACL. If defined, traffic with this traffic class will match this ACL. Command mode: Global configuration</p> |

Table 196. IP version 6 Filtering Options

| Command Syntax and Usage |
|--|
| <pre>default access-control list6 <I-128> ipv6</pre> <p>Resets the IPv6 parameters for the ACL to their default values.</p> <p>Command mode: Global configuration</p> |
| <pre>show access-control list6 <I-128> ipv6</pre> <p>Displays the current IPv6 parameters.</p> <p>Command mode: All</p> |

IPv6 TCP/UDP Filtering Configuration

These commands allows you to define TCP/UDP matching criteria for an ACL.

Table 197. IPv6 ACL TCP/UDP Filtering Options

| Command Syntax and Usage | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
|---|----------|------|----|----------|----|-----|----|-----|----|--------|----|------|----|------|----|------|----|-------|----|--------|----|------|----|--------|----|--------|----|------|
| <pre>[no] access-control list6 <I-128> tcp-udp source-port <I-65535> <mask (0xFFFF)></pre> <p>Defines a source port for the ACL. If defined, traffic with the specified TCP or UDP source port will match this ACL. Specify the port number. Listed here are some of the well-known ports:</p> <table border="1"> <thead> <tr> <th>Number</th> <th>Name</th> </tr> </thead> <tbody> <tr><td>20</td><td>ftp-data</td></tr> <tr><td>21</td><td>ftp</td></tr> <tr><td>22</td><td>ssh</td></tr> <tr><td>23</td><td>telnet</td></tr> <tr><td>25</td><td>smtp</td></tr> <tr><td>37</td><td>time</td></tr> <tr><td>42</td><td>name</td></tr> <tr><td>43</td><td>whois</td></tr> <tr><td>53</td><td>domain</td></tr> <tr><td>69</td><td>tftp</td></tr> <tr><td>70</td><td>gopher</td></tr> <tr><td>79</td><td>finger</td></tr> <tr><td>80</td><td>http</td></tr> </tbody> </table> <p>Command mode: Global configuration</p> | Number | Name | 20 | ftp-data | 21 | ftp | 22 | ssh | 23 | telnet | 25 | smtp | 37 | time | 42 | name | 43 | whois | 53 | domain | 69 | tftp | 70 | gopher | 79 | finger | 80 | http |
| Number | Name | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 20 | ftp-data | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 21 | ftp | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 22 | ssh | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 23 | telnet | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 25 | smtp | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 37 | time | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 42 | name | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 43 | whois | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 53 | domain | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 69 | tftp | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 70 | gopher | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 79 | finger | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 80 | http | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| <pre>[no] access-control list6 <I-128> tcp-udp destination-port <I-65535> <mask (0xFFFF)></pre> <p>Defines a destination port for the ACL. If defined, traffic with the specified TCP or UDP destination port will match this ACL. Specify the port number, just as with <code>sport</code> above.</p> <p>Command mode: Global configuration</p> | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| <pre>[no] access-control list6 <I-128> tcp-udp flags <value (0x0-0x3f)> <mask (0x0-0x3f)></pre> <p>Defines a TCP/UDP flag for the ACL.</p> <p>Command mode: Global configuration</p> | | | | | | | | | | | | | | | | | | | | | | | | | | | | |

Table 197. IPv6 ACL TCP/UDP Filtering Options

| Command Syntax and Usage |
|--|
| <pre>default access-control list6 <1-128> tcp-udp</pre> <p>Resets the TCP/UDP parameters for the ACL to their default values. Command mode: Global configuration</p> |
| <pre>show access-control list6 <1-128> tcp-udp</pre> <p>Displays the current TCP/UDP Filtering parameters. Command mode: All</p> |

IPv6 Re-Mark Configuration

You can choose to re-mark IP header data for the selected ACL. You can configure different re-mark values, based on whether packets fall within the ACL metering profile, or out of the ACL metering profile.

IPv6 Re-Marking In-Profile Configuration

Table 198. IPv6 Re-Marking In-Profile Options

| Command Syntax and Usage |
|---|
| <pre>[no] access-control list6 <1-128> re-mark dot1p <0-7></pre> <p>Re-marks the 802.1p value. The value is the priority bits information in the packet structure. Command mode: Global configuration</p> |
| <pre>[no] access-control list6 <1-128> re-mark in-profile dscp <0-63></pre> <p>Re-marks the DSCP value for in-profile traffic. Command mode: Global configuration</p> |
| <pre>[no] access-control list6 <1-128> re-mark use-tos-precedence</pre> <p>Enables or disables mapping of TOS (Type of Service) priority to 802.1p priority for in-profile packets. When enabled, the TOS value is used to set the 802.1p value. Command mode: Global configuration</p> |
| <pre>default access-control list6 <1-128> re-mark</pre> <p>Sets the ACL re-mark parameters to their default values. Command mode: Global configuration</p> |
| <pre>show access-control list6 <1-128> re-mark</pre> <p>Displays current re-mark parameters. Command mode: All</p> |

Management ACL Filtering Configuration

These commands allow you to define matching criteria for a Management ACL.

Table 199. Management ACL Filtering Configuration Commands

| Command Syntax and Usage | | | | | | | | | | | | | | | |
|---|---|--------|------|---|------|---|------|---|-----|----|-----|----|------|-----|------|
| [no] access-control macl <1-640> ipv4 | <p>Enables the Management ACL.</p> <p>Command mode: Global configuration</p> | | | | | | | | | | | | | | |
| [no] access-control macl <1-640> ipv4 <source IP address> [<address mask>] | <p>Sets IPv4 filtering to filter on the source IP address.</p> <p>Command mode: Global configuration</p> | | | | | | | | | | | | | | |
| [no] access-control macl <1-640> ipv4 <destination IP address> [<address mask>] | <p>Sets IPv4 filtering to filter on the destination IP address.</p> <p>Command mode: Global configuration</p> | | | | | | | | | | | | | | |
| [no] access-control macl <1-640>ipv4 protocol <0-255> | <p>Defines an IP protocol for the MACL. If defined, traffic from the specified protocol matches this filter. Specify the protocol number. Listed here are some of the well-known protocols.</p> <table border="1"> <thead> <tr> <th>Number</th> <th>Name</th> </tr> </thead> <tbody> <tr> <td>1</td> <td>icmp</td> </tr> <tr> <td>2</td> <td>igmp</td> </tr> <tr> <td>6</td> <td>tcp</td> </tr> <tr> <td>17</td> <td>udp</td> </tr> <tr> <td>89</td> <td>ospf</td> </tr> <tr> <td>112</td> <td>vrrp</td> </tr> </tbody> </table> <p>Command mode: Global configuration</p> | Number | Name | 1 | icmp | 2 | igmp | 6 | tcp | 17 | udp | 89 | ospf | 112 | vrrp |
| Number | Name | | | | | | | | | | | | | | |
| 1 | icmp | | | | | | | | | | | | | | |
| 2 | igmp | | | | | | | | | | | | | | |
| 6 | tcp | | | | | | | | | | | | | | |
| 17 | udp | | | | | | | | | | | | | | |
| 89 | ospf | | | | | | | | | | | | | | |
| 112 | vrrp | | | | | | | | | | | | | | |
| default access-control list <1-640> ipv4 | <p>Resets the IPv4 parameters for the ACL to their default values.</p> <p>Command mode: Global configuration</p> | | | | | | | | | | | | | | |
| show access-control list <1-640> packet-format | <p>Displays the current Packet Format parameters for the ACL.</p> <p>Command mode: All</p> | | | | | | | | | | | | | | |

TCP/UDP Filtering Configuration

The following commands allow you to define TCP/UDP matching criteria for a Management ACL.

Table 200. Management ACL TCP/UDP Filtering Configuration Commands

| Command Syntax and Usage | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
|--|--|--------|------|----|----------|----|-----|----|-----|----|--------|----|------|----|------|----|------|----|-------|----|--------|----|------|----|--------|----|--------|----|------|
| <pre>[no] access-control macl <I-640> tcp-udp source-port <I-65535> [<mask (0x0-0x3f)>]</pre> | <p>Defines a source port for the Management ACL. If defined, traffic with the specified TCP or UDP source port will match this Management ACL. Specify the port number. Listed here are some of the well-known ports:</p> <table border="1"> <thead> <tr> <th>Number</th> <th>Name</th> </tr> </thead> <tbody> <tr><td>20</td><td>ftp-data</td></tr> <tr><td>21</td><td>ftp</td></tr> <tr><td>22</td><td>ssh</td></tr> <tr><td>23</td><td>telnet</td></tr> <tr><td>25</td><td>smtp</td></tr> <tr><td>37</td><td>time</td></tr> <tr><td>42</td><td>name</td></tr> <tr><td>43</td><td>whois</td></tr> <tr><td>53</td><td>domain</td></tr> <tr><td>69</td><td>tftp</td></tr> <tr><td>70</td><td>gopher</td></tr> <tr><td>79</td><td>finger</td></tr> <tr><td>80</td><td>http</td></tr> </tbody> </table> <p>Command mode: Global configuration</p> | Number | Name | 20 | ftp-data | 21 | ftp | 22 | ssh | 23 | telnet | 25 | smtp | 37 | time | 42 | name | 43 | whois | 53 | domain | 69 | tftp | 70 | gopher | 79 | finger | 80 | http |
| Number | Name | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 20 | ftp-data | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 21 | ftp | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 22 | ssh | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 23 | telnet | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 25 | smtp | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 37 | time | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 42 | name | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 43 | whois | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 53 | domain | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 69 | tftp | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 70 | gopher | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 79 | finger | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 80 | http | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| <pre>[no] access-control macl <I-640> tcp-udp destination-port <I-65535> [<mask (0xFFFF)>]</pre> | <p>Defines a destination port for the Management ACL. If defined, traffic with the specified TCP or UDP destination port will match this Management ACL. Specify the port number, just as with <code>sport</code>.</p> <p>Command mode: Global configuration</p> | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| <pre>default access-control list <I-640> tcp-udp</pre> | <p>Resets the TCP/UDP parameters for the ACL to their default values.</p> <p>Command mode: Global configuration</p> | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| <pre>show access-control list <I-640> tcp-udp</pre> | <p>Displays the current TCP/UDP Filtering parameters.</p> <p>Command mode: All</p> | | | | | | | | | | | | | | | | | | | | | | | | | | | | |

VMAP Configuration

A VLAN Map is an Access Control List (ACL) that can be assigned to a VLAN or a VM group instead of a port. In a virtualized environment where Virtual Machines move between physical servers, VLAN Maps allow you to create traffic filtering and metering policies associated with a VM's VLAN.

For more information about VLAN Map configuration commands, see [“Access Control List Configuration” on page 303](#).

For more information about assigning VLAN Maps to a VLAN, see [“VLAN Configuration” on page 361](#).

For more information about assigning VLAN Maps to a VM group, see [“VM Group Configuration” on page 478](#).

[Table 201](#) lists the general VMAP configuration commands.

Table 201. VMAP Configuration Commands

| Command Syntax and Usage |
|---|
| <pre>[no] access-control vmap <1-128> egress-port <port alias or number></pre> <p>Configures the VMAP to function on egress packets.</p> <p>Command mode: Global configuration</p> |
| <pre>access-control vmap <1-128> action {permit deny set-priority <0-7>}</pre> <p>Configures a filter action for packets that match the VMAP definitions. You can choose to permit (pass) or deny (drop) packets, or set the 802.1p priority level (0-7).</p> <p>Command mode: Global configuration</p> |
| <pre>[no] access-control vmap <1-640> ethernet source-mac-address <MAC address> <MAC mask></pre> <p>Enables or disables filtering of VMAP statistics collection based on source MAC.</p> <p>Command mode: Global configuration</p> |
| <pre>[no] access-control vmap <1-640> ethernet destination-mac-address <MAC address> <MAC mask></pre> <p>Enables or disables filtering of VMAP statistics collection based on destination MAC.</p> <p>Command mode: Global configuration</p> |

Table 201. VMAP Configuration Commands (continued)

| Command Syntax and Usage |
|--|
| <pre>[no] access-control vmap <1-640> ethernet ether-type {<0x600-0xFFF> arp rarp ip ipv6 mpls any}</pre> <p>Enables or disables filtering of VMAP statistics collection based on the encapsulated protocol:</p> <ul style="list-style-type: none"> – <0x600-0xFFF> filters Ethernet frames with the specified EtherType – arp filters Address Resolution Protocol frames – rarp filters Reverse Address Resolution Protocol frames – ip filters Internet Protocol version 4 frames – ipv6 filters Internet Protocol version 6 frames – mpls filters Multiprotocol Label Switching frames – all filters all frames <p>Command mode: Global configuration</p> |
| <pre>[no] access-control vmap <1-640> ethernet priority <0-7></pre> <p>Enables or disables filtering of VMAP statistics collection based on the IEEE 802.1Q priority code point value.</p> <p>Command mode: Global configuration</p> |
| <pre>[no] access-control vmap <1-640> ethernet vlan <1-4094></pre> <p>Enables or disables filtering of VMAP statistics collection based on VLAN ID.</p> <p>Command mode: Global configuration</p> |
| <pre>[no] access-control vmap <1-640> ipv4 source-ip-address <IPv4 address> <IPv4 mask></pre> <p>Enables or disables filtering of VMAP statistics collection based on source IP address.</p> <p>Command mode: Global configuration</p> |
| <pre>[no] access-control vmap <1-640> ipv4 destination-ip-address <IPv4 address> <IPv4 mask></pre> <p>Enables or disables filtering of VMAP statistics collection based on destination IP address.</p> <p>Command mode: Global configuration</p> |
| <pre>[no] access-control vmap <1-640> ipv4 protocol <0-255></pre> <p>Enables or disables filtering of VMAP statistics collection based on protocol.</p> <p>Command mode: Global configuration</p> |
| <pre>[no] access-control vmap <1-640> ipv4 type-of-service <0-255></pre> <p>Enables or disables filtering of VMAP statistics collection based on type of service.</p> <p>Command mode: Global configuration</p> |
| <pre>access-control vmap <1-640> meter enable</pre> <p>Enables ACL port metering.</p> <p>Command mode: All except User EXEC</p> |

Table 201. VMAP Configuration Commands (continued)

| Command Syntax and Usage |
|---|
| <p>access-control vmap <1-640> meter action drop pass</p> <p>Sets ACL port metering to drop or pass out-of-profile traffic.</p> <p>Command mode: Global configuration</p> |
| <p>access-control vmap <1-640> meter committed-rate <64-10000000></p> <p>Sets the ACL port metering control rate in kilobits per second.</p> <p>Command mode: Global configuration</p> |
| <p>access-control vmap <1-640> meter maximum-burst-size <32-4096></p> <p>Sets the ACL port metering maximum burst size in kilobytes. The following eight values are allowed:</p> <ul style="list-style-type: none"> – 32 – 64 – 128 – 256 – 512 – 1024 – 2048 – 4096 <p>Command mode: Global configuration</p> |
| <p>no access-control vmap <1-640> meter enable</p> <p>Disables ACL port metering.</p> <p>Command mode: Global configuration</p> |
| <p>access-control vmap <1-640> mirror port <port></p> <p>Sets the specified port as the mirror target.</p> <p>Command mode: Global configuration</p> |
| <p>no access-control vmap <1-640> mirror</p> <p>Turns off ACL mirroring.</p> <p>Command mode: Global configuration</p> |
| <p>access-control vmap <1-640> packet-format ethernet ethernet-type2 llc snap</p> <p>Sets to filter the specified ethernet packet format type.</p> <p>Command mode: Global configuration</p> |
| <p>access-control vmap <1-640> packet-format ip ipv4 ipv6</p> <p>Sets to filter the specified IP packet format type.</p> <p>Command mode: Global configuration</p> |

Table 201. VMAP Configuration Commands (continued)

| Command Syntax and Usage |
|---|
| <pre>access-control vmap <I-640> packet-format tagging any none tagged</pre> <p>Sets filtering based on packet tagging. The options are:</p> <ul style="list-style-type: none"> – any: Filter tagged & untagged packets – none: Filter only untagged packets – tagged: Filter only tagged packets <p>Command mode: Global configuration</p> |
| <pre>no access-control vmap <I-640> packet-format ethernet ip tagging</pre> <p>Disables filtering based on the specified packet format.</p> <p>Command mode: Global configuration</p> |
| <pre>access-control vmap <I-640> re-mark dot1p <0-7></pre> <p>Sets the ACL re-mark configuration user update priority.</p> <p>Command mode: Global configuration</p> |
| <pre>no access-control vmap <I-640> re-mark dot1p</pre> <p>Disables the use of dot1p for in-profile traffic ACL re-mark configuration.</p> <p>Command mode: Global configuration</p> |
| <pre>access-control vmap <I-640> re-mark in-profile out-profile dscp <0-63></pre> <p>Sets the ACL re-mark configuration user update priority.</p> <p>Command mode: Global configuration</p> |
| <pre>no access-control vmap <I-640> re-mark in-profile out-profile</pre> <p>Removes all re-mark in-profile or out-profile settings.</p> <p>Command mode: Global configuration</p> |
| <pre>[no] access-control vmap <I-640> re-mark use-tos-precedence</pre> <p>Enables or disables the use of the TOS precedence for in-profile traffic.</p> <p>Command mode: Global configuration</p> |
| <pre>[no] access-control vmap <I-128> statistics</pre> <p>Enables or disables the statistics collection for the VMAP.</p> <p>Command mode: Global configuration</p> |
| <pre>access-control vmap <I-640> tcp-udp source-port destination-port <I-65535> <port mask (0x0001 - 0xFFFF)></pre> <p>Sets the TCP/UDP filtering source port or destination port and port mask for this ACL.</p> <p>Command mode: Global configuration</p> |
| <pre>access-control vmap <I-640> tcp-udp flags [<flags mask (0x0-0x3F)>]</pre> <p>Sets the TCP flags for this ACL.</p> <p>Command mode: Global configuration</p> |

Table 201. VMAP Configuration Commands (continued)

| Command Syntax and Usage |
|--|
| <pre>no access-control vmap <1-640> tcp-udp</pre> <p>Removes TCP/UDP filtering for this ACL. Command mode: Global configuration</p> |
| <pre>default access-control vmap <1-128></pre> <p>Resets the VMAP parameters to their default values. Command mode: Global configuration</p> |
| <pre>show access-control vmap <1-128></pre> <p>Displays the current VMAP parameters. Command mode: All</p> |

ACL Group Configuration

These commands allow you to compile one or more ACLs into an ACL group. Once you create an ACL group, you can assign the ACL group to one or more ports.

Table 202. ACL Group Configuration Commands

| Command Syntax and Usage |
|--|
| <pre>access-control group <1-640> list <1-640></pre> <p>Adds the selected ACL to the ACL group. Command mode: Global configuration</p> |
| <pre>no access-control group <1-640> list <1-640></pre> <p>Removes the selected ACL from the ACL group. Command mode: Global configuration</p> |
| <pre>show access-control group <1-640></pre> <p>Displays the current ACL group parameters. Command mode: All</p> |

ACL Metering Configuration

These commands define the Access Control profile for the selected ACL or ACL Group.

Table 203. ACL Metering Configuration Commands

| Command Syntax and Usage |
|---|
| <pre>access-control list <I-640> meter committed-rate <64-10000000></pre> <p>Configures the committed rate, in Kilobits per second. The committed rate must be a multiple of 64.</p> <p>Command mode: Global configuration</p> |
| <pre>access-control list <I-640> meter maximum-burst-size <32-4096></pre> <p>Configures the maximum burst size, in Kilobits. Enter one of the following values for mbsize: 32, 64, 128, 256, 512, 1024, 2048, 4096</p> <p>Command mode: Global configuration</p> |
| <pre>[no] access-control list <I-640> meter enable</pre> <p>Enables or disables ACL Metering.</p> <p>Command mode: Global configuration</p> |
| <pre>access-control list <I-640> meter action {drop pass}</pre> <p>Configures the ACL meter to either drop or pass out-of-profile traffic.</p> <p>Command mode: Global configuration</p> |
| <pre>default access-control list <I-640> meter</pre> <p>Sets the ACL meter configuration to its default values.</p> <p>Command mode: Global configuration</p> |
| <pre>[no] access-control list <I-640> meter log</pre> <p>Configures the ACL meter to log out-of-profile notifications.</p> <p>Command mode: Global configuration</p> |
| <pre>no access-control list <I-640> meter</pre> <p>Deletes the selected ACL meter.</p> <p>Command mode: Global configuration</p> |
| <pre>show access-control list <I-640> meter</pre> <p>Displays current ACL Metering parameters.</p> <p>Command mode: All</p> |

ACL Re-Mark Configuration

You can choose to re-mark IP header data for the selected ACL or ACL group. You can configure different re-mark values, based on whether packets fall within the ACL metering profile, or out of the ACL metering profile.

Table 204. ACL Re-Marking Configuration Commands

| Command Syntax and Usage |
|--|
| <pre>access-control list <1-640> re-mark dot1p <0-7></pre> <p>Defines 802.1p value. The value is the priority bits information in the packet structure.</p> <p>Command mode: Global configuration</p> |
| <pre>no access-control list <1-640> re-mark dot1p</pre> <p>Disables use of 802.1p value for re-marked packets.</p> <p>Command mode: Global configuration</p> |
| <pre>[no] access-control list <1-640> re-mark use-tos-precedence</pre> <p>Enable or disable mapping of TOS (Type of Service) priority to 802.1p priority for In-Profile packets. When enabled, the TOS value is used to set the 802.1p value.</p> <p>Command mode: Global configuration</p> |
| <pre>default access-control list <1-640> re-mark</pre> <p>Sets the ACL Re-mark configuration to its default values.</p> <p>Command mode: Global configuration</p> |
| <pre>show access-control list <1-640> re-mark</pre> <p>Displays current Re-mark parameters.</p> <p>Command mode: All</p> |

Re-Marking In-Profile Configuration

Table 205. ACL Re-Mark In-Profile Commands

| Command Syntax and Usage |
|--|
| <pre>access-control list <1-640> re-mark in-profile dscp <0-63></pre> <p>Sets the DiffServ Code Point (DSCP) of in-profile packets to the selected value.</p> <p>Command mode: Global configuration</p> |
| <pre>no access-control list <1-640> re-mark in-profile dscp</pre> <p>Disables use of DSCP value for in-profile traffic.</p> <p>Command mode: Global configuration</p> |
| <pre>show access-control list <1-640> re-mark</pre> <p>Displays current re-mark parameters.</p> <p>Command mode: All</p> |

Re-Marking Out-of-Profile Configuration

Table 206. ACL Re-Mark Out-of-Profile Commands

| Command Syntax and Usage |
|---|
| <pre>access-control list <1-640> re-mark out-profile dscp <0-63></pre> <p>Sets the DiffServ Code Point (DSCP) of out-of-profile packets to the selected value. The switch sets the DSCP value on Out-of-Profile packets.</p> <p>Command mode: Global configuration</p> |
| <pre>no access-control list <1-640> re-mark out-profile dscp</pre> <p>Disables use of DSCP value for out-of-profile traffic.</p> <p>Command mode: Global configuration</p> |
| <pre>show access-control list <1-640> re-mark</pre> <p>Displays current re-mark parameters.</p> <p>Command mode: All</p> |

IPv6 Re-Marking Configuration

You can choose to re-mark IP header data for the selected ACL. You can configure different re-mark values, based on whether packets fall within or outside the ACL metering profile.

Table 207. IPv6 General Re-Mark Options

| Command Syntax and Usage |
|--|
| <pre>[no] access-control list6 <1-128> re-mark dot1p <0-7></pre> <p>Re-marks the 802.1p value. The value is the priority bits information in the packet structure.</p> <p>Command mode: Global configuration</p> |
| <pre>[no] no access-control list6 <1-128> re-mark use-tos-precedence</pre> <p>Enables or disables mapping of TOS (Type of Service) priority to 802.1p priority for in-profile packets. When enabled, the TOS value is used to set the 802.1p value.</p> <p>Command mode: Global configuration</p> |
| <pre>default access-control list6 <1-128> re-mark</pre> <p>Sets the ACL re-mark parameters to their default values.</p> <p>Command mode: Global configuration</p> |
| <pre>show access-control list6 <1-128> re-mark</pre> <p>Displays current re-mark parameters.</p> <p>Command mode: All</p> |

IPv6 Re-Marking In-Profile Configuration

Table 208. IPv6 Re-Mark In-Profile Options

| Command Syntax and Usage |
|--|
| <pre>[no] access-control list6 <1-128> re-mark in-profile dscp <0-63></pre> <p>Re-marks the DSCP value for in-profile traffic. Command mode: Global configuration</p> |
| <pre>default access-control list6 <1-128> re-mark</pre> <p>Sets the ACL re-mark parameters to their default values. Command mode: Global configuration</p> |
| <pre>show access-control list6 <1-128> re-mark</pre> <p>Displays current re-mark parameters. Command mode: All</p> |

Port Mirroring

Port mirroring is disabled by default. For more information about port mirroring on the EN4093 and EN4093R, see “Appendix A: Troubleshooting” in the *Networking OS 7.7 Application Guide*.

Note: Traffic on VLAN 4095 is not mirrored to the external ports.

Port Mirroring commands are used to configure, enable, and disable the monitor port. When enabled, network packets being sent and/or received on a target port are duplicated and sent to a monitor port. By attaching a network analyzer to the monitor port, you can collect detailed information about your network performance and usage.

Table 209. Port Mirroring Configuration Commands

| Command Syntax and Usage |
|---|
| <pre>[no] port-mirroring enable</pre> <p>Enables or disables port mirroring.</p> <p>Command mode: Global configuration</p> |
| <pre>show port-mirroring</pre> <p>Displays current settings of the mirrored and monitoring ports.</p> <p>Command mode: All</p> |

Port Mirroring Configuration

Table 210. Port-Based Port Mirroring Configuration Commands

| Command Syntax and Usage |
|--|
| <pre>port-mirroring monitor-port <port alias or number> mirroring-port <port alias or number> {in out both}</pre> <p>Adds the port to be mirrored. This command also allows you to enter the direction of the traffic. It is necessary to specify the direction because:</p> <p>If the source port of the frame matches the mirrored port and the mirrored direction is ingress or both (ingress and egress), the frame is sent to the monitoring port.</p> <p>If the destination port of the frame matches the mirrored port and the mirrored direction is egress or both, the frame is sent to the monitoring port.</p> <p>Command mode: Global configuration</p> |
| <pre>no port-mirroring monitor-port <port alias or number> mirroring-port <port alias or number></pre> <p>Removes the mirrored port.</p> <p>Command mode: Global configuration</p> |
| <pre>show port-mirroring</pre> <p>Displays the current settings of the monitoring port.</p> <p>Command mode: All</p> |

Layer 2 Configuration

The following table describes basic Layer 2 Configuration commands. The following sections provide more detailed information and commands.

Table 211. Layer 2 Configuration Commands

| Command Syntax and Usage |
|---|
| <pre>vlan <VLAN number></pre> <p>Enter VLAN configuration mode. To view command options, see page 361.</p> <p>Command mode: Global configuration</p> |
| <pre>spanning-tree mode disable</pre> <p>When enabled, globally turns Spanning Tree <code>off</code> (selects Spanning-Tree mode “disable”). All ports are placed into forwarding state. Any BPDU’s received are flooded. BPDU Guard is not affected by this command.</p> <p>To enable Spanning-Tree, select another Spanning-Tree mode.</p> <p>Command mode: Global configuration</p> |
| <pre>[no] spanning-tree stg-auto</pre> <p>Enables or disables VLAN Automatic STG Assignment (VASA). When enabled, each time a new VLAN is configured, the switch will automatically assign the new VLAN its own STG. Conversely, when a VLAN is deleted, if its STG is not associated with any other VLAN, the STG is returned to the available pool.</p> <p>Note: VASA applies only to PVRST mode.</p> <p>Command mode: Global configuration</p> |
| <pre>[no] spanning-tree pvst-compatibility</pre> <p>Enables or disables VLAN tagging of Spanning Tree BPDUs. The default setting is <code>enabled</code>.</p> <p>Command mode: Global configuration</p> |
| <pre>[no] spanning-tree loopguard</pre> <p>Enables or disables Spanning Tree Loop Guard.</p> <p>Command mode: Global configuration</p> |
| <pre>show layer2</pre> <p>Displays current Layer 2 parameters.</p> <p>Command mode: All</p> |

802.1X Configuration

These commands allow you to configure the EN4093 and EN4093R as an IEEE 802.1X Authenticator, to provide port-based network access control.

Table 212. 802.1X Configuration Commands

| Command Syntax and Usage |
|--|
| <pre>dot1x enable</pre> <p>Globally enables 802.1X.</p> <p>Command mode: Global configuration</p> |
| <pre>no dot1x enable</pre> <p>Globally disables 802.1X.</p> <p>Command mode: Global configuration</p> |
| <pre>show dot1x</pre> <p>Displays current 802.1X parameters.</p> <p>Command mode: All</p> |

802.1X Global Configuration

The global 802.1X commands allow you to configure parameters that affect all ports in the EN4093 and EN4093R.

Table 213. 802.1X Global Configuration Commands

| Command Syntax and Usage |
|---|
| <pre>dot1x mode [force-unauthorized auto force-authorized]</pre> <p>Sets the type of access control for all ports:</p> <ul style="list-style-type: none">– force-unauthorized - the port is unauthorized unconditionally.– auto - the port is unauthorized until it is successfully authorized by the RADIUS server.– force-authorized - the port is authorized unconditionally, allowing all traffic. <p>The default value is force-authorized.</p> <p>Command mode: Global configuration</p> |
| <pre>dot1x quiet-time <0-65535></pre> <p>Sets the time, in seconds, the authenticator waits before transmitting an EAP-Request/ Identity frame to the supplicant (client) after an authentication failure in the previous round of authentication. The default value is 60 seconds.</p> <p>Command mode: Global configuration</p> |
| <pre>dot1x transmit-interval <1-65535></pre> <p>Sets the time, in seconds, the authenticator waits for an EAP-Response/Identity frame from the supplicant (client) before retransmitting an EAP-Request/Identity frame. The default value is 30 seconds.</p> <p>Command mode: Global configuration</p> |

Table 213. 802.1X Global Configuration Commands (continued)

| Command Syntax and Usage | |
|---|---|
| dot1x supplicant-timeout <1-65535> | <p>Sets the time, in seconds, the authenticator waits for an EAP-Response packet from the supplicant (client) before retransmitting the EAP-Request packet from the authentication server. The default value is 30 seconds.</p> <p>Command mode: Global configuration</p> |
| dot1x server-timeout <1-65535> | <p>Sets the time, in seconds, the authenticator waits for a response from the RADIUS server before declaring an authentication timeout. The default value is 30 seconds.</p> <p>The time interval between transmissions of the RADIUS Access-Request packet containing the supplicant's (client's) EAP-Response packet is determined by the current setting of radius-server timeout <timeout-value> (default is 3 seconds).</p> <p>Command mode: Global configuration</p> |
| dot1x max-request <1-10> | <p>Sets the maximum number of times the authenticator retransmits an EAP-Request packet to the supplicant (client). The default value is 2.</p> <p>Command mode: Global configuration</p> |
| dot1x re-authentication-interval <1-604800> | <p>Sets the time, in seconds, the authenticator waits before re-authenticating a supplicant (client) when periodic re-authentication is enabled. The default value is 3600 seconds.</p> <p>Command mode: Global configuration</p> |
| dot1x re-authenticate | <p>Sets the re-authentication status to on. The default value is off.</p> <p>Command mode: Global configuration</p> |
| [no] dot1x re-authenticate | <p>Sets the re-authentication status to off. The default value is off.</p> <p>Command mode: Global configuration</p> |
| [no] dot1x vlan-assign | <p>Sets the dynamic VLAN assignment status to on or off. The default value is off.</p> <p>Command mode: Global configuration</p> |
| default dot1x | <p>Resets the global 802.1X parameters to their default values.</p> <p>Command mode: Global configuration</p> |
| show dot1x | <p>Displays current global 802.1X parameters.</p> <p>Command mode: All</p> |

802.1X Guest VLAN Configuration

The 802.1X Guest VLAN commands allow you to configure a Guest VLAN for unauthenticated ports. The Guest VLAN provides limited access to switch functions.

Table 214. 802.1X Guest VLAN Configuration Commands

| Command Syntax and Usage |
|--|
| <pre>[no] dot1x guest-vlan vlan <VLAN number></pre> <p>Configures the Guest VLAN number. Command mode: Global configuration</p> |
| <pre>dot1x guest-vlan enable</pre> <p>Enables the 802.1X Guest VLAN. Command mode: Global configuration</p> |
| <pre>no dot1x guest-vlan enable</pre> <p>Disables the 802.1X Guest VLAN. Command mode: Global configuration</p> |
| <pre>show dot1x</pre> <p>Displays current 802.1X parameters. Command mode: All</p> |

802.1X Port Configuration

The 802.1X port commands allows you to configure parameters that affect the selected port in the EN4093 and EN4093R. These settings override the global 802.1X parameters.

Table 215. 802.1X Port Commands

| Command Syntax and Usage |
|--|
| <pre>dot1x mode force-unauthorized auto force-authorized</pre> <p>Sets the type of access control for the port:</p> <ul style="list-style-type: none"> – force-unauthorized - the port is unauthorized unconditionally. – auto - the port is unauthorized until it is successfully authorized by the RADIUS server. – force-authorized - the port is authorized unconditionally, allowing all traffic. <p>The default value is force-authorized.</p> <p>Command mode: Interface port</p> |
| <pre>dot1x quiet-time <0-65535></pre> <p>Sets the time, in seconds, the authenticator waits before transmitting an EAP-Request/ Identity frame to the supplicant (client) after an authentication failure in the previous round of authentication. The default value is 60 seconds.</p> <p>Command mode: Interface port</p> |
| <pre>dot1x transmit-interval <1-65535></pre> <p>Sets the time, in seconds, the authenticator waits for an EAP-Response/Identity frame from the supplicant (client) before retransmitting an EAP-Request/Identity frame. The default value is 30 seconds.</p> <p>Command mode: Interface port</p> |
| <pre>dot1x supplicant-timeout <1-65535></pre> <p>Sets the time, in seconds, the authenticator waits for an EAP-Response packet from the supplicant (client) before retransmitting the EAP-Request packet from the authentication server. The default value is 30 seconds.</p> <p>Command mode: Interface port</p> |
| <pre>dot1x server-timeout <1-65535></pre> <p>Sets the time, in seconds, the authenticator waits for a response from the RADIUS server before declaring an authentication timeout. The default value is 30 seconds.</p> <p>The time interval between transmissions of the RADIUS Access-Request packet containing the supplicant's (client's) EAP-Response packet is determined by the current setting of the radius-server timeout command.</p> <p>Command mode: Interface port</p> |

Table 215. 802.1X Port Commands (continued)

| Command Syntax and Usage | |
|--|--|
| dot1x max-request <1-10> | <p>Sets the maximum number of times the authenticator retransmits an EAP-Request packet to the supplicant (client). The default value is 2.</p> <p>Command mode: Interface port</p> |
| dot1x re-authentication-interval <1-604800> | <p>Sets the time, in seconds, the authenticator waits before re-authenticating a supplicant (client) when periodic re-authentication is enabled. The default value is 3600 seconds.</p> <p>Command mode: Interface port</p> |
| dot1x re-authenticate | <p>Sets the re-authentication status to <i>on</i>. The default value is <i>off</i>.</p> <p>Command mode: Interface port</p> |
| [no] dot1x re-authenticate | <p>Sets the re-authentication status <i>off</i>. The default value is <i>off</i>.</p> <p>Command mode: Interface port</p> |
| [no] dot1x vlan-assign | <p>Sets the dynamic VLAN assignment status to <i>on</i> or <i>off</i>. The default value is <i>off</i>.</p> <p>Command mode: Interface port</p> |
| default dot1x | <p>Resets the 802.1X port parameters to their default values.</p> <p>Command mode: Interface port</p> |
| dot1x apply-global | <p>Applies current global 802.1X configuration parameters to the port.</p> <p>Command mode: Interface port</p> |
| show interface port <port alias or number> dot1x | <p>Displays current 802.1X port parameters.</p> <p>Command mode: All</p> |

Spanning Tree Configuration

Networking OS supports the IEEE 802.1w Rapid Spanning Tree Protocol (RSTP), the IEEE 802.1s Multiple Spanning Tree Protocol (MSTP), and Per VLAN Rapid Spanning Tree Protocol (PVRST+). STP is used to prevent loops in the network topology. Up to 128 Spanning Tree Groups can be configured on the switch (STG 128 is reserved for management).

Note: When VRRP is used for active/active redundancy, STG must be enabled.

Table 216. Spanning Tree Configuration Options

| Command Syntax and Usage | |
|--|---|
| <pre>spanning-tree mode [disable mst pvrst rstp]</pre> | <p>Selects and enables Multiple Spanning Tree mode (<code>mst</code>), Per VLAN Rapid Spanning Tree mode (<code>pvrst</code>), or Rapid Spanning Tree mode (<code>rstp</code>).</p> <p>The default mode is PVRST+.</p> <p>When you select <code>spanning-tree mode disable</code>, the switch globally turns Spanning Tree <code>off</code>. All ports are placed into forwarding state. Any BPDU's received are flooded. BPDU Guard is not affected by this command.</p> <p>Command mode: Global configuration</p> |
| <pre>[no] spanning-tree stg-auto</pre> | <p>Enables or disables VLAN Automatic STG Assignment (VASA). When enabled, each time a new VLAN is configured, the switch will automatically assign the new VLAN its own STG. Conversely, when a VLAN is deleted, if its STG is not associated with any other VLAN, the STG is returned to the available pool.</p> <p>Note: When using VASA, a maximum number of automatically assigned STGs is supported.</p> <p>Note: VASA applies only to PVRST mode.</p> <p>Command mode: Global configuration</p> |
| <pre>[no] spanning-tree pvst-compatibility</pre> | <p>Enables or disables VLAN tagging of Spanning Tree BPDUs. The default setting is <code>enabled</code>.</p> <p>Command mode: Global configuration</p> |
| <pre>[no] spanning-tree edge</pre> | <p>Enables or disables this port as portfast or edge port. An edge port is not connected to a bridge, and can begin forwarding traffic as soon as the link is up. Configure server ports as edge ports (<code>enabled</code>).</p> <p>Note: After you configure the port as an edge port, you must disable the port and then re-enable the port for the change to take effect.</p> <p>Command mode: Interface port/Interface portchannel</p> |

Table 216. Spanning Tree Configuration Options (continued)

| Command Syntax and Usage | |
|---|---|
| <pre>[no] spanning-tree link-type {p2p shared auto}</pre> | <p>Defines the type of link connected to the port, as follows:</p> <ul style="list-style-type: none"> – auto: Configures the port to detect the link type, and automatically match its settings. – p2p: Configures the port for Point-To-Point protocol. – shared: Configures the port to connect to a shared medium (usually a hub). <p>The default link type is auto.</p> <p>Command mode: Interface port/Interface portchannel</p> |
| <pre>spanning-tree guard loop</pre> | <p>Enables STP loop guard. STP loop guard prevents the port from forwarding traffic if no BPDUs are received. The port is placed into a loop-inconsistent blocking state until a BPDU is received.</p> <p>Command mode: Interface port/Interface portchannel</p> |
| <pre>spanning-tree guard root</pre> | <p>Enables STP root guard. STP root guard enforces the position of the root bridge. If the bridge receives a superior BPDU, the port is placed into a root-inconsistent state (listening).</p> <p>Command mode: Interface port/Interface portchannel</p> |
| <pre>spanning-tree guard none</pre> | <p>Disables STP loop guard and root guard.</p> <p>Command mode: Interface port/Interface portchannel</p> |
| <pre>no spanning-tree guard</pre> | <p>Sets the Spanning Tree guard parameters to their default values.</p> <p>Command mode: Interface port/Interface portchannel</p> |
| <pre>show spanning-tree</pre> | <p>Displays Spanning Tree information, including the status (on or off), Spanning Tree mode (RSTP, PVRST, or MSTP), and VLAN membership.</p> <p>In addition to seeing if STG is enabled or disabled, you can view the following STG bridge information:</p> <ul style="list-style-type: none"> – Priority – Hello interval – Maximum age value – Forwarding delay – Aging time <p>You can also see the following port-specific STG information:</p> <ul style="list-style-type: none"> – Port alias and priority – Cost – State <p>Command mode: All</p> |

MSTP/RSTP/PVRST Configuration

IBM N/OS supports STP/PVST+, the IEEE 802.1w Rapid Spanning Tree Protocol (RSTP), IEEE 802.1s Multiple Spanning Tree Protocol (MSTP), and Per VLAN Rapid Spanning Tree Protocol (PVRST+). MSTP allows you to map many VLANs to a small number of Spanning Tree Groups, each with its own topology.

Up to 32 Spanning Tree Groups can be configured in MSTP mode. MSTP is turned off by default and the default STP mode is PVRST+.

Note: When Multiple Spanning Tree is turned on, VLAN 4095 is moved from Spanning Tree Group 128 to the Common Internal Spanning Tree (CIST). When Multiple Spanning Tree is turned off, VLAN 4095 is moved back to Spanning Tree Group 128.

Table 217. Multiple Spanning Tree Configuration Options

| Command Syntax and Usage |
|--|
| <pre>default spanning-tree mstp cist</pre> <p>Resets all CIST parameters to their default values.</p> <p>Command mode: Global configuration</p> |
| <pre>spanning-tree mstp name <1-32 characters></pre> <p>Configures a name for the MSTP region. All devices within an MSTP region must have the same region name.</p> <p>Command mode: Global configuration</p> |
| <pre>spanning-tree mstp version <0-65535></pre> <p>Configures a version number for the MSTP region. The version is used as a numerical identifier for the region. All devices within an MSTP region must have the same version number.</p> <p>Command mode: Global configuration</p> |
| <pre>spanning-tree mstp maximum-hop <4-60></pre> <p>Configures the maximum number of bridge hops a packet may traverse before it is dropped. The default value is 20.</p> <p>Command mode: Global configuration</p> |
| <pre>spanning-tree mode [disable mst pvrst rstp]</pre> <p>Selects and enables Multiple Spanning Tree mode (<code>mst</code>), Per VLAN Rapid Spanning Tree mode (<code>pvrst</code>), or Rapid Spanning Tree mode (<code>rstp</code>).</p> <p>The default mode is STP/PVRST+.</p> <p>When you select <code>spanning-tree disable</code>, the switch globally turns Spanning Tree <code>off</code>. All ports are placed into forwarding state. Any BPDU's received are flooded. BPDU Guard is not affected by this command.</p> <p>Command mode: Global configuration</p> |
| <pre>show spanning-tree mstp mrst</pre> <p>Displays the current RSTP/MSTP/PVRST+ configuration.</p> <p>Command mode: All</p> |

Common Internal Spanning Tree Configuration

[Table 218](#) describes the commands used to configure Common Internal Spanning Tree (CIST) parameters. The CIST provides compatibility with different MSTP regions and with devices running different Spanning Tree instances. It is equivalent to Spanning Tree Group 0.

Table 218. CIST Configuration Commands

| Command Syntax and Usage |
|--|
| <pre>default spanning-tree mstp cist</pre> <p>Resets all CIST parameters to their default values.</p> <p>Command mode: Global configuration</p> |
| <pre>show spanning-tree mstp cist</pre> <p>Displays the current CIST configuration.</p> <p>Command mode: All</p> |

CIST Bridge Configuration

CIST bridge parameters are used only when the switch is in MSTP mode. CIST parameters do not affect operation of STP/PVST+, RSTP, or PVRST+.

Table 219. CIST Bridge Configuration Commands

| Command Syntax and Usage |
|---|
| <pre>spanning-tree mstp cist-add-vlan <VLAN no.></pre> <p>Add the specified VLANs to CIST.</p> <p>Command mode: Global configuration</p> |
| <pre>spanning-tree mstp cist-bridge priority <0-65535></pre> <p>Configures the CIST bridge priority. The bridge priority parameter controls which bridge on the network is the MSTP root bridge. To make this switch the root bridge, configure the bridge priority lower than all other switches and bridges on your network. The lower the value, the higher the bridge priority.</p> <p>The range is 0 to 65535, in steps of 4096 (0, 4096, 8192...), and the default value is 61440.</p> <p>Command mode: Global configuration</p> |
| <pre>spanning-tree mstp cist-bridge maximum-age <6-40></pre> <p>Configures the CIST bridge maximum age. The maximum age parameter specifies the maximum time the bridge waits without receiving a configuration bridge protocol data unit before it reconfigures the MSTP network. The range is 6 to 40 seconds, and the default is 20 seconds.</p> <p>Command mode: Global configuration</p> |

Table 219. CIST Bridge Configuration Commands

| Command Syntax and Usage |
|---|
| <pre>spanning-tree mstp cist-bridge forward-delay <4-30></pre> <p>Configures the CIST bridge forward delay parameter. The forward delay parameter specifies the amount of time that a bridge port has to wait before it changes from the listening state to the learning state and from the learning state to the forwarding state. The range is 4 to 30 seconds, and the default is 15 seconds.</p> <p>Command mode: Global configuration</p> |
| <pre>show spanning-tree mstp cist</pre> <p>Displays the current CIST bridge configuration.</p> <p>Command mode: All</p> |

CIST Port Configuration

CIST port parameters are used to modify CIST operation on an individual port basis. CIST parameters do not affect operation of STP/PVST+. For each port, RSTP/MSTP is turned on by default.

Table 220. CIST Port Configuration Options

| Command Syntax and Usage |
|--|
| <pre>spanning-tree mstp cist interface-priority <0-240></pre> <p>Configures the CIST port priority. The port priority helps determine which bridge port becomes the designated port. In a network topology that has multiple bridge ports connected to a single segment, the port with the lowest port priority becomes the designated port for the segment.</p> <p>The range is 0 to 240, in steps of 16 (0, 16, 32...), and the default is 128.</p> <p>Command mode: Interface port</p> |
| <pre>spanning-tree mstp cist path-cost <0-200000000></pre> <p>Configures the CIST port path cost. The port path cost is used to help determine the designated port for a segment. Port path cost is based on the port speed, and is calculated as follows:</p> <ul style="list-style-type: none"> – 1Gbps = 20000 – 10Gbps = 2000 <p>The default value of 0 (zero) indicates that the default path cost will be computed for an auto negotiated link speed.</p> <p>Command mode: Interface port</p> |
| <pre>spanning-tree mstp cist hello <1-10></pre> <p>Configures the CIST port Hello time. The Hello time specifies how often the root bridge transmits a configuration bridge protocol data unit (BPDU). Any bridge that is not the root bridge uses the root bridge Hello value. The range is 1 to 10 seconds, and the default is 2 seconds.</p> <p>Command mode: Interface port</p> |

Table 220. CIST Port Configuration Options (continued)

| Command Syntax and Usage |
|---|
| <pre>[no] spanning-tree pvst-protection</pre> <p>Configures PVST Protection on the selected port. If the port receives any PVST+/PVRST+ BPDUs, it error disabled. PVST Protection works only in MSTP mode. The default setting is disabled.</p> <p>Note: Not available in stacking.</p> <p>Command mode: Interface port</p> |
| <pre>no spanning-tree mstp cist enable</pre> <p>Disables MRST on the port.</p> <p>Command mode: Interface port</p> |
| <pre>show interface port <port alias or number> spanning-tree mstp cist</pre> <p>Displays the current CIST port configuration.</p> <p>Command mode: All</p> |

RSTP/PVRST Configuration

Table 221 describes the commands used to configure the Rapid Spanning Tree (RSTP) and Per VLAN Rapid Spanning Tree Protocol (PVRST+) protocols.

Table 221. RSTP/PVRST Configuration Options

| Command Syntax and Usage |
|---|
| <pre>spanning-tree stp <STG number> vlan <VLAN number></pre> <p>Associates a VLAN with a Spanning Tree Group and requires a VLAN ID as a parameter. If the VLAN does not exist, it will be created automatically, but it will not be enabled by default.</p> <p>Command mode: Global configuration</p> |
| <pre>no spanning-tree stp <STG number> vlan <VLAN number></pre> <p>Breaks the association between a VLAN and a Spanning Tree Group and requires a VLAN ID as a parameter.</p> <p>Command mode: Global configuration</p> |
| <pre>no spanning-tree stp <STG number> vlan all</pre> <p>Removes all VLANs from a Spanning Tree Group.</p> <p>Command mode: Global configuration</p> |
| <pre>spanning-tree stp <STG number> enable</pre> <p>Globally enables Spanning Tree Protocol. STG is turned on by default.</p> <p>Command mode: Global configuration</p> |
| <pre>no spanning-tree stp <STG number> enable</pre> <p>Globally disables Spanning Tree Protocol.</p> <p>Command mode: Global configuration</p> |

Table 221. RSTP/PVRST Configuration Options (continued)

| Command Syntax and Usage |
|---|
| <pre>default spanning-tree <STG number></pre> <p>Restores a Spanning Tree instance to its default configuration.</p> <p>Command mode: Global configuration</p> |
| <pre>show spanning-tree stp <STG number> [information]</pre> <p>Displays current Spanning Tree Protocol parameters for the specified Spanning Tree Group. See page 50 for details about the <code>information</code> parameter.</p> <p>Command mode: All</p> |

Bridge RSTP/PVRST Configuration

Spanning Tree bridge parameters affect the global STG operation of the switch. STG bridge parameters include:

- Bridge priority
- Bridge hello time
- Bridge maximum age
- Forwarding delay

Table 222. Bridge Spanning Tree Configuration Options

| Command Syntax and Usage |
|---|
| <pre>spanning-tree stp <STG number> bridge priority <0-65535></pre> <p>Configures the bridge priority. The bridge priority parameter controls which bridge on the network is the STG root bridge. To make this switch the root bridge, configure the bridge priority lower than all other switches and bridges on your network. The lower the value, the higher the bridge priority. The range is 0 to 65535, in steps of 4096 (0, 4096, 8192...); the default value is 61440.</p> <p>Command mode: Global configuration</p> |
| <pre>spanning-tree stp <STG number> bridge hello-time <1-10></pre> <p>Configures the bridge Hello time. The Hello time specifies how often the root bridge transmits a configuration bridge protocol data unit (BPDU). Any bridge that is not the root bridge uses the root bridge Hello value. The range is 1 to 10 seconds, and the default is 2 seconds.</p> <p>This command does not apply to MSTP.</p> <p>Command mode: Global configuration</p> |
| <pre>spanning-tree stp <STG number> bridge maximum-age <6-40></pre> <p>Configures the bridge maximum age. The maximum age parameter specifies the maximum time the bridge waits without receiving a configuration bridge protocol data unit before it re configures the STG network. The range is 6 to 40 seconds, and the default is 20 seconds.</p> <p>This command does not apply to MSTP.</p> <p>Command mode: Global configuration</p> |

Table 222. Bridge Spanning Tree Configuration Options

| Command Syntax and Usage |
|--|
| <pre>spanning-tree stp <STG number> bridge forward-delay <4-30></pre> <p>Configures the bridge forward delay parameter. The forward delay parameter specifies the amount of time that a bridge port has to wait before it changes from the listening state to the learning state and from the learning state to the forwarding state. The range is 4 to 30 seconds, and the default is 15 seconds.</p> <p>This command does not apply to MSTP</p> <p>Command mode: Global configuration</p> |
| <pre>show spanning-tree [stp <STG no.>] bridge</pre> <p>Displays the current bridge STG parameters.</p> <p>Command mode: All</p> |

When configuring STG bridge parameters, the following formulas must be used:

- $2*(fwd-1) \geq mxage$
- $2*(hello+1) \leq mxage$

Spanning Tree RSTP/PVRST Port Configuration

By default, Spanning Tree is turned `off` for management ports, and turned `on` for data ports. STG port parameters include:

- Port priority
- Port path cost

Table 223. Spanning Tree Port Options

| Command Syntax and Usage |
|---|
| <pre>spanning-tree stp <STG number> priority <0-240></pre> <p>Configures the port priority. The port priority helps determine which bridge port becomes the designated port. In a network topology that has multiple bridge ports connected to a single segment, the port with the lowest port priority becomes the designated port for the segment. The default value is 128.</p> <p>RSTP/MSTP: The range is 0 to 240, in steps of 16 (0, 16, 32...) and the default is 128.</p> <p>Command mode: Interface port</p> |
| <pre>spanning-tree stp <STG number> path-cost <1-200000000, 0 for default></pre> <p>Configures the port path cost. The port path cost is used to help determine the designated port for a segment. Port path cost is based on the port speed, and is calculated as follows:</p> <ul style="list-style-type: none"> – 1Gbps = 20000 – 10Gbps = 2000 <p>The default value of 0 (zero) indicates that the default path cost will be computed for an auto negotiated link speed.</p> <p>Command mode: Interface port</p> |

Table 223. Spanning Tree Port Options (continued)

| Command Syntax and Usage |
|--|
| <pre>spanning-tree stp link-type {auto p2p shared}</pre> <p>Defines the type of link connected to the port, as follows:</p> <ul style="list-style-type: none"> – auto: Configures the port to detect the link type, and automatically match its settings. – p2p: Configures the port for Point-To-Point protocol. – shared: Configures the port to connect to a shared medium (usually a hub). <p>Command mode: Interface port</p> |
| <pre>spanning-tree stp <STG number> enable</pre> <p>Enables STG on the port.</p> <p>Command mode: Interface port</p> |
| <pre>no spanning-tree stp <STG number> enable</pre> <p>Disables STG on the port.</p> <p>Command mode: Interface port</p> |
| <pre>show interface port <port alias or number> spanning-tree stp <STG number></pre> <p>Displays the current STG port parameters.</p> <p>Command mode: All</p> |

Forwarding Database Configuration

Use the following commands to configure the Forwarding Database (FDB).

Table 224. FDB Configuration Commands

| Command Syntax and Usage |
|--|
| <pre>mac-address-table aging <0-65535></pre> <p>Configures the aging value for FDB entries, in seconds. The default value is 300.</p> <p>Command mode: Global configuration</p> |
| <pre>[no] mac-address-table mac-notification</pre> <p>Enables or disables MAC address notification.</p> <p>Command mode: Global configuration</p> |
| <pre>show mac-address-table</pre> <p>Display current FDB configuration.</p> <p>Command mode: All</p> |

Static FDB Configuration

Use the following commands to configure static entries in the Forwarding Database (FDB).

Table 225. FDB Configuration Commands

| Command Syntax and Usage |
|--|
| <pre>mac-address-table static <MAC address> vlan <VLAN number> {port <port alias or number> portchannel <trunk number> adminkey <I-65535>}</pre> <p>Adds a permanent FDB entry. Enter the MAC address using the following format, xx:xx:xx:xx:xx:xx</p> <p>For example, 08:00:20:12:34:56</p> <p>You can also enter the MAC address as follows: xxxxxxxxxxxx</p> <p>For example, 080020123456</p> <p>Command mode: Global configuration</p> |
| <pre>no mac-address-table static <MAC address> <VLAN number></pre> <p>Deletes a permanent FDB entry.</p> <p>Command mode: Global configuration</p> |
| <pre>show mac-address-table</pre> <p>Display current FDB configuration.</p> <p>Command mode: All</p> |

Static Multicast MAC Configuration

The following options are available to control the forwarding of known and unknown multicast packets:

- All multicast packets are flooded to the entire VLAN. This is the default switch behavior.
- Known multicast packets are forwarded only to those ports specified. Unknown multicast packets are flooded to the entire VLAN. To configure this option, define the Multicast MAC address for the VLAN and specify ports that are to receive multicast packets (`mac-address-table multicast`).
- Known multicast packets are forwarded only to those ports specified. Unknown multicast packets are dropped. To configure this option:
 - Define the Multicast MAC address for the VLAN and specify ports that are to receive multicast packets (`mac-address-table multicast`).
 - Enable Flood Blocking on ports that are not to receive multicast packets (`interface port x`) (`flood-blocking`).

Use the following commands to configure static Multicast MAC entries in the Forwarding Database (FDB).

Table 226. Static Multicast MAC Configuration Commands

| Command Syntax and Usage |
|--|
| <pre>mac-address-table multicast <MAC address> <VLAN number> <port alias or number></pre> <p>Adds a static multicast entry. You can list ports separated by a space, or enter a range of ports separated by a hyphen (-). For example:</p> <pre>mac-address-table multicast 01:00:00:23:3f:01 200 int1-int4</pre> <p>Command mode: Global configuration</p> |
| <pre>no mac-address-table multicast <MAC address> <VLAN number> <port alias or number></pre> <p>Deletes a static multicast entry.</p> <p>Command mode: Global configuration</p> |
| <pre>show mac-address-table multicast</pre> <p>Display the current static multicast entries.</p> <p>Command mode: All</p> |

ECP Configuration

Use the following commands to configure Edge Control Protocol (ECP).

Table 227. ECP Configuration Options

| Command Syntax and Usage |
|--|
| <pre>ecp retransmit-interval <100-9000></pre> <p>Configures ECP retransmit interval in milliseconds. Default value is 1000.</p> <p>Command mode: Global configuration</p> |
| <pre>default ecp retransmit-interval</pre> <p>Resets the ECP retransmit interval to the default 1000 milliseconds.</p> <p>Command mode: Global configuration</p> |
| <pre>show ecp [channels upper-layer-protocols]</pre> <p>Displays settings for all ECP channels or registered ULPs.</p> <p>Command mode: All</p> |

LLDP Configuration

Use the following commands to configure Link Layer Detection Protocol (LLDP).

Table 228. LLDP Configuration Commands

| Command Syntax and Usage |
|--|
| <pre>lldp refresh-interval <5-32768></pre> <p>Configures the message transmission interval, in seconds. The default value is 30.</p> <p>Command mode: Global configuration</p> |
| <pre>lldp holdtime-multiplier <2-10></pre> <p>Configures the message hold time multiplier. The hold time is configured as a multiple of the message transmission interval.</p> <p>The default value is 4.</p> <p>Command mode: Global configuration</p> |
| <pre>lldp trap-notification-interval <1-3600></pre> <p>Configures the trap notification interval, in seconds. The default value is 5.</p> <p>Command mode: Global configuration</p> |
| <pre>lldp transmission-delay <1-8192></pre> <p>Configures the transmission delay interval. The transmit delay timer represents the minimum time permitted between successive LLDP transmissions on a port.</p> <p>The default value is 2.</p> <p>Command mode: Global configuration</p> |

Table 228. LLDP Configuration Commands

| Command Syntax and Usage |
|--|
| <pre>lldp reinit-delay <1-10></pre> <p>Configures the re-initialization delay interval, in seconds. The re-initialization delay allows the port LLDP information to stabilize before transmitting LLDP messages.</p> <p>The default value is 2.</p> <p>Command mode: Global configuration</p> |
| <pre>lldp enable</pre> <p>Globally turns LLDP on. The default setting is on.</p> <p>Command mode: Global configuration</p> |
| <pre>no lldp enable</pre> <p>Globally turns LLDP off.</p> <p>Command mode: Global configuration</p> |
| <pre>show lldp</pre> <p>Display current LLDP configuration.</p> <p>Command mode: All</p> |

LLDP Port Configuration

Use the following commands to configure LLDP port options.

Table 229. LLDP Port Commands

| Command Syntax and Usage |
|--|
| <pre>lldp admin-status {disabled tx_only rx_only tx_rx}</pre> <p>Configures the LLDP transmission type for the port, as follows:</p> <ul style="list-style-type: none"> – Transmit only – Receive only – Transmit and receive – Disabled <p>The default setting is tx_rx.</p> <p>Command mode: Interface port</p> |
| <pre>[no] lldp trap-notification</pre> <p>Enables or disables SNMP trap notification for LLDP messages.</p> <p>Command mode: Interface port</p> |
| <pre>show interface port <port alias or number> lldp</pre> <p>Display current LLDP port configuration.</p> <p>Command mode: All</p> |

LLDP Optional TLV configuration

Use the following commands to configure LLDP port TLV (Type, Length, Value) options for the selected port.

Table 230. *Optional TLV Commands*

| Command Syntax and Usage |
|--|
| [no] lldp tlv portdesc Enables or disables the Port Description information type. Command mode: Interface port |
| [no] lldp tlv sysname Enables or disables the System Name information type. Command mode: Interface port |
| [no] lldp tlv sysdescr Enables or disables the System Description information type. Command mode: Interface port |
| [no] lldp tlv syscap Enables or disables the System Capabilities information type. Command mode: Interface port |
| [no] lldp tlv mgmtaddr Enables or disables the Management Address information type. Command mode: Interface port |
| [no] lldp tlv portvid Enables or disables the Port VLAN ID information type. Command mode: Interface port |
| [no] lldp tlv portprot Enables or disables the Port and VLAN Protocol ID information type. Command mode: Interface port |
| [no] lldp tlv vlanname Enables or disables the VLAN Name information type. Command mode: Interface port |
| [no] lldp tlv protid Enables or disables the Protocol ID information type. Command mode: Interface port |
| [no] lldp tlv macphy Enables or disables the MAC/Phy Configuration information type. Command mode: Interface port |

Table 230. Optional TLV Commands (continued)

| Command Syntax and Usage |
|---|
| <pre>[no] lldp tlv powermdi</pre> <p>Enables or disables the Power via MDI information type. Command mode: Interface port</p> |
| <pre>[no] lldp tlv linkaggr</pre> <p>Enables or disables the Link Aggregation information type. Command mode: Interface port</p> |
| <pre>[no] lldp tlv framesz</pre> <p>Enables or disables the Maximum Frame Size information type. Command mode: Interface port</p> |
| <pre>[no] lldp tlv dcbx</pre> <p>Enables or disables the Data Center Bridging Capability Exchange (DCBX) information type. Command mode: Interface port</p> |
| <pre>[no] lldp tlv all</pre> <p>Enables or disables all optional TLV information types. Command mode: Interface port</p> |
| <pre>show interface port <port alias or number> lldp</pre> <p>Display current LLDP port configuration. Command mode: All</p> |

Trunk Configuration

Trunk groups can provide super-bandwidth connections between EN4093 and EN4093R or other trunk capable devices. A *trunk* is a group of ports that act together, combining their bandwidth to create a single, larger port. Up to 64 trunk groups can be configured on the EN4093 and EN4093R, with the following restrictions:

- Any physical switch port can belong to no more than one trunk group.
- Up to 22 ports can belong to the same trunk group.
- Configure all ports in a trunk group with the same properties (speed, duplex, flow control, STG, VLAN, and so on).
- Trunking from non-IBM devices must comply with Cisco® EtherChannel® technology and exclude the PAgP networking protocol.

By default, each trunk group is empty and disabled.

Table 231. Trunk Configuration Commands

| Command Syntax and Usage | |
|---|---|
| portchannel <1-64> port <port alias or number> | Adds a physical port or ports to the current trunk group. You can add several ports, with each port separated by a comma (,) or a range of ports, separated by a dash (-). Command mode: Global configuration |
| no portchannel <1-64> port <port alias or number> | Removes a physical port or ports from the current trunk group. Command mode: Global configuration |
| [no] portchannel <1-64> enable | Enables or Disables the current trunk group. Command mode: Global configuration |
| no portchannel <1-64> | Removes the current trunk group configuration. Command mode: Global configuration |
| show portchannel <1-64> | Displays current trunk group parameters. Command mode: All |

IP Trunk Hash Configuration

Use the following commands to configure IP trunk hash settings for the EN4093 and EN4093R. Trunk hash parameters are set globally for the EN4093 and EN4093R. The trunk hash settings affect both static trunks and LACP trunks.

To achieve the most even traffic distribution, select options that exhibit a wide range of values for your particular network. You may use the configuration settings listed in [Table 232](#) combined with the hash parameters listed in [Table 233](#).

Table 232. Trunk Hash Settings

| Command Syntax and Usage |
|---|
| <pre>[no] portchannel thash ingress</pre> <p>Enables or disables use of the ingress port to compute the trunk hash value. The default setting is <code>disabled</code>.</p> <p>Command mode: Global configuration</p> |
| <pre>[no] portchannel thash L4port</pre> <p>Enables or disables use of Layer 4 service ports (TCP, UDP, etc.) to compute the hash value. The default setting is <code>disabled</code>.</p> <p>Command mode: Global configuration</p> |
| <pre>show portchannel hash</pre> <p>Display current trunk hash configuration.</p> <p>Command mode: All</p> |

Layer 2 Trunk Hash

Layer 2 trunk hash parameters are set globally. You can enable one or both parameters, to configure any of the following valid combinations:

- SMAC (source MAC only)
- DMAC (destination MAC only)
- SMAC and DMAC

Use the following commands to configure Layer 2 trunk hash parameters for the switch.

Table 233. Layer 2 Trunk Hash Options

| Command Syntax and Usage |
|---|
| <pre>[no] portchannel thash l2hash l2-source-mac-address</pre> <p>Enables or disables Layer 2 trunk hashing on the source MAC.</p> <p>Command mode: Global configuration</p> |
| <pre>[no] portchannel thash l2hash l2-destination-mac-address</pre> <p>Enables or disables Layer 2 trunk hashing on the destination MAC.</p> <p>Command mode: Global configuration</p> |

Table 233. Layer 2 Trunk Hash Options (continued)

| Command Syntax and Usage |
|--|
| <pre>[no] portchannel thash l2hash l2-source-destination-mac</pre> <p>Enables or disables Layer 2 trunk hashing on both the source and destination MAC.</p> <p>Command mode: Global configuration</p> |
| <pre>show portchannel hash</pre> <p>Displays the current trunk hash settings.</p> <p>Command mode: All</p> |

Layer 3 Trunk Hash

Layer 3 trunk hash parameters are set globally. You can enable one or both parameters, to configure any of the following valid combinations:

- SIP (source IP only)
- DIP (destination IP only)
- SIP and DIP

Use the following commands to configure Layer 3 trunk hash parameters for the switch.

Table 234. Layer 3 Trunk Hash Options

| Command Syntax and Usage |
|---|
| <pre>[no] portchannel thash l3thash l3-use-l2-hash</pre> <p>Enables or disables use of Layer 2 hash parameters only. When enabled, Layer 3 hashing parameters are cleared.</p> <p>Command mode: Global configuration</p> |
| <pre>[no] portchannel thash l3thash l3-source-ip-address</pre> <p>Enables or disables Layer 3 trunk hashing on the source IP address.</p> <p>Command mode: Global configuration</p> |
| <pre>[no] portchannel thash l3thash l3-destination-ip-address</pre> <p>Enables or disables Layer 3 trunk hashing on the destination IP address.</p> <p>Command mode: Global configuration</p> |
| <pre>[no] portchannel thash l3thash l3-source-destination-ip</pre> <p>Enables or disables Layer 3 trunk hashing on both the source and the destination IP address.</p> <p>Command mode: Global configuration</p> |
| <pre>show portchannel hash</pre> <p>Displays the current trunk hash settings.</p> <p>Command mode: All</p> |

Virtual Link Aggregation Control Protocol Configuration

Use the following commands to configure Virtual Link Aggregation Control Protocol (vLAG) for the EN4093 and EN4093R.

Table 235. Virtual Link Aggregation Control Protocol Commands

| Command Syntax and Usage |
|---|
| <pre>[no] vlag portchannel <1-64></pre> <p>Enables or disables the vLAG underlying trunk.</p> <p>Command mode: Global configuration</p> |
| <pre>[no] vlag adminkey <1-65535> enable</pre> <p>Enables or disables vLAG on the selected LACP <i>admin key</i>. LACP trunks formed with this <i>admin key</i> will be included in the vLAG configuration.</p> <p>Command mode: Global configuration</p> |
| <pre>[no] vlag enable</pre> <p>Enables or disables vLAG globally.</p> <p>Command mode: Global configuration</p> |
| <pre>[no] vlag tier-id <1-512></pre> <p>Sets the vLAG peer ID.</p> <p>Command mode: Global configuration</p> |
| <pre>vlag priority <0-65535></pre> <p>Configures the vLAG priority for the switch, used for election of Primary and Secondary vLAG switches. The switch with lower priority is elected to the role of Primary vLAG switch.</p> <p>Command mode: Global configuration</p> |
| <pre>vlag auto-recovery <240-3600></pre> <p>Sets the duration in seconds of the auto-recovery timer. This timer configures how long after boot-up configuration load, the switch can assume the Primary role from an unresponsive ISL peer and bring up the vLAG ports.</p> <p>The default value is 300.</p> <p>Command mode: Global configuration</p> |
| <pre>no vlag auto-recovery</pre> <p>Sets the auto-recovery timer to the default 300 seconds duration.</p> <p>Command mode: Global configuration</p> |

Table 235. Virtual Link Aggregation Control Protocol Commands (continued)

| Command Syntax and Usage |
|---|
| <pre>vlag startup-delay <1-3600></pre> <p>Sets the vLAG startup-delay value in seconds to the specified value.</p> <p>Note: Startup delay gives vLAG the ability to prevent traffic loss after a reboot. When a vLAG switch reboots, the vLAG ports are in an errdisabled state. After ISL is up, the vLAG ports are started one by one after the specified startup delay time. This specified time allows the switch to get BGP/OSFP ready through the uplinks so when the vLAG port starts up, all the traffic through those links flows smoothly. Admin status of the ports is honored by the vlag startup delay. For example, if the admin status of the vLAG port is down, those ports will be kept down even after the vLAG start-up delay.</p> <p>Command mode: Global configuration</p> |
| <pre>show vlag</pre> <p>Display current vLAG configuration.</p> <p>Command mode: All</p> |

vLAG Health Check Configuration

These commands allow you to configure a health check of synchronization between vLAG peers.

Table 236. vLAG Health Check Configuration Options

| Command Syntax and Usage |
|--|
| <pre>vlag hlthchk peer-ip {<IP address> <IPv6 address>}</pre> <p>Configures the IP address of the vLAG peer.</p> <p>Command mode: Global configuration</p> |
| <pre>[no] vlag hlthchk connect-retry-interval <1-300></pre> <p>Sets in seconds the vLAG health check connect retry interval, in seconds. The default value is 30.</p> <p>Command mode: Global configuration</p> |
| <pre>[no] vlag hlthchk keepalive-attempts <1-24></pre> <p>Sets the number of vLAG keep alive attempts. The default value is 3.</p> <p>Command mode: Global configuration</p> |
| <pre>[no] vlag hlthchk keepalive-interval <2-300></pre> <p>Sets the time between vLAG keep alive attempts, in seconds. The default value is 5.</p> <p>Command mode: Global configuration</p> |

vLAG ISL Configuration

These commands allow you to configure a dedicated inter-switch link (ISL) for synchronization between vLAG peers.

Table 237. vLAG ISL Configuration Options

| Command Syntax and Usage |
|--|
| <pre>[no] vlag isl portchannel <1-64> enable</pre> <p>Enables or disables vLAG Inter-Switch Link (ISL) on the selected trunk group.</p> <p>Command mode: Global configuration</p> |
| <pre>[no] vlag isl adminkey <1-65535></pre> <p>Enables or disables vLAG Inter-Switch Link (ISL) on the selected LACP <i>admin key</i>. LACP trunks formed with this <i>admin key</i> will be included in the ISL.</p> <p>Command mode: Global configuration</p> |
| <pre>show vlag information</pre> <p>Displays current vLAG parameters.</p> <p>Command mode: All</p> |

Link Aggregation Control Protocol Configuration

Use the following commands to configure Link Aggregation Control Protocol (LACP) for the EN4093 and EN4093R.

Table 238. Link Aggregation Control Protocol Commands

| Command Syntax and Usage |
|--|
| <pre>lacp system-priority <1-65535></pre> <p>Defines the priority value for the EN4093 and EN4093R. Lower numbers provide higher priority. The default value is 32768.</p> <p>Command mode: Global configuration</p> |
| <pre>lacp timeout {short long}</pre> <p>Defines the timeout period before invalidating LACP data from a remote partner. Choose <code>short</code> (3 seconds) or <code>long</code> (90 seconds). The default value is <code>long</code>.</p> <p>Note: It is recommended that you use a timeout value of <code>long</code>, to reduce LACPDU processing. If your EN4093 and EN4093R's CPU utilization rate remains at 100% for periods of 90 seconds or more, consider using static trunks instead of LACP.</p> <p>Command mode: Global configuration</p> |
| <pre>default lacp [system-priority timeout]</pre> <p>Restores either the VFSM priority value, timeout period or both to their default values.</p> <p>Command mode: Global configuration</p> |
| <pre>no lacp <1-65535></pre> <p>Deletes a selected LACP trunk, based on its <i>admin key</i>. This command is equivalent to disabling LACP on each of the ports configured with the same <i>admin key</i>.</p> <p>Command mode: Global configuration</p> |
| <pre>portchannel <trunk ID> lacp key <1-65535> suspend-individual</pre> <p>Enables a static LACP trunk. In this mode, ports sharing the same LACP admin key can form a single trunk, with the specified <code>trunk ID</code>. The active trunk is picked based on the ports which occupy first the trunk ID. Member ports that cannot join this trunk are prohibited from forming secondary LACP groups. Instead, they are set in a suspend state where they discard all non-LACP traffic.</p> <p>Command mode: Global configuration</p> |
| <pre>no portchannel <trunk ID></pre> <p>Disables a static LACP trunk.</p> <p>Command mode: Global configuration</p> |
| <pre>show lacp</pre> <p>Display current LACP configuration.</p> <p>Command mode: All</p> |

LACP Port Configuration

Use the following commands to configure Link Aggregation Control Protocol (LACP) for the selected port.

Table 239. Link Aggregation Control Protocol Commands

| Command Syntax and Usage |
|---|
| <pre>lacp mode {off active passive}</pre> <p>Set the LACP mode for this port, as follows:</p> <ul style="list-style-type: none"> – off Turn LACP off for this port. You can use this port to manually configure a static trunk. The default value is <code>off</code>. – active Turn LACP on and set this port to active. Active ports initiate LACPDUs. – passive Turn LACP on and set this port to passive. Passive ports do not initiate LACPDUs, but respond to LACPDUs from active ports. <p>Command mode: Interface port</p> |
| <pre>lacp priority <1-65535></pre> <p>Sets the priority value for the selected port. Lower numbers provide higher priority. The default value is 32768.</p> <p>Command mode: Interface port</p> |
| <pre>lacp key <1-65535></pre> <p>Set the admin key for this port. Only ports with the same <i>admin key</i> and <i>oper key</i> (operational state generated internally) can form a LACP trunk group.</p> <p>Command mode: Interface port</p> |
| <pre>port-channel min-links <1-32></pre> <p>Set the minimum number of links for this port. If the specified minimum number of ports are not available, the trunk is placed in the <code>down</code> state.</p> <p>Command mode: Interface port</p> |
| <pre>default lacp [key mode priority]</pre> <p>Restores the selected parameters to their default values.</p> <p>Command mode: Interface port</p> |
| <pre>show interface port <port alias or number> lacp</pre> <p>Displays the current LACP configuration for this port.</p> <p>Command mode: All</p> |

Layer 2 Failover Configuration

Use these commands to configure Layer 2 Failover. For more information about Layer 2 Failover, see “High Availability” in the *Networking OS Application Guide*.

Table 240. Layer 2 Failover Configuration Commands

| Command Syntax and Usage | |
|------------------------------------|---|
| <code>failover vlan</code> | <p>Globally turns VLAN monitor <code>on</code>. When the VLAN Monitor is <code>on</code>, the switch automatically disables only internal ports that belong to the same VLAN as ports in the failover trigger. The default value is <code>off</code>.</p> <p>Command mode: Global configuration</p> |
| <code>no failover vlan</code> | <p>Globally turns VLAN monitor <code>off</code>. When the VLAN Monitor is <code>on</code>, the switch automatically disables only internal ports that belong to the same VLAN as ports in the failover trigger. The default value is <code>off</code>.</p> <p>Command mode: Global configuration</p> |
| <code>failover enable</code> | <p>Globally turns Layer 2 Failover <code>on</code>.</p> <p>Command mode: Global configuration</p> |
| <code>no failover enable</code> | <p>Globally turns Layer 2 Failover <code>off</code>.</p> <p>Command mode: Global configuration</p> |
| <code>show failover trigger</code> | <p>Displays current Layer 2 Failover parameters.</p> <p>Command mode: All</p> |

Failover Trigger Configuration

Table 241. Failover Trigger Configuration Commands

| Command Syntax and Usage |
|---|
| <pre>[no] failover trigger <I-8> enable</pre> <p>Enables or disables the Failover trigger. Command mode: Global configuration</p> |
| <pre>no failover trigger <I-8></pre> <p>Deletes the Failover trigger. Command mode: Global configuration</p> |
| <pre>failover trigger <I-8> limit <0-1024></pre> <p>Configures the minimum number of operational links allowed within each trigger before the trigger initiates a failover event. If you enter a value of zero (0), the switch triggers a failover event only when no links in the trigger are operational. Command mode: Global configuration</p> |
| <pre>show failover trigger <I-8></pre> <p>Displays the current failover trigger settings. Command mode: All</p> |

Auto Monitor Configuration

Table 242. Auto Monitor Configuration Commands

| Command Syntax and Usage |
|---|
| <pre>failover trigger <I-8> amon portchannel <trunk group number></pre> <p>Adds a trunk group to the Auto Monitor. Command mode: Global configuration</p> |
| <pre>no failover trigger <I-8> amon portchannel <trunk group number></pre> <p>Removes a trunk group from the Auto Monitor. Command mode: Global configuration</p> |
| <pre>failover trigger <I-8> amon adminkey <I-65535></pre> <p>Adds an LACP <i>admin key</i> to the Auto Monitor. LACP trunks formed with this <i>admin key</i> will be included in the Auto Monitor. Command mode: Global configuration</p> |
| <pre>no failover trigger <I-8> amon adminkey <I-65535></pre> <p>Removes an LACP <i>admin key</i> from the Auto Monitor. Command mode: Global configuration</p> |

Failover Manual Monitor Port Configuration

Use these commands to define the port link(s) to monitor. The Manual Monitor Port configuration accepts only external uplink ports.

Note: AMON and MMON configurations are mutually exclusive.

Table 243. Failover Manual Monitor Port Commands

| Command Syntax and Usage |
|--|
| <pre>failover trigger <1-8> mmon monitor member <port alias or number></pre> <p>Adds the selected port to the Manual Monitor Port configuration.</p> <p>Command mode: Global configuration</p> |
| <pre>no failover trigger <1-8> mmon monitor member <port alias or number></pre> <p>Removes the selected port from the Manual Monitor Port configuration.</p> <p>Command mode: Global configuration</p> |
| <pre>failover trigger <1-8> mmon monitor portchannel <trunk number></pre> <p>Adds the selected trunk group to the Manual Monitor Port configuration.</p> <p>Command mode: Global configuration</p> |
| <pre>no failover trigger <1-8> mmon monitor portchannel <trunk number></pre> <p>Removes the selected trunk group to the Manual Monitor Port configuration.</p> <p>Command mode: Global configuration</p> |
| <pre>failover trigger <1-8> mmon monitor adminkey <1-65535></pre> <p>Adds an LACP <i>admin key</i> to the Manual Monitor Port configuration. LACP trunks formed with this <i>admin key</i> will be included in the Manual Monitor Port configuration.</p> <p>Command mode: Global configuration</p> |
| <pre>no failover trigger <1-8> mmon monitor adminkey <1-65535></pre> <p>Removes an LACP admin key from the Manual Monitor Port configuration.</p> <p>Command mode: Global configuration</p> |
| <pre>show failover trigger <1-8></pre> <p>Displays the current Failover settings.</p> <p>Command mode: All</p> |

Failover Manual Monitor Control Configuration

Use these commands to define the port link(s) to control. The Manual Monitor Control configuration accepts internal and external ports, but not management ports.

Table 244. Failover Manual Monitor Control Commands

| Command Syntax and Usage |
|--|
| <pre>failover trigger <1-8> mmon control member <port alias or number></pre> <p>Adds the selected port to the Manual Monitor Control configuration.</p> <p>Command mode: Global configuration</p> |
| <pre>no failover trigger <1-8> mmon control member <port alias or number></pre> <p>Removes the selected port from the Manual Monitor Control configuration.</p> <p>Command mode: Global configuration</p> |
| <pre>failover trigger <1-8> mmon control portchannel <trunk number></pre> <p>Adds the selected trunk group to the Manual Monitor Control configuration.</p> <p>Command mode: Global configuration</p> |
| <pre>no failover trigger <1-8> mmon control portchannel <trunk number></pre> <p>Removes the selected trunk group to the Manual Monitor Control configuration.</p> <p>Command mode: Global configuration</p> |
| <pre>failover trigger <1-8> mmon control adminkey <1-65535></pre> <p>Adds an LACP <i>admin key</i> to the Manual Monitor Control configuration. LACP trunks formed with this <i>admin key</i> will be included in the Manual Monitor Control configuration.</p> <p>Command mode: Global configuration</p> |
| <pre>no failover trigger <1-8> mmon control adminkey <1-65535></pre> <p>Removes an LACP admin key from the Manual Monitor Control configuration.</p> <p>Command mode: Global configuration</p> |
| <pre>show failover trigger <1-8></pre> <p>Displays the current Failover settings.</p> <p>Command mode: All</p> |

Hot Links Configuration

Use these commands to configure Hot Links. For more information about Hot Links, see "Hot Links" in the *Networking OS 7.7 Application Guide*.

Table 245. Hot Links Configuration Commands

| Command Syntax and Usage | |
|-----------------------------------|--|
| [no] hotlinks bpdu | <p>Enables or disables flooding of Spanning-Tree BPDUs on the active Hot Links interface when the interface belongs to a Spanning Tree group that is globally turned <code>off</code>. This feature can prevent unintentional loop scenarios (for example, if two uplinks come up at the same time).</p> <p>The default setting is <code>disabled</code>.</p> <p>Command mode: Global configuration</p> |
| [no] hotlinks fdb-update | <p>Enables or disables FDB Update, which allows the switch to send FDB and MAC update packets over the active interface.</p> <p>The default value is <code>disabled</code>.</p> <p>Command mode: Global configuration</p> |
| hotlinks fdb-update-rate <10-200> | <p>Configures the FDB Update rate, in packets per second.</p> <p>Command mode: Global configuration</p> |
| hotlinks enable | <p>Globally enables Hot Links.</p> <p>Command mode: Global configuration</p> |
| no hotlinks enable | <p>Globally disables Hot Links.</p> <p>Command mode: Global configuration</p> |
| show hotlinks | <p>Displays current Hot Links parameters.</p> <p>Command mode: All</p> |

Hot Links Trigger Configuration

Table 246. Hot Links Trigger Configuration Commands

| Command Syntax and Usage | |
|--|---|
| hotlinks trigger <I-200> forward-delay <0-3600> | Configures the Forward Delay interval, in seconds. The default value is 1. Command mode: Global configuration |
| [no] hotlinks trigger <I-200> name <I-32 characters> | Defines a name for the Hot Links trigger. Command mode: Global configuration |
| [no] hotlinks trigger <I-200> preemption | Enables or disables pre-emption, which allows the Master interface to transition to the Active state whenever it becomes available. The default setting is enabled. Command mode: Global configuration |
| [no] hotlinks trigger <I-200> enable | Enables or disables the Hot Links trigger. Command mode: Global configuration |
| no hotlinks trigger <I-200> | Deletes the Hot Links trigger. Command mode: Global configuration |
| show hotlinks trigger <I-200> | Displays the current Hot Links trigger settings. Command mode: All |

Hot Links Master Configuration

Use the following commands to configure the Hot Links Master interface.

Table 247. Hot Links Master Configuration Commands

| Command Syntax and Usage |
|--|
| <pre>[no] hotlinks trigger <1-200> master port <port alias or number></pre> <p>Adds or removes the selected port to the Hot Links Master interface.</p> <p>Command mode: Global configuration</p> |
| <pre>[no] hotlinks trigger <1-200> master portchannel <trunk group number></pre> <p>Adds or removes the selected trunk group to the Master interface.</p> <p>Command mode: Global configuration</p> |
| <pre>[no] hotlinks trigger <1-200> master adminkey <0-65535></pre> <p>Adds or removes an LACP <i>admin key</i> to the Master interface. LACP trunks formed with this <i>admin key</i> will be included in the Master interface.</p> <p>Command mode: Global configuration</p> |
| <pre>show hotlinks trigger <1-200></pre> <p>Displays the current Hot Links trigger settings.</p> <p>Command mode: All</p> |

Hot Links Backup Configuration

Use the following commands to configure the Hot Links Backup interface.

Table 248. Hot Links Backup Configuration Commands

| Command Syntax and Usage |
|--|
| <pre>[no] hotlinks trigger <1-200> backup port <port alias or number></pre> <p>Adds or removes the selected port to the Hot Links Backup interface.</p> <p>Command mode: Global configuration</p> |
| <pre>[no] hotlinks trigger <1-200> backup portchannel <trunk group number></pre> <p>Adds or removes the selected trunk group to the Backup interface.</p> <p>Command mode: Global configuration</p> |
| <pre>[no] hotlinks trigger <1-200> backup adminkey <0-65535></pre> <p>Adds or removes an LACP <i>admin key</i> to the Backup interface. LACP trunks formed with this <i>admin key</i> will be included in the Backup interface.</p> <p>Command mode: Global configuration</p> |
| <pre>show hotlinks trigger <1-200></pre> <p>Displays the current Hot Links trigger settings.</p> <p>Command mode: All</p> |

VLAN Configuration

These commands configure VLAN attributes, change the status of each VLAN, change the port membership of each VLAN, and delete VLANs.

By default, VLAN 1 is the only VLAN configured on the switch. Internal server ports and external uplink ports are members of VLAN 1 by default. Up to 4096 VLANs can be configured on the EN4093 and EN4093R.

VLANs can be assigned any number between 1 and 4094. VLAN 4095 is reserved for switch management.

Table 249. VLAN Configuration Commands

| Command Syntax and Usage |
|--|
| <pre>vlan <VLAN number></pre> <p>Enter VLAN configuration mode.</p> <p>Command mode: Global configuration</p> |
| <pre>protocol-vlan <1-8></pre> <p>Configures the Protocol-based VLAN (PVLAN).</p> <p>Command mode: VLAN</p> |
| <pre>name <1-32 characters></pre> <p>Assigns a name to the VLAN or changes the existing name. The default VLAN name is the first one.</p> <p>Command mode: VLAN</p> |
| <pre>stg <STG number></pre> <p>Assigns a VLAN to a Spanning Tree Group.</p> <p>Command mode: VLAN</p> |
| <pre>[no] vmap <1-128> [extports intports]</pre> <p>Adds or removes a VLAN Map to the VLAN membership. You can choose to limit operation of the VLAN Map to internal ports only or external ports only. If you do not select a port type, the VMAP is applied to the entire VLAN.</p> <p>Command mode: VLAN</p> |
| <pre>member <port alias or number></pre> <p>Adds port(s) to the VLAN membership.</p> <p>Command mode: VLAN</p> |
| <pre>no member <port alias or number></pre> <p>Removes port(s) from this VLAN.</p> <p>Command mode: VLAN</p> |
| <pre>[no] management</pre> <p>Configures this VLAN as a management VLAN. You must add the management ports (MGT1 and MGT2) to each new management VLAN. External ports cannot be added to management VLANs.</p> <p>Command mode: VLAN</p> |

Table 249. VLAN Configuration Commands (continued)

| Command Syntax and Usage | |
|--------------------------|---|
| [no] flood | <p>Configures the switch to flood unregistered IP multicast traffic to all ports. The default setting is enabled.</p> <p>Note: If none of the IGMP hosts reside on the VLAN of the streaming server for a IPMC group, you must disable IGMP flooding to ensure that multicast data is forwarded across the VLANs for that IPMC group.</p> <p>Command mode: VLAN</p> |
| [no] cpu | <p>Configures the switch to forward unregistered IP multicast traffic to the MP, which adds an entry in the IPMC table, as follows:</p> <ul style="list-style-type: none"> – If no Mrouter is present, drop subsequent packets with same IPMC. – If an Mrouter is present, forward subsequent packets to the Mrouter(s) on the ingress VLAN. <p>The default setting is enabled.</p> <p>Note: If both <code>flood</code> and <code>cpu</code> are disabled, then the switch drops all unregistered IPMC traffic.</p> <p>Command mode: VLAN</p> |
| [no] optflood | <p>Enables or disables optimized flooding. When enabled, optimized flooding avoids packet loss during the learning period. The default setting is disabled.</p> <p>Command mode: VLAN</p> |
| enable | <p>Enables this VLAN.</p> <p>Command mode: VLAN</p> |
| no enable | <p>Disables this VLAN without removing it from the configuration.</p> <p>Command mode: VLAN</p> |
| no vlan <VLAN number> | <p>Deletes this VLAN.</p> <p>Command mode: VLAN</p> |
| show vlan information | <p>Displays the current VLAN configuration.</p> <p>Command mode: All</p> |

Note: All ports must belong to at least one VLAN. Any port which is removed from a VLAN and which is not a member of any other VLAN is automatically added to default VLAN 1. You cannot remove a port from VLAN 1 if the port has no membership in any other VLAN. Also, you cannot add a port to more than one VLAN unless the port has VLAN tagging turned on.

Protocol-Based VLAN Configuration

Use the following commands to configure Protocol-based VLAN for the selected VLAN.

Table 250. Protocol VLAN Configuration Commands

| Command Syntax and Usage |
|--|
| <pre>protocol-vlan <1-8> frame-type {ether2 llc snap} <Ethernet type></pre> <p>Configures the frame type and the Ethernet type for the selected protocol. Ethernet type consists of a 4-digit (16 bit) hex code, such as 0080 (IPv4).</p> <p>Command mode: VLAN</p> |
| <pre>protocol-vlan <1-8> protocol <protocol type></pre> <p>Selects a pre-defined protocol, as follows:</p> <ul style="list-style-type: none"> - decEther2:DEC Local Area Transport - ipv4Ether2:Internet IP (IPv4) - ipv6Ether2:IPv6 - ipx802.2:Novell IPX 802.2 - ipx802.3:Novell IPX 802.3 - ipxEther2:Novell IPX - ipxSnap:Novell IPX SNAP - netbios:NetBIOS 802.2 - rarpEther2:Reverse ARP - sna802.2:SNA 802.2 - snaEther2:IBM SNA Service on Ethernet - vinesEther2:Banyan VINES - xnsEther2:XNS Compatibility <p>Command mode: VLAN</p> |
| <pre>protocol-vlan <1-8> priority <0-7></pre> <p>Configures the priority value for this PVLAN.</p> <p>Command mode: VLAN</p> |
| <pre>protocol-vlan <1-8> member <port alias or number></pre> <p>Adds a port to the selected PVLAN.</p> <p>Command mode: VLAN</p> |
| <pre>no protocol-vlan <1-8> member <port alias or number></pre> <p>Removes a port from the selected PVLAN.</p> <p>Command mode: VLAN</p> |
| <pre>[no] protocol-vlan <1-8> tag-pvlan <port alias or number></pre> <p>Defines a port that will be tagged by the selected protocol on this VLAN.</p> <p>Command mode: VLAN</p> |

Table 250. Protocol VLAN Configuration Commands (continued)

| Command Syntax and Usage |
|---|
| <pre>protocol-vlan <1-8> enable</pre> <p>Enables the selected protocol on the VLAN. Command mode: VLAN</p> |
| <pre>no protocol-vlan <1-8> enable</pre> <p>Disables the selected protocol on the VLAN. Command mode: VLAN</p> |
| <pre>no protocol-vlan <1-8></pre> <p>Deletes the selected protocol configuration from the VLAN. Command mode: VLAN</p> |
| <pre>show protocol-vlan <1-8></pre> <p>Displays current parameters for the selected PVLAN. Command mode: All</p> |

Private VLAN Configuration

Use the following commands to configure Private VLAN.

Table 251. Private VLAN Configuration Commands

| Command Syntax and Usage | |
|---|--|
| <code>[no] private-vlan type primary</code> | <p>Enables or disables the VLAN type as a Primary VLAN.</p> <p>A Private VLAN must have only one primary VLAN. The primary VLAN carries unidirectional traffic to ports on the isolated VLAN or to community VLAN.</p> <p>Command mode: VLAN</p> |
| <code>[no] private-vlan type community</code> | <p>Enables or disables the VLAN type as a community VLAN.</p> <p>Community VLANs carry upstream traffic from host ports. A Private VLAN may have multiple community VLANs.</p> <p>Command mode: VLAN</p> |
| <code>[no] private-vlan type isolated</code> | <p>Enables or disables the VLAN type as an isolated VLAN.</p> <p>The isolated VLAN carries unidirectional traffic from host ports. A Private VLAN may have only one isolated VLAN.</p> <p>Command mode: VLAN</p> |
| <code>no private-vlan type</code> | <p>Clears the private-VLAN type.</p> <p>Command mode: VLAN</p> |
| <code>[no] private-vlan map [add remove] <secondary VLAN list></code> | <p>Configures Private VLAN mapping between a primary VLAN and secondary VLANs. Enter the primary VLAN ID. Secondary VLANs have the type defined as isolated or community. Use the no form to remove the</p> <ul style="list-style-type: none"> – mapping between the secondary VLAN and the primary VLAN <p>Command mode: VLAN</p> |
| <code>private-vlan enable</code> | <p>Enables the private VLAN.</p> <p>Command mode: VLAN</p> |
| <code>no private-vlan enable</code> | <p>Disables the Private VLAN.</p> <p>Command mode: VLAN</p> |
| <code>show private-vlan [<2-4094>]</code> | <p>Displays current parameters for the selected Private VLAN(s).</p> <p>Command mode: VLAN</p> |

Layer 3 Configuration

The following table describes basic Layer 3 Configuration commands. The following sections provide more detailed information and commands.

Table 252. Layer 3 Configuration Commands

| Command Syntax and Usage |
|---|
| <pre>interface ip <interface number></pre> <p>Configures the IP Interface. The EN4093 and EN4093R supports up to 128 IP interfaces. To view command options, see page 368.</p> <p>Command mode: Global configuration</p> |
| <pre>route-map {<1-32>}</pre> <p>Enter IP Route Map mode. To view command options, see page 379.</p> <p>Command mode: Global configuration</p> |
| <pre>router rip</pre> <p>Configures the Routing Interface Protocol. To view command options, see page 383.</p> <p>Command mode: Global configuration</p> |
| <pre>router ospf</pre> <p>Configures OSPF. To view command options, see page 387.</p> <p>Command mode: Global configuration</p> |
| <pre>ipv6 router ospf</pre> <p>Enters OSPFv3 configuration mode. To view command options, see page 446.</p> <p>Command mode: Global configuration</p> |
| <pre>router bgp</pre> <p>Configures Border Gateway Protocol. To view command options, see page 397.</p> <p>Command mode: Global configuration</p> |
| <pre>router vrrp</pre> <p>Configures Virtual Router Redundancy. To view command options, see page 429.</p> <p>Command mode: Global configuration</p> |
| <pre>ip pim component <1-2></pre> <p>Enters Protocol Independent Multicast (PIM) component configuration mode. To view command options, see page 442.</p> <p>Command mode: Global configuration</p> |

Table 252. Layer 3 Configuration Commands

| Command Syntax and Usage |
|--|
| <pre>ip router-id <IP address></pre> <p>Sets the router ID.</p> <p>Command mode: Global configuration</p> |
| <pre>show layer3</pre> <p>Displays the current IP configuration.</p> <p>Command mode: All</p> |

IP Interface Configuration

The EN4093 and EN4093R supports up to 128 IP interfaces. Each IP interface represents the EN4093 and EN4093R on an IP subnet on your network. The Interface option is disabled by default.

IP Interface 127 and 128 are reserved for switch management. If the IPv6 feature is enabled on the switch, IP Interface 125 and 126 are also reserved.

Note: To maintain connectivity between the management module and the EN4093 and EN4093R, use the management module interface to change the IP address of the switch.

Table 253. IP Interface Configuration Commands

| Command Syntax and Usage | |
|---|---|
| <code>interface ip <interface number></code> | Enter IP interface mode. Command mode: Global configuration |
| <code>ip address <IP address> [<IP netmask>]</code> | Configures the IP address of the switch interface, using dotted decimal notation. Command mode: Interface IP |
| <code>ip netmask <IP netmask></code> | Configures the IP subnet address mask for the interface, using dotted decimal notation. Command mode: Interface IP |
| <code>ipv6 address <IP address (such as 3001:0:0:0:0:abcd:12)> [<IPv6 prefix length (1-128)>] [enable anycast]</code> | Configures the IPv6 address of the switch interface, using hexadecimal format with colons. Command mode: Interface IP |
| <code>ipv6 secaddr6 address <IP address (such as 3001:0:0:0:0:abcd:12)> <prefix length> [anycast]</code> | Configures the secondary IPv6 address of the switch interface, using hexadecimal format with colons. Command mode: Interface IP |
| <code>ipv6 prefixlen <IPv6 prefix length (1-128)></code> | Configures the subnet IPv6 prefix length. The default value is 0 (zero). Command mode: Interface IP |
| <code>vlan <VLAN number></code> | Configures the VLAN number for this interface. Each interface can belong to one VLAN. Command mode: Interface IP |

Table 253. IP Interface Configuration Commands (continued)

| Command Syntax and Usage | |
|--------------------------------------|--|
| [no] relay | <p>Enables or disables the BOOTP relay on this interface. The default setting is enabled.</p> <p>Command mode: Interface IP</p> |
| [no] ip6host | <p>Enables or disables the IPv6 Host Mode on this interface. The default setting is disabled for data interfaces, and enabled for the management interface.</p> <p>Command mode: Interface IP</p> |
| [no] ipv6 unreachable | <p>Enables or disables sending of ICMP Unreachable messages. The default setting is enabled.</p> <p>Command mode: Interface IP</p> |
| enable | <p>Enables this IP interface.</p> <p>Command mode: Interface IP</p> |
| no enable | <p>Disables this IP interface.</p> <p>Command mode: Interface IP</p> |
| no interface ip <interface number> | <p>Removes this IP interface.</p> <p>Command mode: Interface IP</p> |
| show interface ip <interface number> | <p>Displays the current interface settings.</p> <p>Command mode: All</p> |

IPv6 Neighbor Discovery Configuration

The following table describes the IPv6 Neighbor Discovery Configuration commands.

Table 254. IPv6 Neighbor Discovery Configuration Options

| Command Syntax and Usage | |
|--|---|
| [no] ipv6 nd suppress-ra | <p>Enables or disables IPv6 Router Advertisements on the interface. The default setting is disabled (suppress Router Advertisements).</p> <p>Command mode: Interface IP</p> |
| [no] ipv6 nd managed-config | <p>Enables or disables the managed address configuration flag of the interface. When enabled, the host IP address can be set automatically through DHCP. The default setting is disabled.</p> <p>Command mode: Interface IP</p> |
| [no] ipv6 nd other-config | <p>Enables or disables the other stateful configuration flag, which allows the interface to use DHCP for other stateful configuration. The default setting is disabled.</p> <p>Command mode: Interface IP</p> |
| ipv6 nd ra-lifetime <0-9000> | <p>Configures the IPv6 Router Advertisement lifetime interval. The RA lifetime interval must be greater than or equal to the RA maximum interval (advint). The default value is 1800 seconds.</p> <p>Command mode: Interface IP</p> |
| [no] ipv6 nd dad-attempts <1-10> | <p>Configures the maximum number of duplicate address detection attempts. The default value is 1.</p> <p>Command mode: Interface IP</p> |
| [no] ipv6 nd reachable-time <1-3600> [no] ipv6 nd reachable-time <1-3600000> ms | <p>Configures the advertised reachability time, in seconds or milliseconds (ms). The default value is 30 seconds.</p> <p>Command mode: Interface IP</p> |
| [no] ipv6 nd ra-interval <4-1800> | <p>Configures the Router Advertisement maximum interval. The default value is 600 seconds.</p> <p>Note: Set the maximum RA interval to a value greater than or equal to 4/3 of the minimum RA interval.</p> <p>Command mode: Interface IP</p> |

Table 254. IPv6 Neighbor Discovery Configuration Options (continued)

| Command Syntax and Usage | |
|--|---|
| <pre>[no] ipv6 nd ra-intervalmin <3-1800></pre> | <p>Configures the Router Advertisement minimum interval. The default value is 198 seconds.</p> <p>Note: Set the minimum RA interval to a value less than or equal to 0.75 of the maximum RA interval.</p> <p>Command mode: Interface IP</p> |
| <pre>[no] ipv6 nd retransmit-time <0-4294967> [no] ipv6 nd retransmit-time <0-4294967295> ms</pre> | <p>Configures the Router Advertisement re-transmit timer, in seconds or milliseconds (ms). The default value is 1 second.</p> <p>Command mode: Interface IP</p> |
| <pre>[no] ipv6 nd hops-limit <0-255></pre> | <p>Configures the Router Advertisement hop limit. The default value is 64.</p> <p>Command mode: Interface IP</p> |
| <pre>[no] ipv6 nd advmtu</pre> | <p>Enables or disables the MTU option in Router Advertisements. The default setting is enabled.</p> <p>Command mode: Interface IP</p> |

Default Gateway Configuration

The switch can be configured with up to 4 IPv4 gateways. Gateways 1–4 are reserved for default gateways. Gateway 4 is reserved for switch management. Default gateway indices are:

- 1-2: Data gateways
- 3: External management gateway
- 4: Internal management gateway

This option is disabled by default.

Table 255. Default Gateway Configuration Commands

| Command Syntax and Usage | |
|--|--|
| <code>ip gateway <1-4> address <IP address></code> | Configures the IP address of the default IP gateway using dotted decimal notation. Default gateway indices are: Command mode: Global configuration |
| <code>ip gateway <1-4> interval <0-60></code> | The switch pings the default gateway to verify that it's up. This command sets the time between health checks. The range is from 0 to 60 seconds. The default is 2 seconds. Command mode: Global configuration |
| <code>ip gateway <1-4> retry <1-120></code> | Sets the number of failed health check attempts required before declaring this default gateway inoperative. The range is from 1 to 120 attempts. The default is 8 attempts. Command mode: Global configuration |
| <code>[no] ip gateway <1-4> arp-health-check</code> | Enables or disables Address Resolution Protocol (ARP) health checks. The default setting is disabled. The <code>arp</code> option does not apply to management gateways. Command mode: Global configuration |
| <code>ip gateway <1-4> enable</code> | Enables the gateway for use. Command mode: Global configuration |
| <code>no ip gateway <1-4> enable</code> | Disables the gateway. Command mode: Global configuration |

Table 255. Default Gateway Configuration Commands (continued)

| Command Syntax and Usage |
|--|
| <pre>no ip gateway <I-4></pre> <p>Deletes the gateway from the configuration. Command mode: Global configuration</p> |
| <pre>show ip gateway <I-4></pre> <p>Displays the current gateway settings. Command mode: All</p> |

IPv4 Static Route Configuration

Up to 128 IPv4 static routes can be configured.

Table 256. IPv4 Static Route Configuration Commands

| Command Syntax and Usage |
|--|
| <pre>ip route <IP subnet> <IP netmask> <IP nexthop> [<interface number>]</pre> <p>Adds a static route. You will be prompted to enter a destination IP address, destination subnet mask, and gateway address. Enter all addresses using dotted decimal notation. Command mode: Global configuration</p> |
| <pre>no ip route <IP subnet> <IP netmask> [<interface number>]</pre> <p>Removes a static route. The destination address of the route to remove must be specified using dotted decimal notation. Command mode: Global configuration</p> |
| <pre>no ip route destination-address <IP address></pre> <p>Clears all IP static routes with this destination. Command mode: Global configuration</p> |
| <pre>no ip route gateway <IP address></pre> <p>Clears all IP static routes that use this gateway. Command mode: Global configuration</p> |
| <pre>ip route interval <I-60></pre> <p>Configures the ping interval for ECMP health checks, in seconds. The default value is one second. Command mode: Global configuration</p> |
| <pre>ip route retries <I-60></pre> <p>Configures the number of health check retries allowed before the switch declares that the gateway is down. The default value is 3. Command mode: Global configuration</p> |
| <pre>show ip route static</pre> <p>Displays the current IP static routes. Command mode: All</p> |

IP Multicast Route Configuration

The following table describes the IP Multicast (IPMC) route commands.

Note: Before you can add an IPMC route, IGMP must be turned on and IGMP Relay/Snooping must be enabled.

Table 257. IP Multicast Route Configuration Commands

| Command Syntax and Usage | |
|--|---|
| <pre>ip mroute <IPMC destination> <VLAN number> <port alias or number> {primary backup host} [<virtual router ID> none]</pre> | <p>Adds a static multicast route. The destination address, VLAN, and member port of the route must be specified. Indicate whether the route is used for a primary, backup, or host multicast router.</p> <p>Command mode: Global configuration</p> |
| <pre>no ip mroute <IPMC destination> <VLAN number> <port alias or number> {primary backup host} [<virtual router ID> none]</pre> | <p>Removes a static multicast route. The destination address, VLAN, and member port of the route to remove must be specified.</p> <p>Command mode: Global configuration</p> |
| <pre>ip mroute <IP address> <VLAN number> portchannel <trunk group number> {primary backup host} [<virtual router ID> none]</pre> | <p>Adds a static multicast route. The destination address, VLAN, and member trunk group of the route must be specified. Indicate whether the route is used for a primary, backup, or host multicast router.</p> <p>Command mode: Global configuration</p> |
| <pre>no ip mroute <IP address> <VLAN number> portchannel <trunk group number> {primary backup host} [<virtual router ID> none]</pre> | <p>Removes a static multicast route. The destination address, VLAN, and member trunk group of the route to remove must be specified.</p> <p>Command mode: Global configuration</p> |
| <pre>ip mroute <IP address> <VLAN number> adminkey <1-65535> {primary backup host} [<virtual router ID> none]</pre> | <p>Adds a static multicast route. The destination address, VLAN, and LACP <i>admin key</i> of the route must be specified. Indicate whether the route is used for a primary, backup, or host multicast router.</p> <p>Command mode: Global configuration</p> |
| <pre>no ip mroute <IP address> <VLAN number> adminkey <1-65535> {primary backup host} [<virtual router ID> none]</pre> | <p>Removes a static multicast route. The destination address, VLAN, and LACP <i>admin key</i> of the route to remove must be specified.</p> <p>Command mode: Global configuration</p> |

Table 257. IP Multicast Route Configuration Commands (continued)

| Command Syntax and Usage |
|---|
| <pre>no ip mroute all</pre> <p>Removes all the static multicast routes configured.</p> <p>Command mode: Global configuration</p> |
| <pre>show ip mroute</pre> <p>Displays the current IP multicast routes.</p> <p>Command mode: All</p> |

ARP Configuration

Address Resolution Protocol (ARP) is the TCP/IP protocol that resides within the Internet layer. ARP resolves a physical address from an IP address. ARP queries machines on the local network for their physical addresses. ARP also maintains IP to physical address pairs in its cache memory. In any IP communication, the ARP cache is consulted to see if the IP address of the computer or the router is present in the ARP cache. Then the corresponding physical address is used to send a packet.

Table 258. ARP Configuration Commands

| Command Syntax and Usage |
|--|
| <pre>ip arp rearp <2-120></pre> <p>Defines re-ARP period, in minutes, for entries in the switch arp table. When ARP entries reach this value the switch will re-ARP for the address to attempt to refresh the ARP cache.</p> <p>The default value is 5 minutes.</p> <p>Command mode: Global configuration</p> |
| <pre>show ip arp</pre> <p>Displays the current ARP configurations.</p> <p>Command mode: All</p> |

ARP Static Configuration

Static ARP entries are permanent in the ARP cache and do not age out like the ARP entries that are learned dynamically. Static ARP entries enable the switch to reach the hosts without sending an ARP broadcast request to the network. Static ARPs are also useful to communicate with devices that do not respond to ARP requests. Static ARPs can also be configured on some gateways as a protection against malicious ARP Cache corruption and possible DOS attacks.

Table 259. ARP Static Configuration Commands

| Command Syntax and Usage |
|---|
| <pre>ip arp <IP address> <MAC address> vlan <vlan number> port <port alias or number></pre> <p>Adds a permanent ARP entry.</p> <p>Command mode: Global configuration</p> |
| <pre>ip arp <destination unicast IP address> <destination multicast MAC address> vlan <cluster vlan number></pre> <p>Adds a static multicast ARP entry for Network Load Balancing (NLB).</p> <p>Command mode: Global configuration</p> |
| <pre>no ip arp <IP address></pre> <p>Deletes a permanent ARP entry.</p> <p>Command mode: Global configuration</p> |
| <pre>no ip arp all</pre> <p>Deletes all static ARP entries.</p> <p>Command mode: Global configuration</p> |
| <pre>show ip arp static</pre> <p>Displays current static ARP configuration.</p> <p>Command mode: All</p> |

IP Forwarding Configuration

Table 260. IP Forwarding Configuration Commands

| Command Syntax and Usage | |
|-------------------------------------|--|
| [no] ip routing directed-broadcasts | <p>Enables or disables forwarding directed broadcasts. The default setting is disabled.</p> <p>Command mode: Global configuration</p> |
| [no] ip routing no-icmp-redirect | <p>Enables or disables ICMP re-directs. The default setting is disabled.</p> <p>Command mode: Global configuration</p> |
| [no] ip routing icmp6-redirect | <p>Enables or disables IPv6 ICMP re-directs. The default setting is disabled.</p> <p>Command mode: Global configuration</p> |
| ip routing | <p>Enables IP forwarding (routing) on the EN4093 and EN4093R. Forwarding is turned on by default.</p> <p>Command mode: Global configuration</p> |
| no ip routing | <p>Disables IP forwarding (routing) on the EN4093 and EN4093R.</p> <p>Command mode: Global configuration</p> |
| show ip routing | <p>Displays the current IP forwarding settings.</p> <p>Command mode: All</p> |

Network Filter Configuration

Table 261. IP Network Filter Configuration Commands

| Command Syntax and Usage | |
|---|--|
| <pre>ip match-address <1-256> <IP address> <IP netmask></pre> | <p>Sets the starting IP address and IP Netmask for this filter to define the range of IP addresses that will be accepted by the peer when the filter is enabled. The default address is 0.0.0.0 0.0.0.0</p> <p>For Border Gateway Protocol (BGP), assign the network filter to an access-list in a route map, then assign the route map to the peer.</p> <p>Command mode: Global configuration.</p> |
| <pre>ip match-address <1-256> enable</pre> | <p>Enables the Network Filter configuration.</p> <p>Command mode: Global configuration</p> |
| <pre>no ip match-address <1-256> enable</pre> | <p>Disables the Network Filter configuration.</p> <p>Command mode: Global configuration</p> |
| <pre>no ip match-address <1-256></pre> | <p>Deletes the Network Filter configuration.</p> <p>Command mode: Global configuration</p> |
| <pre>show ip match-address [<1-256>]</pre> | <p>Displays the current the Network Filter configuration.</p> <p>Command mode: All</p> |

Routing Map Configuration

Note: The *map number* (1-32) represents the routing map you wish to configure.

Routing maps control and modify routing information.

Table 262. Routing Map Configuration Commands

| Command Syntax and Usage | |
|--------------------------------------|---|
| route-map <1-32> | Enter route map configuration mode. Command mode: Route map |
| [no] access-list <1-8> | Configures the Access List. For more information, see page 381 . Command mode: Route map |
| [no] as-path-list <1-8> | Configures the Autonomous System (AS) Filter. For more information, see page 382 . Command mode: Route map |
| [no] as-path-preference <1-65535> | Sets the AS path preference of the matched route. You can configure up to three path preferences. Command mode: Route map |
| [no] local-preference <0-4294967294> | Sets the local preference of the matched route, which affects both inbound and outbound directions. The path with the higher preference is preferred. Command mode: Route map |
| [no] metric <1-4294967294> | Sets the metric of the matched route. Command mode: Route map |
| [no] metric-type {1 2} | Assigns the type of OSPF metric. The default is type 1. <ul style="list-style-type: none"> – Type 1—External routes are calculated using both internal and external metrics. – Type 2—External routes are calculated using only the external metrics. Type 1 routes have more cost than Type 2. – none—Removes the OSPF metric. Command mode: Route map |
| precedence <1-255> | Sets the precedence of the route map. The smaller the value, the higher the precedence. Default value is 10. Command mode: Route map |

Table 262. Routing Map Configuration Commands (continued)

| Command Syntax and Usage | |
|--------------------------|---|
| [no] weight <0-65534> | Sets the weight of the route map. Command mode: Route map |
| enable | Enables the route map. Command mode: Route map |
| no enable | Disables the route map. Command mode: Route map |
| no route-map <1-32> | Deletes the route map. Command mode: Route map |
| show route-map [<1-32>] | Displays the current route configuration. Command mode: All |

IP Access List Configuration

Note: The *route map number* (1-32) and the *access list number* (1-8) represent the IP access list you wish to configure.

Table 263. IP Access List Configuration Commands

| Command Syntax and Usage |
|--|
| <pre>[no] access-list <1-8> match-address <1-256></pre> <p>Sets the network filter number. See “Network Filter Configuration” on page 378 for details.</p> <p>Command mode: Route map</p> |
| <pre>[no] access-list <1-8> metric <1-4294967294></pre> <p>Sets the metric value in the AS-External (ASE) LSA.</p> <p>Command mode: Route map</p> |
| <pre>access-list <1-8> action {permit deny}</pre> <p>Permits or denies action for the access list.</p> <p>Command mode: Route map</p> |
| <pre>access-list <1-8> enable</pre> <p>Enables the access list.</p> <p>Command mode: Route map</p> |
| <pre>no access-list <1-8> enable</pre> <p>Disables the access list.</p> <p>Command mode: Route map</p> |
| <pre>no access-list <1-8></pre> <p>Deletes the access list.</p> <p>Command mode: Route map</p> |
| <pre>show route-map <1-32> access-list <1-8></pre> <p>Displays the current Access List configuration.</p> <p>Command mode: All</p> |

Autonomous System Filter Path Configuration

Note: The *rmap number* and the *path number* represent the AS path you wish to configure.

Table 264. AS Filter Configuration Commands

| Command Syntax and Usage |
|---|
| <pre>as-path-list <1-8> as-path <1-65535></pre> <p>Sets the Autonomous System filter's path number.</p> <p>Command mode: Route map</p> |
| <pre>as-path-list <1-8> action {permit deny}</pre> <p>Permits or denies Autonomous System filter action.</p> <p>Command mode: Route map</p> |
| <pre>as-path-list <1-8> enable</pre> <p>Enables the Autonomous System filter.</p> <p>Command mode: Route map</p> |
| <pre>no as-path-list <1-8> enable</pre> <p>Disables the Autonomous System filter.</p> <p>Command mode: Route map</p> |
| <pre>no as-path-list <1-8></pre> <p>Deletes the Autonomous System filter.</p> <p>Command mode: Route map</p> |
| <pre>show route-map <1-32> as-path-list <1-8></pre> <p>Displays the current Autonomous System filter configuration.</p> <p>Command mode: All</p> |

Routing Information Protocol Configuration

RIP commands are used for configuring Routing Information Protocol parameters. This option is turned off by default.

Table 265. Routing Information Protocol Commands

| Command Syntax and Usage |
|--|
| <pre>router rip</pre> <p>Enter Router RIP configuration mode. Command mode: Global Configuration</p> |
| <pre>timers update <1-120></pre> <p>Configures the time interval for sending for RIP table updates, in seconds. The default value is 30 seconds. Command mode: Router RIP</p> |
| <pre>enable</pre> <p>Globally turns RIP on. Command mode: Router RIP</p> |
| <pre>no enable</pre> <p>Globally turns RIP off. Command mode: Router RIP</p> |
| <pre>show ip rip</pre> <p>Displays the current RIP configuration. Command mode: All</p> |

Routing Information Protocol Interface Configuration

The RIP Interface commands are used for configuring Routing Information Protocol parameters for the selected interface.

Note: Do not configure RIP version 1 parameters if your routing equipment uses RIP version 2.

Table 266. RIP Interface Commands

| Command Syntax and Usage | |
|--|---|
| <code>ip rip version {1 2 both}</code> | Configures the RIP version used by this interface. The default value is version 2. Command mode: Interface IP |
| <code>[no] ip rip supply</code> | When enabled, the switch supplies routes to other routers. The default value is enabled. Command mode: Interface IP |
| <code>[no] ip rip listen</code> | When enabled, the switch learns routes from other routers. The default value is enabled. Command mode: Interface IP |
| <code>[no] ip rip poison</code> | When enabled, the switch uses split horizon with poisoned reverse. When disabled, the switch uses only split horizon. The default value is disabled. Command mode: Interface IP |
| <code>[no] ip rip split-horizon</code> | Enables or disables split horizon. The default value is enabled. Command mode: Interface IP |
| <code>[no] ip rip triggered</code> | Enables or disables Triggered Updates. Triggered Updates are used to speed convergence. When enabled, Triggered Updates force a router to send update messages immediately, even if it is not yet time for the update message. The default value is enabled. Command mode: Interface IP |
| <code>[no] ip rip multicast-updates</code> | Enables or disables multicast updates of the routing table (using address 224.0.0.9). The default value is enabled. Command mode: Interface IP |
| <code>[no] ip rip default-action {listen supply both}</code> | When enabled, the switch accepts RIP default routes from other routers, but gives them lower priority than configured default gateways. When disabled, the switch rejects RIP default routes. The default value is none. Command mode: Interface IP |

Table 266. RIP Interface Commands (continued)

| Command Syntax and Usage | |
|---|---|
| [no] ip rip metric [<i><1-15></i>] | Configures the route metric, which indicates the relative distance to the destination. The default value is 1. Command mode: Interface IP |
| [no] ip rip authentication type [<i><password></i>] | Configures the authentication type. The default is none. Command mode: Interface IP |
| [no] ip rip authentication key <i><password></i> | Configures the authentication key password. Command mode: Interface IP |
| ip rip enable | Enables this RIP interface. Command mode: Interface IP |
| no ip rip enable | Disables this RIP interface. Command mode: Interface IP |
| show interface ip <i><interface number></i> rip | Displays the current RIP configuration. Command mode: All |

RIP Route Redistribution Configuration

The following table describes the RIP Route Redistribution commands.

Table 267. RIP Redistribution Commands

| Command Syntax and Usage |
|--|
| <pre>redistribute {fixed static ospf eospf ebgp ibgp} <1-32></pre> <p>Adds selected routing maps to the RIP route redistribution list. To add specific route maps, enter routing map numbers, separated by a comma (,). To add all 32 route maps, type <code>all</code>.</p> <p>The routes of the redistribution protocol matched by the route maps in the route redistribution list will be redistributed.</p> <p>Command mode: Router RIP</p> |
| <pre>no redistribute {fixed static ospf eospf ebgp ibgp} <1-32></pre> <p>Removes the route map from the RIP route redistribution list.</p> <p>To remove specific route maps, enter routing map numbers, separated by a comma (,). To remove all 32 route maps, type <code>all</code>.</p> <p>Command mode: Router RIP</p> |
| <pre>redistribute {fixed static ospf eospf ebgp ibgp} export <1-15></pre> <p>Exports the routes of this protocol in which the metric and metric type are specified. To remove a previous configuration and stop exporting the routes of the protocol, enter <code>none</code>.</p> <p>Command mode: Router RIP</p> |
| <pre>show ip rip redistribute</pre> <p>Displays the current RIP route redistribute configuration.</p> <p>Command mode: All</p> |

Open Shortest Path First Configuration

Table 268. OSPF Configuration Commands

| Command Syntax and Usage | |
|--|--|
| router ospf | Enter Router OSPF configuration mode. Command mode: Global configuration |
| area-range <I-16> | Configures summary routes for up to 16 IP addresses. See page 391 to view command options. Command mode: Router OSPF |
| ip ospf <interface number> | Configures the OSPF interface. See page 392 to view command options. Command mode: Interface IP |
| area-virtual-link <I-3> | Configures the Virtual Links used to configure OSPF for a Virtual Link. See page 394 to view command options. Command mode: Router OSPF |
| message-digest-key <I-255> md5-key <text string> | Assigns a string to MD5 authentication key. Command mode: Router OSPF |
| host <I-128> | Configures OSPF for the host routes. Up to 128 host routes can be configured. Host routes are used for advertising network device IP addresses to external networks to perform server load balancing within OSPF. It also makes Area Border Route (ABR) load sharing and ABR failover possible. See page 395 to view command options. Command mode: Router OSPF |
| lsdb-limit <LSDB limit (0-2048, 0 for no limit)> | Sets the link state database limit. Command mode: Router OSPF |
| [no] default-information <I-1677214> {<AS external metric type (1-2)>} | Sets one default route among multiple choices in an area. Use none for no default. Command mode: Router OSPF |
| enable | Enables OSPF on the EN4093 and EN4093R. Command mode: Router OSPF |

Table 268. OSPF Configuration Commands (continued)

| Command Syntax and Usage |
|--|
| <code>no enable</code> Disables OSPF on the EN4093 and EN4093R. Command mode: Router OSPF |
| <code>show ip ospf</code> Displays the current OSPF configuration settings. Command mode: All |

Area Index Configuration

Table 269. Area Index Configuration Commands

| Command Syntax and Usage | |
|---|--|
| <pre>area <0-2> area-id <IP address></pre> | <p>Defines the IP address of the OSPF area number.</p> <p>Command mode: Router OSPF</p> |
| <pre>area <0-2> type {transit stub nssa}</pre> | <p>Defines the type of area. For example, when a virtual link has to be established with the backbone, the area type must be defined as transit.</p> <p>Transit area: allows area summary information to be exchanged between routing devices. Any area that is not a stub area or NSSA is considered to be transit area.</p> <p>Stub area: is an area where external routing information is not distributed. Typically, a stub area is connected to only one other area.</p> <p>NSSA: Not-So-Stubby Area (NSSA) is similar to stub area with additional capabilities. For example, routes originating from within the NSSA can be propagated to adjacent transit and backbone areas.</p> <p>Command mode: Router OSPF</p> |
| <pre>area <0-2> stub-metric <1-65535></pre> | <p>Configures a stub area to send a numeric metric value. All routes received via that stub area carry the configured metric to potentially influencing routing decisions.</p> <p>Metric value assigns the priority for choosing the switch for default route. Metric type determines the method for influencing routing decisions for external routes.</p> <p>Command mode: Router OSPF</p> |
| <pre>[no] area <0-2> authentication-type {password md5}</pre> | <p>None: No authentication required.</p> <p>Password: Authenticates simple passwords so that only trusted routing devices can participate.</p> <p>MD5: This parameter is used when MD5 cryptographic authentication is required.</p> <p>Command mode: Router OSPF</p> |
| <pre>area <0-2> spf-interval <1-255></pre> | <p>Configures the minimum time interval, in seconds, between two successive SPF (shortest path first) calculations of the shortest path tree using the Dijkstra's algorithm. The default value is 10 seconds.</p> <p>Command mode: Router OSPF</p> |
| <pre>area <0-2> enable</pre> | <p>Enables the OSPF area.</p> <p>Command mode: Router OSPF</p> |

Table 269. Area Index Configuration Commands (continued)

| Command Syntax and Usage |
|--|
| <pre>no area <0-2> enable</pre> <p>Disables the OSPF area.</p> <p>Command mode: Router OSPF</p> |
| <pre>no area <0-2></pre> <p>Deletes the OSPF area.</p> <p>Command mode: Router OSPF</p> |
| <pre>show ip ospf area <0-2></pre> <p>Displays the current OSPF configuration.</p> <p>Command mode: All</p> |

OSPF Summary Range Configuration

Table 270. OSPF Summary Range Configuration Commands

| Command Syntax and Usage | |
|--|---|
| <pre>area-range <1-16> address <IP address> <IP netmask></pre> | <p>Displays the base IP address or the IP address mask for the range. Command mode: Router OSPF</p> |
| <pre>area-range <1-16> area <0-2></pre> | <p>Displays the area index used by the EN4093 and EN4093R. Command mode: Router OSPF</p> |
| <pre>[no] area-range <1-16> hide</pre> | <p>Hides the OSPF summary range. Command mode: Router OSPF</p> |
| <pre>area-range <1-16> enable</pre> | <p>Enables the OSPF summary range. Command mode: Router OSPF</p> |
| <pre>no area-range <1-16> enable</pre> | <p>Disables the OSPF summary range. Command mode: Router OSPF</p> |
| <pre>no area-range <1-16></pre> | <p>Deletes the OSPF summary range. Command mode: Router OSPF</p> |
| <pre>show ip ospf area-range <1-16></pre> | <p>Displays the current OSPF summary range. Command mode: Router OSPF</p> |

OSPF Interface Configuration

Table 271. OSPF Interface Configuration Commands

| Command Syntax and Usage | |
|--|--|
| <pre>ip ospf area <0-2></pre> | <p>Configures the OSPF area index.</p> <p>Command mode: Interface IP</p> |
| <pre>ip ospf priority <0-255></pre> | <p>Configures the priority value for the EN4093 and EN4093R's OSPF interfaces. A priority value of 255 is the highest and 1 is the lowest. A priority value of 0 specifies that the interface cannot be used as Designated Router (DR) or Backup Designated Router (BDR).</p> <p>Command mode: Interface IP</p> |
| <pre>ip ospf cost <1-65535></pre> | <p>Configures cost set for the selected path—preferred or backup. Usually the cost is inversely proportional to the bandwidth of the interface. Low cost indicates high bandwidth.</p> <p>Command mode: Interface IP</p> |
| <pre>ip ospf hello-interval <1-65535></pre> <pre>ip ospf hello-interval <50-65535ms></pre> | <p>Configures the interval, in seconds or milliseconds, between the hello packets for the interfaces.</p> <p>Command mode: Interface IP</p> |
| <pre>ip ospf dead-interval <1-65535></pre> <pre>ip ospf dead-interval <1000-65535ms></pre> | <p>Configures the health parameters of a hello packet, in seconds or milliseconds, before declaring a silent router to be down.</p> <p>Command mode: Interface IP</p> |
| <pre>ip ospf transit-delay <1-3600></pre> | <p>Configures the transit delay in seconds.</p> <p>Command mode: Interface IP</p> |
| <pre>ip ospf retransmit-interval <1-3600></pre> | <p>Configures the retransmit interval in seconds.</p> <p>Command mode: Interface IP</p> |
| <pre>[no] ip ospf key <key string></pre> | <p>Sets the authentication key to clear the password.</p> <p>Command mode: Interface IP</p> |
| <pre>[no] ip ospf message-digest-key <1-255></pre> | <p>Assigns an MD5 key to the interface.</p> <p>Command mode: Interface IP</p> |

Table 271. OSPF Interface Configuration Commands (continued)

| Command Syntax and Usage | |
|---|--|
| [no] ip ospf passive-interface | <p>Sets the interface as passive. On a passive interface, you can disable OSPF protocol exchanges, but the router advertises the interface in its LSAs so that IP connectivity to the attached network segment will be established.</p> <p>Command mode: Interface IP</p> |
| [no] ip ospf point-to-point | <p>Sets the interface as point-to-point.</p> <p>Command mode: Interface IP</p> |
| ip ospf enable | <p>Enables OSPF interface.</p> <p>Command mode: Interface IP</p> |
| no ip ospf enable | <p>Disables OSPF interface.</p> <p>Command mode: Interface IP</p> |
| no ip ospf | <p>Deletes the OSPF interface.</p> <p>Command mode: Interface IP</p> |
| show interface ip <interface number> ospf | <p>Displays the current settings for OSPF interface.</p> <p>Command mode: All</p> |

OSPF Virtual Link Configuration

Table 272. OSPF Virtual Link Configuration Commands

| Command Syntax and Usage |
|--|
| <pre>area-virtual-link <1-3> area <0-2></pre> <p>Configures the OSPF area index for the virtual link.</p> <p>Command mode: Router OSPF</p> |
| <pre>area-virtual-link <1-3> hello-interval <1-65535></pre> <pre>area-virtual-link <1-3> hello-interval <50-65535ms></pre> <p>Configures the authentication parameters of a hello packet, in seconds or milliseconds. The default value is 10 seconds.</p> <p>Command mode: Router OSPF</p> |
| <pre>area-virtual-link <1-3> dead-interval <1-65535></pre> <pre>area-virtual-link <1-3> dead-interval <1000-65535ms></pre> <p>Configures the health parameters of a hello packet, in seconds or milliseconds. The default value is 40 seconds.</p> <p>Command mode: Router OSPF</p> |
| <pre>area-virtual-link <1-3> transit-delay <1-3600></pre> <p>Configures the delay in transit, in seconds. The default value is one second.</p> <p>Command mode: Router OSPF</p> |
| <pre>area-virtual-link <1-3> retransmit-interval <1-3600></pre> <p>Configures the retransmit interval, in seconds. The default value is five seconds.</p> <p>Command mode: Router OSPF</p> |
| <pre>area-virtual-link <1-3> neighbor-router <IP address></pre> <p>Configures the router ID of the virtual neighbor. The default value is 0.0.0.0.</p> <p>Command mode: Router OSPF</p> |
| <pre>[no] area-virtual-link <1-3> key <password></pre> <p>Configures the password (up to eight characters) for each virtual link. The default setting is none.</p> <p>Command mode: Router OSPF</p> |
| <pre>area-virtual-link <1-3> message-digest-key <1-255></pre> <p>Sets MD5 key ID for each virtual link. The default setting is none.</p> <p>Command mode: Router OSPF</p> |
| <pre>area-virtual-link <1-3> enable</pre> <p>Enables OSPF virtual link.</p> <p>Command mode: Router OSPF</p> |

Table 272. OSPF Virtual Link Configuration Commands (continued)

| Command Syntax and Usage |
|--|
| <pre>no area-virtual-link <1-3> enable</pre> <p>Disables OSPF virtual link. Command mode: Router OSPF</p> |
| <pre>no area-virtual-link <1-3></pre> <p>Deletes OSPF virtual link. Command mode: Router OSPF</p> |
| <pre>show ip ospf area-virtual-link <1-3></pre> <p>Displays the current OSPF virtual link settings. Command mode: All</p> |

OSPF Host Entry Configuration

Table 273. OSPF Host Entry Configuration Commands

| Command Syntax and Usage |
|---|
| <pre>host <1-128> address <IP address></pre> <p>Configures the base IP address for the host entry. Command mode: Router OSPF</p> |
| <pre>host <1-128> area <0-2></pre> <p>Configures the area index of the host. Command mode: Router OSPF</p> |
| <pre>host <1-128> cost <1-65535></pre> <p>Configures the cost value of the host. Command mode: Router OSPF</p> |
| <pre>host <1-128> enable</pre> <p>Enables OSPF host entry. Command mode: Router OSPF</p> |
| <pre>no host <1-128> enable</pre> <p>Disables OSPF host entry. Command mode: Router OSPF</p> |
| <pre>no host <1-128></pre> <p>Deletes OSPF host entry. Command mode: Router OSPF</p> |
| <pre>show ip ospf host <1-128></pre> <p>Displays the current OSPF host entries. Command mode: All</p> |

OSPF Route Redistribution Configuration.

Table 274. OSPF Route Redistribution Configuration Commands

| Command Syntax and Usage |
|--|
| <pre>redistribute {fixed static rip ebgp ibgp} <rmap ID (1-32)></pre> <p>Adds selected routing map to the rmap list.</p> <p>This option adds a route map to the route redistribution list. The routes of the redistribution protocol matched by the route maps in the route redistribution list will be redistributed.</p> <p>Command mode: Router OSPF</p> |
| <pre>no redistribute {fixed static rip ebgp ibgp} <rmap ID (1-32)></pre> <p>Removes the route map from the route redistribution list.</p> <p>Removes routing maps from the rmap list.</p> <p>Command mode: Router OSPF</p> |
| <pre>[no] redistribute {fixed static rip ebgp ibgp} export metric <1-16777214> metric-type {type1 type2}</pre> <p>Exports the routes of this protocol as external OSPF AS-external LSAs in which the metric and metric type are specified. To remove a previous configuration and stop exporting the routes of the protocol, enter none.</p> <p>Command mode: Router OSPF</p> |
| <pre>show ip ospf redistribute</pre> <p>Displays the current route map settings.</p> <p>Command mode: All</p> |

OSPF MD5 Key Configuration

Table 275. OSPF MD5 Key Commands

| Command Syntax and Usage |
|--|
| <pre>message-digest-key <1-255> md5-key <1-16 characters></pre> <p>Sets the authentication key for this OSPF packet.</p> <p>Command mode: Router OSPF</p> |
| <pre>no message-digest-key <1-255></pre> <p>Deletes the authentication key for this OSPF packet.</p> <p>Command mode: Router OSPF</p> |
| <pre>show ip ospf message-digest-key <1-255></pre> <p>Displays the current MD5 key configuration.</p> <p>Command mode: All</p> |

Border Gateway Protocol Configuration

Border Gateway Protocol (BGP) is an Internet protocol that enables routers on a network to share routing information with each other and advertise information about the segments of the IP address space they can access within their network with routers on external networks. BGP allows you to decide what is the “best” route for a packet to take from your network to a destination on another network, rather than simply setting a default route from your border router(s) to your upstream provider(s). You can configure BGP either within an autonomous system or between different autonomous systems. When run within an autonomous system, it’s called internal BGP (iBGP). When run between different autonomous systems, it’s called external BGP (eBGP). BGP is defined in RFC 1771.

BGP commands enable you to configure the switch to receive routes and to advertise static routes, fixed routes and virtual server IP addresses with other internal and external routers. In the current Networking OS implementation, the EN4093 and EN4093R 10Gb Scalable Switch does not advertise BGP routes that are learned from one iBGP *speaker* to another iBGP *speaker*.

BGP is turned off by default.

Note: Fixed routes are subnet routes. There is one fixed route per IP interface.

Table 276. Border Gateway Protocol Commands

| Command Syntax and Usage | |
|--|---|
| <code>router bgp</code> | Enter Router BGP configuration mode. Command mode: Global configuration |
| <code>neighbor <I-12></code> | Configures each BGP <i>peer</i> . Each border router, within an autonomous system, exchanges routing information with routers on other external networks. To view command options, see page 399 . Command mode: Router BGP |
| <code>as <0-65535></code> | Set Autonomous System number. Command mode: Router BGP |
| <code>[no] asn4comp</code> | Enables or disables ASN4 to ASN2 compatibility. Command mode: Router BGP |
| <code>cluster-id <IP address></code> | Specifies the router’s Cluster ID used when operating as a route reflector. Route reflectors that are part of the same cluster (assigned to the same group of clients) must use identical Cluster IDs. Command mode: Router BGP |
| <code>no cluster-id</code> | Removes the router’s Cluster ID. Command mode: Router BGP |

Table 276. Border Gateway Protocol Commands (continued)

| Command Syntax and Usage | |
|----------------------------------|---|
| [no] client-to-client reflection | <p>Enables or disables client-to-client IBGP route reflection when operating as a route reflector. The default state is enabled.</p> <p>Command mode: Router BGP</p> |
| local-preference <0-4294967294> | <p>Sets the local preference. The path with the higher value is preferred.</p> <p>When multiple peers advertise the same route, use the route with the shortest AS path as the preferred route if you are using eBGP, or use the local preference if you are using iBGP.</p> <p>Command mode: Router BGP</p> |
| enable | <p>Globally turns BGP on.</p> <p>Command mode: Router BGP</p> |
| no enable | <p>Globally turns BGP off.</p> <p>Command mode: Router BGP</p> |
| show ip bgp | <p>Displays the current BGP configuration.</p> <p>Command mode: All</p> |

BGP Peer Configuration

These commands are used to configure BGP peers, which are border routers that exchange routing information with routers on internal and external networks. The peer option is disabled by default.

Table 277. BGP Peer Configuration Commands

| Command Syntax and Usage |
|--|
| <pre>neighbor <I-12> remote-address <IP address></pre> <p>Defines the IP address for the specified peer (border router), using dotted decimal notation. The default address is 0.0.0.0.</p> <p>Command mode: Router BGP</p> |
| <pre>neighbor <I-12> remote-as <I-65535></pre> <p>Sets the remote autonomous system number for the specified peer.</p> <p>Command mode: Router BGP</p> |
| <pre>[no] neighbor <I-12> route-reflector-client</pre> <p>Enables or disables the peer as a route reflector client. Configuring route reflector clients, implicitly sets up the local router as a route reflector.</p> <p>Command mode: Router BGP</p> |
| <pre>neighbor <I-12> update-source {<interface number> loopback <I-5>}</pre> <p>Sets the source interface number for this peer.</p> <p>Command mode: Router BGP</p> |
| <pre>neighbor <I-12> timers hold-time <0, 3-65535></pre> <p>Sets the period of time, in seconds, that will elapse before the peer session is torn down because the switch hasn't received a "keep alive" message from the peer. The default value is 180 seconds.</p> <p>Command mode: Router BGP</p> |
| <pre>neighbor <I-12> timers keep-alive <0, 1-21845></pre> <p>Sets the keep-alive time for the specified peer, in seconds. The default value is 60 seconds.</p> <p>Command mode: Router BGP</p> |
| <pre>neighbor <I-12> advertisement-interval <I-65535></pre> <p>Sets time, in seconds, between advertisements. The default value is 60 seconds.</p> <p>Command mode: Router BGP</p> |
| <pre>neighbor <I-12> retry-interval <I-65535></pre> <p>Sets connection retry interval, in seconds. The default value is 120 seconds.</p> <p>Command mode: Router BGP</p> |
| <pre>neighbor <I-12> route-origination-interval <I-65535></pre> <p>Sets the minimum time between route originations, in seconds. The default value is 15 seconds.</p> <p>Command mode: Router BGP</p> |

Table 277. BGP Peer Configuration Commands (continued)

| Command Syntax and Usage | |
|---|--|
| neighbor <I-12> time-to-live <I-255> | <p>Time-to-live (TTL) is a value in an IP packet that tells a network router whether or not the packet has been in the network too long and should be discarded. TTL specifies a certain time span in seconds that, when exhausted, would cause the packet to be discarded. The TTL is determined by the number of router hops the packet is allowed before it must be discarded.</p> <p>This command specifies the number of router hops that the IP packet can make. This value is used to restrict the number of “hops” the advertisement makes. It is also used to support multi-hops, which allow BGP peers to talk across a routed network. The default number is set at 1.</p> <p>Note: The TTL value is significant only to eBGP peers, for iBGP peers the TTL value in the IP packets is always 255 (regardless of the configured value).</p> <p>Command mode: Router BGP</p> |
| neighbor <I-12> route-map in <I-32> | <p>Adds route map into in-route map list.</p> <p>Command mode: Router BGP</p> |
| neighbor <I-12> route-map out <I-32> | <p>Adds route map into out-route map list.</p> <p>Command mode: Router BGP</p> |
| no neighbor <I-12> route-map in <I-32> | <p>Removes route map from in-route map list.</p> <p>Command mode: Router BGP</p> |
| no neighbor <I-12> route-map out <I-32> | <p>Removes route map from out-route map list.</p> <p>Command mode: Router BGP</p> |
| no neighbor <I-12> shutdown | <p>Enables this peer configuration.</p> <p>Command mode: Router BGP</p> |
| neighbor <I-12> shutdown | <p>Disables this peer configuration.</p> <p>Command mode: Router BGP</p> |
| no neighbor <I-12> | <p>Deletes this peer configuration.</p> <p>Command mode: Router BGP</p> |

Table 277. BGP Peer Configuration Commands (continued)

| Command Syntax and Usage |
|--|
| <pre>[no] neighbor <I-12> password <I-16 characters></pre> <p>Configures the BGP peer password.</p> <p>Command mode: Router BGP</p> |
| <pre>show ip bgp neighbor [<I-12>]</pre> <p>Displays the current BGP peer configuration.</p> <p>Command mode: All</p> |

BGP Redistribution Configuration

Table 278. BGP Redistribution Configuration Commands

| Command Syntax and Usage |
|---|
| <pre>[no] neighbor <1-12> redistribute default-metric <1-4294967294></pre> <p>Sets default metric of advertised routes.</p> <p>Command mode: Router BGP</p> |
| <pre>[no] neighbor <1-12> redistribute default-action {import originate redistribute}</pre> <p>Sets default route action.</p> <p>Defaults routes can be configured as import, originate, redistribute, or none.</p> <p>None: No routes are configured</p> <p>Import: Import these routes.</p> <p>Originate: The switch sends a default route to peers if it does not have any default routes in its routing table.</p> <p>Redistribute: Default routes are either configured through default gateway or learned through other protocols and redistributed to peer. If the routes are learned from default gateway configuration, you have to enable static routes since the routes from default gateway are static routes. Similarly, if the routes are learned from a certain routing protocol, you have to enable that protocol.</p> <p>Command mode: Router BGP</p> |
| <pre>[no] neighbor <1-12> redistribute rip</pre> <p>Enables or disables advertising RIP routes.</p> <p>Command mode: Router BGP</p> |
| <pre>[no] neighbor <1-12> redistribute ospf</pre> <p>Enables or disables advertising OSPF routes.</p> <p>Command mode: Router BGP</p> |
| <pre>[no] neighbor <1-12> redistribute fixed</pre> <p>Enables or disables advertising fixed routes.</p> <p>Command mode: Router BGP</p> |
| <pre>[no] neighbor <1-12> redistribute static</pre> <p>Enables or disables advertising static routes.</p> <p>Command mode: Router BGP</p> |
| <pre>show ip bgp neighbor <1-12> redistribute</pre> <p>Displays current redistribution configuration.</p> <p>Command mode: All</p> |

BGP Aggregation Configuration

These commands enable you to configure BGP aggregation to specify the routes/range of IP destinations a peer router accepts from other peers. All matched routes are aggregated to one route, to reduce the size of the routing table. By default, the first aggregation number is enabled and the rest are disabled.

Table 279. BGP Aggregation Configuration Commands

| Command Syntax and Usage | |
|---|---|
| <pre>aggregate-address <1-16> <IP address> <IP netmask></pre> | <p>Defines the starting subnet IP address for this aggregation, using dotted decimal notation. The default address is 0.0.0.0.</p> <p>Command mode: Router BGP</p> |
| <pre>aggregate-address <1-16> enable</pre> | <p>Enables this BGP aggregation.</p> <p>Command mode: Router BGP</p> |
| <pre>no aggregate-address <1-16> enable</pre> | <p>Disables this BGP aggregation.</p> <p>Command mode: Router BGP</p> |
| <pre>no aggregate-address <1-16></pre> | <p>Deletes this BGP aggregation.</p> <p>Command mode: Router BGP</p> |
| <pre>show ip bgp aggregate-address [<1-16>]</pre> | <p>Displays the current BGP aggregation configuration.</p> <p>Command mode: All</p> |

Multicast Listener Discovery Protocol Configuration

[Table 280](#) describes the commands used to configure MLD parameters..

Table 280. MLD Protocol Configuration Commands

| Command Syntax and Usage |
|--|
| <pre>ipv6 mld</pre> <p>Enter MLD global configuration mode. Command mode: Global configuration</p> |
| <pre>default</pre> <p>Resets MLD parameters to their default values. Command mode: MLD Configuration</p> |
| <pre>enable</pre> <p>Globally turns MLD on. Command mode: MLD Configuration</p> |
| <pre>no enable</pre> <p>Globally turns MLD off. Command mode: MLD Configuration</p> |
| <pre>exit</pre> <p>Exit from MLD configuration mode. Command mode: MLD Configuration</p> |
| <pre>show ipv6 mld</pre> <p>Displays the current MLD configuration parameters. Command mode: All</p> |

MLD Interface Configuration

[Table 281](#) describes the commands used to configure MLD parameters for an interface.

Table 281. MLD Interface Configuration Commands

| Command Syntax and Usage |
|--|
| <pre>ipv6 mld default</pre> <p>Resets MLD parameters for the selected interface to their default values. Command mode: Interface IP</p> |
| <pre>ipv6 mld dmrtr enable disable</pre> <p>Enables or disables dynamic Mrouter learning on the interface. The default setting is disabled. Command mode: Interface IP</p> |

Table 281. MLD Interface Configuration Commands (continued)

| Command Syntax and Usage | |
|---|---|
| <pre>ipv6 mld enable</pre> | <p>Enables this MLD interface.</p> <p>Command mode: Interface IP</p> |
| <pre>no ipv6 mld enable</pre> | <p>Disables this MLD interface.</p> <p>Command mode: Interface IP</p> |
| <pre>ipv6 mld llistnr <1-32></pre> | <p>Configures the Last Listener query interval. The default value is 1 second.</p> <p>Command mode: Interface IP</p> |
| <pre>ipv6 mld qinterval <2-65535></pre> | <p>Configures the interval for MLD Query Reports. The default value is 125 seconds.</p> <p>Command mode: Interface IP</p> |
| <pre>ipv6 mld qri <1000-65535></pre> | <p>Configures the interval for MLD Query Response Reports. The default value is 10,000 milliseconds.</p> <p>Command mode: Interface IP</p> |
| <pre>ipv6 mld robust <2-10></pre> | <p>Configures the MLD Robustness variable, which allows you to tune the switch for expected packet loss on the subnet. If the subnet is expected to be lossy (high rate of packet loss), increase the value. The default value is 2.</p> <p>Command mode: Interface IP</p> |
| <pre>ipv6 mld version <1-2></pre> | <p>Defines the MLD protocol version number.</p> <p>Command mode: Interface IP</p> |
| <pre>show ipv6 mld interface <interface number></pre> | <p>Displays the current MLD interface configuration.</p> <p>Command mode: All</p> |

IGMP Configuration

[Table 282](#) describes the commands used to configure basic IGMP parameters.

Table 282. IGMP Configuration Commands

| Command Syntax and Usage |
|--|
| <pre>[no] ip igmp aggregate</pre> <p>Enables or disables IGMP Membership Report aggregation. Command mode: Global configuration</p> |
| <pre>ip igmp enable</pre> <p>Globally turns IGMP on. Command mode: Global configuration</p> |
| <pre>no ip igmp enable</pre> <p>Globally turns IGMP off. Command mode: Global configuration</p> |
| <pre>show ip igmp</pre> <p>Displays the current IGMP configuration parameters. Command mode: All</p> |

The following sections describe the IGMP configuration options.

- [“IGMP Snooping Configuration” on page 407](#)
- [“IGMPv3 Configuration” on page 408](#)
- [“IGMP Relay Configuration” on page 409](#)
- [“IGMP Relay Multicast Router Configuration” on page 410](#)
- [“IGMP Static Multicast Router Configuration” on page 411](#)
- [“IGMP Filtering Configuration” on page 412](#)
- [“IGMP Advanced Configuration” on page 415](#)
- [“IGMP Querier Configuration” on page 415](#)

IGMP Snooping Configuration

IGMP Snooping allows the switch to forward multicast traffic only to those ports that request it. IGMP Snooping prevents multicast traffic from being flooded to all ports. The switch learns which server hosts are interested in receiving multicast traffic, and forwards it only to ports connected to those servers.

Table 283 describes the commands used to configure IGMP Snooping.

Table 283. IGMP Snooping Configuration Commands

| Command Syntax and Usage | |
|--|--|
| <code>ip igmp snoop mrouter-timeout <1-600></code> | Configures the timeout value for IGMP Membership Queries (mrouter). Once the timeout value is reached, the switch removes the multicast router from its IGMP table, if the proper conditions are met. The range is from 1 to 600 seconds. The default is 255 seconds. Command mode: Global configuration |
| <code>ip igmp snoop source-ip <IP address></code> | Configures the source IP address used as a proxy for IGMP Group Specific Queries. Command mode: Global configuration |
| <code>ip igmp snoop vlan <VLAN number></code> | Adds the selected VLAN(s) to IGMP Snooping. Command mode: Global configuration |
| <code>no ip igmp snoop vlan <VLAN number></code> | Removes the selected VLAN(s) from IGMP Snooping. Command mode: Global configuration |
| <code>no ip igmp snoop vlan all</code> | Removes all VLANs from IGMP Snooping. Command mode: Global configuration |
| <code>ip igmp snoop enable</code> | Enables IGMP Snooping. Command mode: Global configuration |
| <code>no ip igmp snoop enable</code> | Disables IGMP Snooping. Command mode: Global configuration |
| <code>show ip igmp snoop</code> | Displays the current IGMP Snooping parameters. Command mode: All |

IGMPv3 Configuration

Table 284 describes the commands used to configure IGMP version 3.

Table 284. IGMP version 3 Configuration Commands

| Command Syntax and Usage | |
|--|--|
| <pre>ip igmp snoop igmpv3 sources <1-64></pre> | <p>Configures the maximum number of IGMP multicast sources to snoop from within the group record. Use this command to limit the number of IGMP sources to provide more refined control. The default value is 8.</p> <p>Command mode: Global configuration</p> |
| <pre>[no] ip igmp snoop igmpv3 v1v2</pre> | <p>Enables or disables snooping on IGMP version 1 and version 2 reports. When disabled, the switch drops IGMPv1 and IGMPv2 reports. The default value is enabled.</p> <p>Command mode: Global configuration</p> |
| <pre>[no] ip igmp snoop igmpv3 exclude</pre> | <p>Enables or disables snooping on IGMPv3 Exclude Reports. When disabled, the switch ignores Exclude Reports. The default value is enabled.</p> <p>Command mode: Global configuration</p> |
| <pre>ip igmp snoop igmpv3 enable</pre> | <p>Enables IGMP version 3. The default value is disabled.</p> <p>Command mode: Global configuration</p> |
| <pre>no ip igmp snoop igmpv3 enable</pre> | <p>Disables IGMP version 3.</p> <p>Command mode: Global configuration</p> |
| <pre>show ip igmp snoop igmpv3</pre> | <p>Displays the current IGMP v3 Snooping configuration.</p> <p>Command mode: All</p> |

IGMP Relay Configuration

When you configure IGMP Relay, also configure the IGMP Relay multicast routers.

[Table 285](#) describes the commands used to configure IGMP Relay.

Table 285. IGMP Relay Configuration Commands

| Command Syntax and Usage | |
|--|---|
| <code>ip igmp relay vlan <VLAN number></code> | Adds the VLAN to the list of IGMP Relay VLANs. Command mode: Global configuration |
| <code>no ip igmp relay vlan <VLAN number></code> | Removes the VLAN from the list of IGMP Relay VLANs. Command mode: Global configuration |
| <code>ip igmp relay report <0-150></code> | Configures the interval between unsolicited Join reports sent by the switch, in seconds. The default value is 10. Command mode: Global configuration |
| <code>ip igmp relay enable</code> | Enables IGMP Relay. Command mode: Global configuration |
| <code>no ip igmp relay enable</code> | Disables IGMP Relay. Command mode: Global configuration |
| <code>show ip igmp relay</code> | Displays the current IGMP Relay configuration. Command mode: All |

IGMP Relay Multicast Router Configuration

Table 286 describes the commands used to configure multicast routers for IGMP Relay.

Table 286. IGMP Relay Mrouter Configuration Commands

| Command Syntax and Usage | |
|---|--|
| <code>ip igmp relay mrouter <I-2> address <IP address></code> | Configures the IP address of the IGMP multicast router used for IGMP Relay. Command mode: Global configuration |
| <code>ip igmp relay mrouter <I-2> interval <I-60></code> | Configures the time interval between ping attempts to the upstream Mroouters, in seconds. The default value is 2. Command mode: Global configuration |
| <code>ip igmp relay mrouter <I-2> retry <I-120></code> | Configures the number of failed ping attempts required before the switch declares this Mrouter is down. The default value is 4. Command mode: Global configuration |
| <code>ip igmp relay mrouter <I-2> attempt <I-128></code> | Configures the number of successful ping attempts required before the switch declares this Mrouter is up. The default value is 5. Command mode: Global configuration |
| <code>ip igmp relay mrouter <I-2> version <I-2></code> | Configures the IGMP version (1 or 2) of the multicast router. Command mode: Global configuration |
| <code>ip igmp relay mrouter <I-2> enable</code> | Enables the multicast router. Command mode: Global configuration |
| <code>no ip igmp relay mrouter <I-2> enable</code> | Disables the multicast router. Command mode: Global configuration |
| <code>no ip igmp relay mrouter <I-2></code> | Deletes the multicast router from IGMP Relay. Command mode: Global configuration |

IGMP Static Multicast Router Configuration

Table 287 describes the commands used to configure a static multicast router.

Note: When static Mrouters are used, the switch continues learning dynamic Mrouters via IGMP snooping. However, dynamic Mrouters may not replace static Mrouters. If a dynamic Mrouter has the same port and VLAN combination as a static Mrouter, the dynamic Mrouter is not learned.

Table 287. IGMP Static Multicast Router Configuration Commands

| Command Syntax and Usage | |
|--|---|
| <pre>ip igmp mrouter <port alias or number> <VLAN number> <version (1-3)></pre> | <p>Selects a port/VLAN combination on which the static multicast router is connected, and configures the IGMP version (1, 2 or 3) of the multicast router.</p> <p>Command mode: Global configuration</p> |
| <pre>no ip igmp mrouter <port alias or number> <VLAN number> <version (1-3)></pre> | <p>Removes a static multicast router from the selected port/VLAN combination.</p> <p>Command mode: Global configuration</p> |
| <pre>no ip igmp mrouter all</pre> | <p>Removes all static multicast routers.</p> <p>Command mode: Global configuration</p> |
| <pre>clear ip igmp mrouter</pre> | <p>Clears the multicast router port table.</p> <p>Command mode: Global configuration</p> |
| <pre>show ip igmp mrouter</pre> | <p>Displays the current IGMP Static Multicast Router parameters.</p> <p>Command mode: All</p> |

IGMP Filtering Configuration

[Table 288](#) describes the commands used to configure an IGMP filter.

Table 288. IGMP Filtering Configuration Commands

| Command Syntax and Usage |
|--|
| <pre>ip igmp profile <1-16></pre> <p>Configures the IGMP filter. To view command options, see page 413.</p> <p>Command mode: Global configuration</p> |
| <pre>ip igmp filtering</pre> <p>Enables IGMP filtering globally.</p> <p>Command mode: Global configuration</p> |
| <pre>no ip igmp filtering</pre> <p>Disables IGMP filtering globally.</p> <p>Command mode: Global configuration</p> |
| <pre>show ip igmp filtering</pre> <p>Displays the current IGMP Filtering parameters.</p> <p>Command mode: All</p> |

IGMP Filter Definition

Table 289 describes the commands used to define an IGMP filter.

Table 289. IGMP Filter Definition Commands

| Command Syntax and Usage |
|---|
| <pre>ip igmp profile <1-16> range <IP address 1> <IP address 2></pre> <p>Configures the range of IP multicast addresses for this filter. Command mode: Global configuration</p> |
| <pre>ip igmp profile <1-16> action {allow deny}</pre> <p>Allows or denies multicast traffic for the IP multicast addresses specified. The default action is deny. Command mode: Global configuration</p> |
| <pre>ip igmp profile <1-16> enable</pre> <p>Enables this IGMP filter. Command mode: Global configuration</p> |
| <pre>no ip igmp profile <1-16> enable</pre> <p>Disables this IGMP filter. Command mode: Global configuration</p> |
| <pre>no ip igmp profile <1-16></pre> <p>Deletes this filter's parameter definitions. Command mode: Global configuration</p> |
| <pre>show ip igmp profile <1-16></pre> <p>Displays the current IGMP filter. Command mode: All</p> |

IGMP Filtering Port Configuration

Table 290 describes the commands used to configure a port for IGMP filtering.

Table 290. IGMP Filter Port Configuration Commands

| Command Syntax and Usage |
|---|
| <pre>[no] ip igmp filtering</pre> <p>Enables or disables IGMP filtering on this port. Command mode: Interface port</p> |
| <pre>ip igmp profile <1-16></pre> <p>Adds an IGMP filter to this port. Command mode: Interface port</p> |
| <pre>no ip igmp profile <1-16></pre> <p>Removes an IGMP filter from this port. Command mode: Interface port</p> |
| <pre>show interface port <port alias or number> igmp-filtering</pre> <p>Displays the current IGMP filter parameters for this port. Command mode: All</p> |

IGMP Advanced Configuration

Table 291 describes the commands used to configure advanced IGMP parameters.

Table 291. IGMP Advanced Configuration Commands

| Command Syntax and Usage |
|---|
| <pre>ip igmp query-interval <1-600></pre> <p>Sets the IGMP router query interval, in seconds. The default value is 125.</p> <p>Command mode: Global configuration</p> |
| <pre>ip igmp robust <2-10></pre> <p>Configures the IGMP Robustness variable, which allows you to tune the switch for expected packet loss on the subnet. If you expect the subnet to have a high rate of packet loss, increase the value. The default value is 2.</p> <p>Command mode: Global configuration</p> |
| <pre>ip igmp timeout <1-255></pre> <p>Configures the timeout value for IGMP Membership Reports (host). Once the timeout value is reached, the switch removes the host from its IGMP table, if the conditions are met. The range is from 1 to 255 seconds. The default is 10 seconds.</p> <p>Command mode: Global configuration</p> |
| <pre>[no] ip igmp fastleave <VLAN number></pre> <p>Enables or disables Fastleave processing. Fastleave lets the switch immediately remove a port from the IGMP port list if the host sends a Leave message and the proper conditions are met. This command is disabled by default.</p> <p>Command mode: Global configuration</p> |
| <pre>[no] ip igmp rtralert</pre> <p>Enables or disables the Router Alert option in IGMP messages.</p> <p>Command mode: Global configuration</p> |

IGMP Querier Configuration

Table 292. describes the commands used to configure IGMP Querier.

Table 292. IGMP Querier Configuration Options

| Command Syntax and Usage |
|---|
| <pre>[no] ip igmp querier vlan <VLAN number> enable</pre> <p>Enables or disables the IGMP Querier globally.</p> <p>Command mode: Global configuration</p> |
| <pre>ip igmp querier vlan <VLAN number> source-ip <IP address></pre> <p>Configures the IGMP source IP address for the selected VLAN.</p> <p>Command mode: Global configuration</p> |

Table 292. IGMP Querier Configuration Options (continued)

| Command Syntax and Usage | |
|--|---|
| <pre>ip igmp querier vlan <VLAN number> max-response <1-256></pre> | <p>Configures the maximum time, in tenths of a second, allowed before responding to a Membership Query message. The default value is 100.</p> <p>By varying the Query Response Interval, an administrator may tune the burstiness of IGMP messages on the subnet; larger values make the traffic less bursty, as host responses are spread out over a larger interval.</p> <p>Command mode: Global configuration</p> |
| <pre>ip igmp querier vlan <VLAN number> query-interval <1-608></pre> | <p>Configures the interval between IGMP Query broadcasts. The default value is 125 seconds.</p> <p>Command mode: Global configuration</p> |
| <pre>ip igmp querier vlan <VLAN number> robustness <2-10></pre> | <p>Configures the IGMP Robustness variable, which is the number of times that the switch sends each IGMP message. The default value is 2.</p> <p>Command mode: Global configuration</p> |
| <pre>ip igmp querier vlan <VLAN number> election-type [ipv4 mac]</pre> | <p>Sets the IGMP Querier election criteria as IP address or Mac address. The default setting is IPv4.</p> <p>Command mode: Global configuration</p> |
| <pre>ip igmp querier vlan <VLAN number> startup-interval <1-608></pre> | <p>Configures the Startup Query Interval, which is the interval between General Queries sent out at startup.</p> <p>Command mode: Global configuration</p> |
| <pre>ip igmp querier vlan <VLAN number> startup-count <1-10></pre> | <p>Configures the Startup Query Count, which is the number of IGMP Queries sent out at startup. Each Query is separated by the Startup Query Interval. The default value is 2.</p> <p>Command mode: Global configuration</p> |
| <pre>ip igmp querier vlan <VLAN number> version [v1 v2 v3]</pre> | <p>Configures the IGMP version. The default version is v3.</p> <p>Command mode: Global configuration</p> |
| <pre>ip igmp querier enable</pre> | <p>Enables IGMP Querier.</p> <p>Command mode: Global configuration</p> |
| <pre>no ip igmp querier enable</pre> | <p>Disables IGMP Querier.</p> <p>Command mode: Global configuration</p> |

Table 292. IGMP Querier Configuration Options (continued)

| Command Syntax and Usage |
|---|
| <pre>show ip igmp querier vlan <VLAN number></pre> <p>Displays IGMP Querier information for the selected VLAN.</p> <p>Command mode: Global configuration</p> |
| <pre>show ip igmp querier</pre> <p>Displays the current IGMP Querier parameters.</p> <p>Command mode: All</p> |

IKEv2 Configuration

Table 293 describes the commands used to configure IKEv2.

Table 293. IKEv2 Options

| Command Syntax and Usage |
|---|
| <pre>ikev2 retransmit-interval <1-20></pre> <p>Sets the interval, in seconds, the timeout value in case a packet is not received by the peer and needs to be retransmitted. The default value is 20 seconds.</p> <p>Command mode: Global configuration</p> |
| <pre>[no] ikev2 cookie</pre> <p>Enables or disables cookie notification.</p> <p>Command mode: Global configuration</p> |
| <pre>show ikev2</pre> <p>Displays the current IKEv2 settings.</p> <p>Command mode: All</p> |

IKEv2 Proposal Configuration

Table 294 describes the commands used to configure an IKEv2 proposal.

Table 294. IKEv2 Proposal Options

| Command Syntax and Usage |
|--|
| <pre>ikev2 proposal</pre> <p>Enter IKEv2 proposal mode.</p> <p>Command mode: Global configuration</p> |
| <pre>encryption {3des aes-cbc des}</pre> <p>Configures IKEv2 encryption mode. The default value is 3des.</p> <p>Command mode: IKEv2 proposal</p> |
| <pre>integrity {md5 sha1}</pre> <p>Configures the IKEv2 authentication algorithm type. The default value is sha1.</p> <p>Command mode: IKEv2 proposal</p> |
| <pre>group {1 2 5 14 24}</pre> <p>Configures the the DH group. The default group is 2.</p> <p>Command mode: IKEv2 proposal</p> |

IKEv2 Preshare Key Configuration

Table 295 describes the commands used to configure IKEv2 preshare keys.

Table 295. IKEv2 Preshare Key Options

| Command Syntax and Usage |
|--|
| <pre>ikev2 preshare-key local <1-32 characters></pre> <p>Configures the local preshare key. The default value is <code>ibm123</code>.</p> <p>Command mode: Global configuration</p> |
| <pre>ikev2 preshare-key remote <1-32 characters> <IPv6 address></pre> <p>Configures the remote preshare key for the IPv6 address.</p> <p>Command mode: Global configuration</p> |
| <pre>show ikev2 preshare-key</pre> <p>Displays the current IKEv2 Preshare key settings.</p> <p>Command mode: Global configuration</p> |

IKEv2 Identification Configuration

Table 296 describes the commands used to configure IKEv2 identification.

Table 296. IKEv2 Identification Options

| Command Syntax and Usage |
|--|
| <pre>ikev2 identity local address</pre> <p>Configures the switch to use the supplied IPv6 address as identification.</p> <p>Command mode: Global configuration</p> |
| <pre>ikev2 identity local fqdn <1-32 characters></pre> <p>Configures the switch to use the fully-qualified domain name (such as "example.com") as identification.</p> <p>Command mode: Global configuration</p> |
| <pre>ikev2 identity local email <1-32 characters></pre> <p>Configures the switch to use the supplied email address (such as "xyz@example.com") as identification.</p> <p>Command mode: Global configuration</p> |
| <pre>show ikev2 identity</pre> <p>Displays the current IKEv2 identification settings.</p> <p>Command mode: All</p> |

IPsec Configuration

[Table 297](#) describes the commands used to configure IPsec.

Table 297. IPsec Options

| Command Syntax and Usage |
|---|
| <pre>ipsec enable</pre> <p>Enables IPsec. Command mode: Global configuration</p> |
| <pre>no ipsec enable</pre> <p>Disables IPsec. Command mode: Global configuration</p> |
| <pre>show ipsec</pre> <p>Displays the current IPsec settings. Command mode: All</p> |

IPsec Transform Set Configuration

Table 298 describes the commands used to configure IPsec transforms.

Table 298. IPsec Transform Set Options

| Command Syntax and Usage |
|---|
| <pre>ipsec transform-set <1-10> {ah-md5 ah-sha1 esp-3des esp-aes-cbc esp-des esp-md5 esp-null esp sha1}</pre> <p>Sets the AH or ESP authentication, encryption, or integrity algorithm. The available algorithms are as follows:</p> <ul style="list-style-type: none"> - ah-md5 - ah-sha1 - esp-3des - esp-aes-cbc - esp-des - esp-md5 - esp-null - esp - sha1 <p>Command mode: Global configuration</p> |
| <pre>ipsec transform-set <1-10> transport {ah-md5 ah-sha1 esp-3des esp-aes-cbc esp-des esp-md5 esp-null esp sha1}</pre> <p>Sets transport mode and the AH or ESP authentication, encryption, or integrity algorithm.</p> <p>Command mode: Global configuration</p> |
| <pre>ipsec transform-set <1-10> tunnel {ah-md5 ah-sha1 esp-3des esp-aes-cbc esp-des esp-md5 esp-null esp sha1}</pre> <p>Sets tunnel mode and the AH or ESP authentication, encryption, or integrity algorithm.</p> <p>Command mode: Global configuration</p> |
| <pre>no ipsec transform <1-10></pre> <p>Deletes the transform set.</p> <p>Command mode: Global configuration</p> |
| <pre>show ipsec transform-set <1-10></pre> <p>Displays the current IPsec Transform Set settings.</p> <p>Command mode: All</p> |

IPsec Traffic Selector Configuration

Table 299 describes the commands used to configure an IPsec traffic selector.

Table 299. IPsec Traffic Selector Options

| Command Syntax and Usage | |
|---|--|
| <pre>ipsec traffic-selector <1-10> action {permit deny} {any icmp tcp} {<IPv6 address> any}</pre> | <p>Sets the traffic-selector to permit or deny the specified type of traffic.</p> <p>Command mode: Global configuration</p> |
| <pre>src <IPv6 address> any</pre> | <p>Sets the source IPv6 address.</p> <p>Command mode: Global configuration</p> |
| <pre>prefix <1-128></pre> | <p>Sets the destination IPv6 prefix length.</p> <p>Command mode: Global configuration</p> |
| <pre>dst <IPv6 address> any</pre> | <p>Sets the destination IP address.</p> <p>Command mode: Global configuration</p> |
| <pre>del</pre> | <p>Deletes the traffic selector.</p> <p>Command mode: Global configuration</p> |
| <pre>cur</pre> | <p>Displays the current IPsec Traffic Selector settings.</p> <p>Command mode: All</p> |

IPsec Dynamic Policy Configuration

Table 300 describes the commands used to configure an IPsec dynamic policy.

Table 300. IPsec Dynamic Policy Options

| Command Syntax and Usage |
|---|
| <pre>ipsec dynamic-policy <I-10></pre> <p>Enter IPsec dynamic policy mode. Command mode: Global configuration</p> |
| <pre>peer <IPv6 address></pre> <p>Sets the remote peer IP address. Command mode: IPsec dynamic policy</p> |
| <pre>traffic-selector <I-10></pre> <p>Sets the traffic selector for the IPsec policy. Command mode: IPsec dynamic policy</p> |
| <pre>transform-set <I-10></pre> <p>Sets the transform set for the IPsec policy. Command mode: IPsec dynamic policy</p> |
| <pre>sa-lifetime <120-86400></pre> <p>Sets the IPsec SA lifetime in seconds. The default value is 86400 seconds. Command mode: IPsec dynamic policy</p> |
| <pre>pfs enable disable</pre> <p>Enables/disables perfect forward security. Command mode: IPsec dynamic policy</p> |
| <pre>show ipsec dynamic-policy <I-10></pre> <p>Displays the current IPsec dynamic policy settings. Command mode: All</p> |

IPsec Manual Policy Configuration

Table 301 describes the commands used to configure an IPsec manual policy.

Table 301. IPsec Manual Policy Options

| Command Syntax and Usage |
|--|
| <pre>ipsec manual-policy <I-I0></pre> <p>Enter IPsec manual policy mode.</p> <p>Command mode: Global configuration</p> |
| <pre>in-ah auth-key <key code (hexadecimal)></pre> <p>Sets inbound Authentication Header (AH) authenticator key.</p> <p>Note: For manual policies, when peering with a third-party device, key lengths are fixed to 20 characters for SHA1 and 16 characters for MD5 encryption.</p> <p>Command mode: IPsec manual policy</p> |
| <pre>peer <IPv6 address></pre> <p>Sets the remote peer IP address.</p> <p>Command mode: IPsec manual policy</p> |
| <pre>traffic-selector <I-I0></pre> <p>Sets the traffic selector for the IPsec policy.</p> <p>Command mode: IPsec manual policy</p> |
| <pre>transform-set <I-I0></pre> <p>Sets the transform set for the IPsec policy.</p> <p>Command mode: IPsec manual policy</p> |
| <pre>in-ah spi <256-4294967295></pre> <p>Sets the inbound Authentication Header (AH) Security Parameter Index (SPI).</p> <p>Note: For manual policies, when peering with a third-party device, key lengths are fixed to 20 characters for SHA1 and 16 characters for MD5 encryption.</p> <p>Command mode: IPsec manual policy</p> |
| <pre>in-esp cipher-key <key code (hexadecimal)></pre> <p>Sets the inbound Encapsulating Security Payload (ESP) cipher key.</p> <p>Note: For manual policies, when peering with a third-party device, key lengths are fixed to 8 characters for DES and to 24 characters for 3DES and AES-CBC encryption.</p> <p>Command mode: IPsec manual policy</p> |
| <pre>in-esp auth-key <key code (hexadecimal)></pre> <p>Sets the inbound Encapsulating Security Payload (ESP) authenticator key.</p> <p>Note: For manual policies, when peering with a third-party device, key lengths are fixed to 8 characters for DES and to 24 characters for 3DES and AES-CBC encryption.</p> <p>Command mode: IPsec manual policy</p> |

Table 301. IPsec Manual Policy Options (continued)

| Command Syntax and Usage | |
|--|---|
| <code>in-esp auth-key spi <256-4294967295></code> | <p>Sets the inbound Encapsulating Security Payload (ESP) Security Parameter Index (SPI).</p> <p>Note: For manual policies, when peering with a third-party device, key lengths are fixed to 20 characters for SHA1 and 16 characters for MD5 encryption.</p> <p>Command mode: IPsec manual policy</p> |
| <code>out-ah auth-key <key code (hexadecimal)></code> | <p>Sets the outbound Authentication Header (AH) authenticator key.</p> <p>Note: For manual policies, when peering with a third-party device, key lengths are fixed to 20 characters for SHA1 and 16 characters for MD5 encryption.</p> <p>Command mode: IPsec manual policy</p> |
| <code>out-ah spi <256-4294967295></code> | <p>Sets the outbound Authentication Header (AH) Security Parameter Index (SPI).</p> <p>Note: For manual policies, when peering with a third-party device, key lengths are fixed to 20 characters for SHA1 and 16 characters for MD5 encryption.</p> <p>Command mode: IPsec manual policy</p> |
| <code>out-esp auth-key <key code (hexadecimal)></code> | <p>Sets the outbound Encapsulating Security Payload (ESP) authenticator key.</p> <p>Note: For manual policies, when peering with a third-party device, key lengths are fixed to 8 characters for DES and to 24 characters for 3DES and AES-CBC encryption.</p> <p>Command mode: IPsec manual policy</p> |
| <code>out-esp cipher-key <key code (hexadecimal)></code> | <p>Sets the outbound Encapsulating Security Payload (ESP) cipher key.</p> <p>Note: For manual policies, when peering with a third-party device, key lengths are fixed to 8 characters for DES and to 24 characters for 3DES and AES-CBC encryption.</p> <p>Command mode: IPsec manual policy</p> |
| <code>out-esp auth-key spi <256-4294967295></code> | <p>Sets the outbound Encapsulating Security Payload (ESP) Security Parameter Index (SPI).</p> <p>Note: For manual policies, when peering with a third-party device, key lengths are fixed to 20 characters for SHA1 and 16 characters for MD5 encryption.</p> <p>Command mode: IPsec manual policy</p> |
| <code>show ipsec manual-policy <1-10></code> | <p>Displays the current IPsec manual policy settings.</p> <p>Command mode: All</p> |

Domain Name System Configuration

The Domain Name System (DNS) commands are used for defining the primary and secondary DNS servers on your local network, and for setting the default domain name served by the switch services. DNS parameters must be configured prior to using hostname parameters with the `ping`, `traceroute`, and `tftp` commands.

Table 302. Domain Name Service Commands

| Command Syntax and Usage | |
|---|---|
| <code>[no] ip dns primary-server <IP address></code> | <p>You are prompted to set the IPv4 address for your primary DNS server, using dotted decimal notation.</p> <p>Command mode: Global configuration</p> |
| <code>[no] ip dns secondary-server <IP address></code> | <p>You are prompted to set the IPv4 address for your secondary DNS server, using dotted decimal notation. If the primary DNS server fails, the configured secondary will be used instead.</p> <p>Command mode: Global configuration</p> |
| <code>[no] ip dns ipv6 primary-server <IP address></code> | <p>You are prompted to set the IPv6 address for your primary DNS server, using hexadecimal format with colons.</p> <p>Command mode: Global configuration</p> |
| <code>[no] ip dns ipv6 secondary-server <IP address></code> | <p>You are prompted to set the IPv6 address for your secondary DNS server, using hexadecimal format with colons. If the primary DNS server fails, the configured secondary will be used instead.</p> <p>Command mode: Global configuration</p> |
| <code>ip dns ipv6 request-version {ipv4 ipv6}</code> | <p>Sets the protocol used for the first request to the DNS server, as follows:</p> <ul style="list-style-type: none"> – IPv4 – IPv6 <p>Command mode: Global configuration</p> |
| <code>[no] ip dns domain-name <string></code> | <p>Sets the default domain name used by the switch. For example: <code>mycompany.com</code></p> <p>Command mode: Global configuration</p> |
| <code>show ip dns</code> | <p>Displays the current Domain Name System settings.</p> <p>Command mode: All</p> |

Bootstrap Protocol Relay Configuration

The Bootstrap Protocol (BOOTP) Relay commands are used to let hosts get their configurations from a Dynamic Host Configuration Protocol (DHCP) server. The BOOTP configuration enables the switch to forward a client request for an IP address to two DHCP/BOOTP servers with IP addresses that have been configured on the EN4093 and EN4093R.

BOOTP relay is turned off by default.

Table 303. Global BOOTP Relay Configuration Options

| Command Syntax and Usage |
|---|
| <pre>[no] ip bootp-relay server <I-4> address <IP address></pre> <p>Sets the IP address of the selected global BOOTP server.</p> <p>Command mode: Global configuration</p> |
| <pre>ip bootp-relay enable</pre> <p>Globally turns on BOOTP relay.</p> <p>Command mode: Global configuration</p> |
| <pre>no ip bootp-relay enable</pre> <p>Globally turns off BOOTP relay.</p> <p>Command mode: Global configuration</p> |

BOOTP Relay Broadcast Domain Configuration

These commands allow you to configure a BOOTP server for a specific broadcast domain, based on its associated VLAN.

Table 304. BOOTP Relay Broadcast Domain Configuration Options

| Command Syntax and Usage |
|--|
| <pre>ip bootp-relay bcast-domain <I-10> vlan <VLAN number></pre> <p>Configures the VLAN of the broadcast domain. Each broadcast domain must have a unique VLAN.</p> <p>Command mode: Global configuration</p> |
| <pre>ip bootp-relay bcast-domain <I-10> server <I-4> address <IPv4 address></pre> <p>Sets the IP address of the BOOTP server.</p> <p>Command mode: Global configuration</p> |
| <pre>ip bootp-relay bcast-domain <I-10> enable</pre> <p>Enables BOOTP Relay for the broadcast domain.</p> <p>Command mode: Global configuration</p> |
| <pre>no ip bootp-relay bcast-domain <I-10> enable</pre> <p>Disables BOOTP Relay for the broadcast domain. When disabled, BOOTP Relay is performed by one of the global BOOTP servers.</p> <p>Command mode: Global configuration</p> |

Table 304. BOOTP Relay Broadcast Domain Configuration Options

| Command Syntax and Usage |
|---|
| <pre>no ip bootp-relay bcast-domain <1-10></pre> <p>Deletes the selected broadcast domain configuration.</p> <p>Command mode: Global configuration</p> |
| <pre>show ip bootp-relay</pre> <p>Displays the current parameters for the BOOTP Relay broadcast domain.</p> <p>Command mode: All</p> |

VRRP Configuration

Virtual Router Redundancy Protocol (VRRP) support on the EN4093 and EN4093R provides redundancy between routers in a LAN. This is accomplished by configuring the same virtual router IP address and ID number on each participating VRRP-capable routing device. One of the virtual routers is then elected as the master, based on a number of priority criteria, and assumes control of the shared virtual router IP address. If the master fails, one of the backup virtual routers will assume routing authority and take control of the virtual router IP address.

By default, VRRP is disabled. Networking OS has extended VRRP to include virtual servers as well, allowing for full active/active redundancy between switches. For more information on VRRP, see the “High Availability” chapter in the *Networking OS 7.7 Application Guide*.

Table 305. Virtual Router Redundancy Protocol Commands

| Command Syntax and Usage | |
|-------------------------------|---|
| <code>router vrrp</code> | Enter Router VRRP configuration mode. Command mode: Global configuration |
| <code>[no] hot-standby</code> | Enables or disables hot standby processing, in which two or more switches provide redundancy for each other. By default, this option is disabled. Command mode: Router VRRP |
| <code>enable</code> | Globally enables VRRP on this switch. Command mode: Router VRRP |
| <code>no enable</code> | Globally disables VRRP on this switch. Command mode: Router VRRP |
| <code>show ip vrrp</code> | Displays the current VRRP parameters. Command mode: All |

Virtual Router Configuration

These commands are used for configuring virtual routers for this switch. A virtual router is defined by its virtual router ID and an IP address. On each VRRP-capable routing device participating in redundancy for this virtual router, a virtual router will be configured to share the same virtual router ID and IP address.

Virtual routers are disabled by default.

Table 306. VRRP Virtual Router Configuration Commands

| Command Syntax and Usage |
|--|
| <pre>virtual-router <1-15> virtual-router-id <1-255></pre> <p>Defines the virtual router ID (VRID). This is used in conjunction with the <code>[no] virtual-router <VRID> address <IP address></code> command below to define a virtual router on this switch. To create a pool of VRRP-enabled routing devices which can provide redundancy to each other, each participating VRRP device must be configured with the same virtual router.</p> <p>The VRID for standard virtual routers (where the virtual router IP address is not the same as any virtual server) can be any integer between 1 and 255. The default value is 1.</p> <p>All VRID values must be unique within the VLAN to which the virtual router's IP interface belongs.</p> <p>Command mode: Router VRRP</p> |
| <pre>[no] virtual-router <1-15> address <IP address></pre> <p>Defines the IP address for this virtual router using dotted decimal notation. This is used in conjunction with the VRID (above) to configure the same virtual router on each participating VRRP device. The default address is 0.0.0.0.</p> <p>Command mode: Router VRRP</p> |
| <pre>virtual-router <1-15> interface <interface number></pre> <p>Selects a switch IP interface. If the IP interface has the same IP address as the <code>addr</code> option above, this switch is considered the "owner" of the defined virtual router. An owner has a special priority of 255 (highest) and will always assume the role of master router, even if it must pre-empt another virtual router which has assumed master routing authority. This pre-emption occurs even if the <code>preem</code> option below is disabled. The default value is 1.</p> <p>Command mode: Router VRRP</p> |
| <pre>virtual-router <1-15> priority <1-254></pre> <p>Defines the election priority bias for this virtual server. The priority value can be any integer between 1 and 254. The default value is 100.</p> <p>During the master router election process, the routing device with the highest virtual router priority number wins. If there is a tie, the device with the highest IP interface address wins. If this virtual router's IP address is the same as the one used by the IP interface, the priority for this virtual router will automatically be set to 255 (highest).</p> <p>When priority tracking is used, this base priority value can be modified according to a number of performance and operational criteria.</p> <p>Command mode: Router VRRP</p> |

Table 306. VRRP Virtual Router Configuration Commands (continued)

| Command Syntax and Usage | |
|---|---|
| <pre>virtual-router <1-15> timers advertise <1-255></pre> | <p>Defines the time interval between VRRP master advertisements. This can be any integer between 1 and 255 seconds. The default value is 1.</p> <p>Command mode: Router VRRP</p> |
| <pre>[no] virtual-router <1-15> preemption</pre> | <p>Enables or disables master preemption. When enabled, if this virtual router is in backup mode but has a higher priority than the current master, this virtual router will preempt the lower priority master and assume control. Note that even when <code>preemption</code> is disabled, this virtual router will always pre-empt any other master if this switch is the owner (the IP interface address and virtual router <code>addr</code> are the same). By default, this option is enabled.</p> <p>Command mode: Router VRRP</p> |
| <pre>virtual-router <1-15> enable</pre> | <p>Enables this virtual router.</p> <p>Command mode: Router VRRP</p> |
| <pre>no virtual-router <1-15> enable</pre> | <p>Disables this virtual router.</p> <p>Command mode: Router VRRP</p> |
| <pre>no virtual-router <1-15></pre> | <p>Deletes this virtual router from the switch configuration.</p> <p>Command mode: Router VRRP</p> |
| <pre>show ip vrrp virtual-router <1-15></pre> | <p>Displays the current configuration information for this virtual router.</p> <p>Command mode: All</p> |

Virtual Router Priority Tracking Configuration

These commands are used for modifying the priority system used when electing the master router from a pool of virtual routers. Various tracking criteria can be used to bias the election results. Each time one of the tracking criteria is met, the priority level for the virtual router is increased by an amount defined through the VRRP Tracking commands.

Criteria are tracked dynamically, continuously updating virtual router priority levels when enabled. If the virtual router preemption option is enabled, this virtual router can assume master routing authority when its priority level rises above that of the current master.

Some tracking criteria apply to standard virtual routers, otherwise called “virtual interface routers.” A virtual *server* router is defined as any virtual router whose IP address is the same as any configured virtual server IP address.

Table 307. VRRP Priority Tracking Configuration Commands

| Command Syntax and Usage |
|---|
| <pre>[no] virtual-router <1-15> track virtual-routers</pre> <p>When enabled, the priority for this virtual router will be increased for each virtual router in master mode on this switch. This is useful for making sure that traffic for any particular client/server pairing are handled by the same switch, increasing routing and load balancing efficiency. This command is disabled by default.</p> <p>Command mode: Router VRRP</p> |
| <pre>[no] virtual-router <1-15> track interfaces</pre> <p>When enabled, the priority for this virtual router will be increased for each other IP interface active on this switch. An IP interface is considered active when there is at least one active port on the same VLAN. This helps elect the virtual routers with the most available routes as the master. This command is disabled by default.</p> <p>Command mode: Router VRRP</p> |
| <pre>[no] virtual-router <1-15> track ports</pre> <p>When enabled, the priority for this virtual router will be increased for each active port on the same VLAN. A port is considered “active” if it has a link and is forwarding traffic. This helps elect the virtual routers with the most available ports as the master. This command is disabled by default.</p> <p>Command mode: Router VRRP</p> |
| <pre>show ip vrrp virtual-router <1-15> track</pre> <p>Displays the current configuration for priority tracking for this virtual router.</p> <p>Command mode: All</p> |

Virtual Router Group Configuration

Virtual Router Group commands are used for associating all virtual routers into a single logical virtual router, which forces all virtual routers on the EN4093 and EN4093R to either be master or backup as a group. A virtual router is defined by its virtual router ID and an IP address. On each VRRP-capable routing device participating in redundancy for this virtual router, a virtual router will be configured to share the same virtual router ID and IP address.

Note: This option is required to be configured only when using at least two EN4093 and EN4093Rs in a hot-standby failover configuration, where only one switch is active at any time.

Table 308. VRRP Virtual Router Group Configuration Commands

| Command Syntax and Usage |
|---|
| <pre>group virtual-router-id <1-255></pre> <p>Defines the virtual router ID (VRID).</p> <p>The VRID for standard virtual routers (where the virtual router IP address is not the same as any virtual server) can be any integer between 1 and 255. All VRID values must be unique within the VLAN to which the virtual router's IP interface (see <code>interface</code> below) belongs. The default virtual router ID is 1.</p> <p>Command mode: Router VRRP</p> |
| <pre>group interface <interface number></pre> <p>Selects a switch IP interface. The default switch IP interface number is 1.</p> <p>Command mode: Router VRRP</p> |
| <pre>group priority <1-254></pre> <p>Defines the election priority bias for this virtual router group. This can be any integer between 1 and 254. The default value is 100.</p> <p>During the master router election process, the routing device with the highest virtual router priority number wins.</p> <p>Each virtual router group is treated as one entity regardless of how many virtual routers are in the group. When the switch tracks the virtual router group, it measures the resources contained in the group (such as interfaces, VLAN ports, real servers). The priority is updated as a group. Every virtual router in the group has the same priority.</p> <p>The <i>owner</i> parameter does not apply to the virtual router group. The group itself cannot be an owner and therefore the priority is 1-254.</p> <p>Command mode: Router VRRP</p> |
| <pre>group advertisement <1-255></pre> <p>Defines the time interval between VRRP master advertisements. This can be any integer between 1 and 255 seconds. The default is 1.</p> <p>Command mode: Router VRRP</p> |

Table 308. VRRP Virtual Router Group Configuration Commands (continued)

| Command Syntax and Usage | |
|------------------------------------|--|
| [no] group <code>preemption</code> | <p>Enables or disables master pre-emption. When enabled, if the virtual router group is in backup mode but has a higher priority than the current master, this virtual router will pre-empt the lower priority master and assume control. Note that even when <code>preemption</code> is disabled, this virtual router will always pre-empt any other master if this switch is the owner (the IP interface address and virtual router address are the same). By default, this option is enabled.</p> <p>Command mode: Router VRRP</p> |
| group <code>enable</code> | <p>Enables the virtual router group.</p> <p>Command mode: Router VRRP</p> |
| no group <code>enable</code> | <p>Disables the virtual router group.</p> <p>Command mode: Router VRRP</p> |
| no group | <p>Deletes the virtual router group from the switch configuration.</p> <p>Command mode: Router VRRP</p> |
| show ip vrrp group | <p>Displays the current configuration information for the virtual router group.</p> <p>Command mode: All</p> |

Virtual Router Group Priority Tracking Configuration

Note: If *Virtual Router Group Tracking* is enabled, the tracking option will be available only under *group* option. The tracking setting for the other individual virtual routers will be ignored.

Table 309. *Virtual Router Group Priority Tracking Configuration Commands*

| Command Syntax and Usage |
|---|
| <pre>[no] group track interfaces</pre> <p>When enabled, the priority for this virtual router will be increased for each other IP interface active on this switch. An IP interface is considered active when there is at least one active port on the same VLAN. This helps elect the virtual routers with the most available routes as the master. This command is disabled by default.</p> <p>Command mode: Router VRRP</p> |
| <pre>[no] group track ports</pre> <p>When enabled, the priority for this virtual router will be increased for each active port on the same VLAN. A port is considered “active” if it has a link and is forwarding traffic. This helps elect the virtual routers with the most available ports as the master. This command is disabled by default.</p> <p>Command mode: Router VRRP</p> |
| <pre>show ip vrrp group track</pre> <p>Displays the current configuration for priority tracking for this virtual router.</p> <p>Command mode: All</p> |

VRRP Interface Configuration

Note: The *interface* represents the IP interface on which authentication parameters must be configured.

These commands are used for configuring VRRP authentication parameters for the IP interfaces used with the virtual routers.

Table 310. VRRP Interface Commands

| Command Syntax and Usage | |
|--|---|
| <pre>interface <interface number> authentication {password none}</pre> | <p>Defines the type of authentication that will be used: <i>none</i> (no authentication) or <i>password</i> (password authentication).</p> <p>Command mode: Router VRRP</p> |
| <pre>[no] interface <interface number> password <password></pre> | <p>Defines a plain text password up to eight characters long. This password will be added to each VRRP packet transmitted by this interface when password authentication is chosen (see <i>interface authentication</i> above).</p> <p>Command mode: Router VRRP</p> |
| <pre>no interface <interface number></pre> | <p>Clears the authentication configuration parameters for this IP interface. The IP interface itself is not deleted.</p> <p>Command mode: Router VRRP</p> |
| <pre>show ip vrrp interface <interface number></pre> | <p>Displays the current configuration for this IP interface's authentication parameters.</p> <p>Command mode: All</p> |

VRRP Tracking Configuration

These commands are used for setting weights for the various criteria used to modify priority levels during the master router election process. Each time one of the tracking criteria is met (see “VRRP Virtual Router Priority Tracking Commands” on [page 432](#)), the priority level for the virtual router is increased by a defined amount.

Table 311. VRRP Tracking Configuration Commands

| Command Syntax and Usage |
|--|
| <pre>tracking-priority-increment virtual-routers <0-254></pre> <p>Defines the priority increment value (0 through 254) for virtual routers in master mode detected on this switch. The default value is 2.</p> <p>Command mode: Router VRRP</p> |
| <pre>tracking-priority-increment interfaces <0-254></pre> <p>Defines the priority increment value for active IP interfaces detected on this switch. The default value is 2.</p> <p>Command mode: Router VRRP</p> |
| <pre>tracking-priority-increment ports <0-254></pre> <p>Defines the priority increment value for active ports on the virtual router’s VLAN. The default value is 2.</p> <p>Command mode: Router VRRP</p> |
| <pre>show ip vrrp tracking-priority-increment</pre> <p>Displays the current configuration of priority tracking increment values.</p> <p>Command mode: All</p> |

Note: These priority tracking options only define increment values. These options do not affect the VRRP master router election process until options under the VRRP Virtual Router Priority Tracking Commands (see [page 432](#)) are enabled.

Protocol Independent Multicast Configuration

Table 312. PIM Configuration Options

| Command Syntax and Usage |
|--|
| <pre>ip pim component <I-2></pre> <p>Enter PIM component mode. See page 438 to view options. Command mode: Global configuration</p> |
| <pre>ip pim regstop-ratelimit-period <0-2147483647></pre> <p>Configures the register stop rate limit, in seconds. The default value is 5. Command mode: Global configuration</p> |
| <pre>[no] ip pim static-rp enable</pre> <p>Enables or disables static RP configuration. The default setting is disabled. Command mode: Global configuration</p> |
| <pre>[no] ip pim pmbr enable</pre> <p>Enables or disables PIM border router. The default setting is disabled. Command mode: Global configuration</p> |
| <pre>ip pim enable</pre> <p>Globally turns PIM on. Command mode: Global configuration</p> |
| <pre>no ip pim enable</pre> <p>Globally turns PIM off. Command mode: Global configuration</p> |
| <pre>clear ip pim mroute</pre> <p>Clears PIM multicast router entries. Command mode: Global configuration</p> |

PIM Component Configuration

Table 313. PIM Component Configuration Options

| Command Syntax and Usage |
|--|
| <pre>ip pim component <I-2></pre> <p>Enter PIM component mode. Command mode: Global configuration</p> |
| <pre>mode {dense sparse}</pre> <p>Configures the operational mode of the PIM router (dense or sparse). Command mode: PIM Component</p> |
| <pre>show ip pim component [<I-2>]</pre> <p>Displays the current PIM component configuration settings. Command mode: All</p> |

RP Candidate Configuration

Use these commands to configure a PIM router Rendezvous Point (RP) candidate.

Table 314. RP Candidate Configuration Options

| Command Syntax and Usage |
|---|
| <pre>rp-candidate rp-address <group multicast address> <group subnet mask> <IP address></pre> <p>Adds an RP candidate.</p> <p>Command mode: PIM Component</p> |
| <pre>no rp-candidate rp-address <group multicast address> <group subnet mask> <IP address></pre> <p>Removes the specified RP candidate.</p> <p>Command mode: PIM Component</p> |
| <pre>rp-candidate holdtime <0-255></pre> <p>Configures the hold time of the RP candidate, in seconds.</p> <p>Command mode: PIM Component</p> |

RP Static Configuration

Use these commands to configure a static PIM router Rendezvous Point (RP).

Table 315. RP Static Configuration Options

| Command Syntax and Usage |
|---|
| <pre>rp-static rp-address <group multicast address> <group subnet mask> <IP address></pre> <p>Adds a static RP.</p> <p>Command mode: PIM Component</p> |
| <pre>no rp-static rp-address <group multicast address> <group subnet mask> <IP address></pre> <p>Removes the specified static RP.</p> <p>Command mode: PIM Component</p> |

PIM Interface Configuration

Table 316. PIM Interface Configuration Options

| Command Syntax and Usage |
|---|
| <pre>interface ip <interface number></pre> <p>Enter Interface IP mode. Command mode: Global Configuration</p> |
| <pre>ip pim hello-interval <0-65535></pre> <p>Configures the time interval, in seconds, between PIM Hello packets. The default value is 30. Command mode: Interface IP</p> |
| <pre>ip pim join-prune-interval <0-65535></pre> <p>Configures the interval between Join Prune messages, in seconds. The default value is 60. Command mode: Interface IP</p> |
| <pre>[no] ip pim cbsr-preference <0-255></pre> <p>Configures the candidate bootstrap router preference. Command mode: Interface IP</p> |
| <pre>ip pim component-id <1-2></pre> <p>Defines the component ID for the interface. Command mode: Interface IP</p> |
| <pre>ip pim hello-holdtime <1-65535></pre> <p>Configures the time period for which a neighbor is to consider this switch to be operative (up). The default value is 105. Command mode: Interface IP</p> |
| <pre>ip pim dr-priority <0-4294967294></pre> <p>Configures the designated router priority. The default value is 1. Command mode: Interface IP</p> |
| <pre>ip pim override-interval <0-65535></pre> <p>Configures the override interval for the router interface, in seconds. Command mode: Interface IP</p> |
| <pre>ip pim lan-delay <0-32767></pre> <p>Configures the LAN delay value for the router interface, in seconds. Command mode: Interface IP</p> |
| <pre>[no] ip pim border-bit</pre> <p>Enables or disables the interface as a border router. The default setting is disabled. Command mode: Interface IP</p> |

Table 316. PIM Interface Configuration Options (continued)

| Command Syntax and Usage | |
|---|--|
| [no] ip pim lan-prune-delay | <p>Enables or disables LAN delay advertisements on the interface. The default setting is disabled.</p> <p>Command mode: Interface IP</p> |
| ip pim neighbor-addr <IP address> allow deny | <p>Allows or denies PIM access to the specified neighbor. You can configure a list of up to 72 neighbors that bypass the neighbor filter. Once you configure the interface to allow a neighbor, you can configure the interface to deny the neighbor.</p> <p>Command mode: Interface IP</p> |
| [no] ip pim neighbor-filter | <p>Enables or disables the PIM neighbor filter on the interface. When enabled, this interface does not accept any PIM neighbors, unless specifically permitted using the following command:</p> <p>ip pim neighbor-addr <IP address></p> <p>Command mode: Interface IP</p> |
| ip pim enable | <p>Enables PIM on the interface.</p> <p>Command mode: Interface IP</p> |
| no ip pim enable | <p>Disables PIM on the interface.</p> <p>Command mode: Interface IP</p> |
| show ip pim neighbor-filters | <p>Displays the configured PIM neighbor filters.</p> <p>Command mode: All</p> |
| show ip pim interface [<interface number> detail] | <p>Displays the current PIM interface parameters.</p> <p>Command mode: All</p> |

IPv6 Default Gateway Configuration

The switch supports IPv6 default gateways.

- Gateway 1 is used for data traffic.
- Gateway 132 is reserved for management.

[Table 317](#) describes the IPv6 Default Gateway Configuration commands.

Table 317. IPv6 Default Gateway Configuration Commands

| Command Syntax and Usage |
|--|
| <pre>ip gateway6 {<gateway number>} address <IPv6 address></pre> <p>Configures the IPv6 address of the default gateway, in hexadecimal format with colons (such as 3001:0:0:0:0:abcd:12).</p> <p>Command mode: Global configuration</p> |
| <pre>[no] ip gateway6 {<gateway number>} enable</pre> <p>Enables or disables the default gateway.</p> <p>Command mode: Global configuration</p> |
| <pre>no ip gateway6 {<gateway number>}</pre> <p>Deletes the default gateway.</p> <p>Command mode: Global configuration</p> |
| <pre>show ipv6 gateway6 {<gateway number>}</pre> <p>Displays the current IPv6 default gateway configuration.</p> <p>Command mode: All</p> |

IPv6 Static Route Configuration

Table 318 describes the IPv6 static route configuration commands.

Table 318. IPv6 Static Route Configuration Commands

| Command Syntax and Usage |
|---|
| <pre>ip route6 <IPv6 address> <prefix length> <IPv6 gateway address> [<interface number>]</pre> <p>Adds an IPv6 static route.</p> <p>Command mode: Global configuration</p> |
| <pre>no ip route6 <IPv6 address> <prefix length></pre> <p>Removes the selected route.</p> <p>Command mode: Global configuration</p> |
| <pre>no ip route6 [destination-address <IPv6 address> gateway <default gateway address> interface <1-128> all]</pre> <p>Clears IPv6 static routes. You are prompted to select the routes to clear, based on the following criteria:</p> <ul style="list-style-type: none"> – dest: Destination IPv6 address of the route – gw: Default gateway address used by the route – if: Interface used by the route – all: All IPv6 static routes <p>Command mode: Global configuration</p> |
| <pre>show ipv6 route static</pre> <p>Displays the current static route configuration.</p> <p>Command mode: All</p> |

IPv6 Neighbor Discovery Cache Configuration

Table 319 describes the IPv6 Neighbor Discovery cache configuration commands.

Table 319. IPv6 Neighbor Discovery Cache Configuration Commands

| Command Syntax and Usage |
|--|
| <pre>ip neighbors <IPv6 address> <MAC address> vlan <VLAN number> port <port number or alias></pre> <p>Adds a static entry to the Neighbor Discovery cache table.</p> <p>Command mode: Global configuration</p> |
| <pre>no ip neighbors {<IPv6 address> all}</pre> <p>Deletes the selected entry from the static Neighbor Discovery cache table.</p> <p>Command mode: Global configuration</p> |
| <pre>no ip neighbors [all if all interface port all vlan <VLAN number> all]</pre> <p>Clears the selected static entries in the Neighbor Discovery cache table.</p> <p>Command mode: Global configuration</p> |

IPv6 Path MTU Configuration

The following table describes the configuration options for Path MTU (Maximum Transmission Unit). The Path MTU cache can consume system memory and affect performance. These commands allow you to manage the Path MTU cache.

Table 320. IPv6 Path MTU Commands

| Command Syntax and Usage |
|---|
| <pre>ip pmtu6 timeout 0 <10-100></pre> <p>Sets the timeout value for Path MTU cache entries, in minutes. Enter 0 (zero) to set the timeout to infinity (no timeout). The default value is 10 minutes. Command mode: Global configuration</p> |
| <pre>clear ipv6 pmtu</pre> <p>Clears all entries in the Path MTU cache. Command mode: All Except User EXEC</p> |
| <pre>show ipv6 pmtu</pre> <p>Displays the current Path MTU configuration. Command mode: All</p> |

IPv6 Neighbor Discovery Prefix Configuration

The following table describes the Neighbor Discovery prefix configuration options. These commands allow you to define a list of prefixes to be placed in Prefix Information options in Router Advertisement messages sent from an interface.

Table 321. IPv6 Neighbor Discovery Prefix Commands

| Command Syntax and Usage |
|--|
| <pre>interface ip <1-127></pre> <p>Enters Interface IP mode. Command mode: Global configuration</p> |
| <pre>ipv6 nd prefix {<IPv6 prefix> <prefix length>} [no-advertise]</pre> <p>Adds a Neighbor Discovery prefix to the interface. The default setting is enabled. To disable the prefix and not advertise it in the Prefix Information options in Router Advertisement messages sent from the interface use the <code>no-advertise</code> option. Additional prefix options are listed in this table. Command mode: Interface IP</p> |
| <pre>no ipv6 nd prefix [<IPv6 prefix> <prefix length>] interface all</pre> <p>Removes the selected Neighbor Discovery prefix(es). If you specify an interface number, all prefixes for the interface are removed. Command mode: Interface IP</p> |

Table 321. IPv6 Neighbor Discovery Prefix Commands (continued)

| Command Syntax and Usage | |
|---|--|
| <pre>ipv6 nd prefix {<IPv6 prefix> <prefix length>} valid-lifetime <0-4294967295> [infinite variable] preferred-lifetime <0-4294967295> [infinite variable]</pre> | <p>Configures the Valid Lifetime and (optionally) the Preferred Lifetime of the prefix, in seconds.</p> <p>The Valid Lifetime is the length of time (relative to the time the packet is sent) that the prefix is valid for the purpose of on-link determination. The default value is 2592000.</p> <p>The Preferred Lifetime is the length of time (relative to the time the packet is sent) that addresses generated from the prefix via stateless address autoconfiguration remain preferred. The default value is 604800.</p> <p>Note: The Preferred Lifetime value must not exceed the Valid Lifetime value.</p> <p>Command mode: Interface IP</p> |
| <pre>ipv6 nd prefix {<IPv6 prefix> <prefix length>} off-link [no-autoconfig]</pre> | <p>Disables the on-link flag. When enabled, the on-link flag indicates that this prefix can be used for on-link determination. When disabled, the advertisement makes no statement about on-link or off-link properties of the prefix. The default setting is enabled.</p> <p>To clear the off-link flag, omit the off-link parameter when you issue this command.</p> <p>Command mode: Interface IP</p> |
| <pre>ipv6 nd prefix {<IPv6 prefix> <prefix length>} no-autoconfig</pre> | <p>Disables the autonomous flag. When enabled, the autonomous flag indicates that the prefix can be used for stateless address configuration. The default setting is enabled.</p> <p>Command mode: Interface IP</p> |
| <pre>show ipv6 prefix {<interface number>}</pre> | <p>Displays current Neighbor Discovery prefix parameters.</p> <p>Command mode: All</p> |

IPv6 Prefix Policy Table Configuration

The following table describes the configuration options for the IPv6 Prefix Policy Table. The Prefix Policy Table allows you to override the default address selection criteria.

Table 322. IPv6 Prefix Policy Table Options

| Command Syntax and Usage |
|---|
| <pre>ip prefix-policy <IPv6 prefix> <prefix length> <precedence (0-100)> <label (0-100)></pre> <p>Adds a Prefix Policy Table entry. Enter the following parameters:</p> <ul style="list-style-type: none">– IPv6 address prefix– Prefix length– Precedence: The precedence is used to sort destination addresses. Prefixes with a higher precedence are sorted before those with a lower precedence.– Label: The label allows you to select prefixes based on matching labels. Source prefixes are coupled with destination prefixes if their labels match. <p>Command mode: Global configuration</p> |
| <pre>no ip prefix-policy <IPv6 prefix> <prefix length> <precedence (0-100)> <label (0-100)></pre> <p>Removes a prefix policy table entry.</p> <p>Command mode: Global configuration</p> |
| <pre>show ip prefix-policy</pre> <p>Displays the current Prefix Policy Table configuration.</p> <p>Command mode: All</p> |

Open Shortest Path First Version 3 Configuration

Table 323. OSPFv3 Configuration Commands

| Command Syntax and Usage |
|--|
| <pre>[no] ipv6 router ospf</pre> <p>Enter OSPFv3 configuration mode. Enables or disables OSPFv3 routing protocol.</p> <p>Command mode: Global configuration</p> |
| <pre>abr-type [standard cisco ibm]</pre> <p>Configures the Area Border Router (ABR) type, as follows:</p> <ul style="list-style-type: none">– Standard– Cisco– IBM <p>The default setting is <code>standard</code>.</p> <p>Command mode: Router OSPF3</p> |

Table 323. OSPFv3 Configuration Commands (continued)

| Command Syntax and Usage | |
|--|---|
| <pre>as-external lsdb-limit <LSDB limit (0-2147483647, -1 for no limit)></pre> | <p>Sets the link state database limit.</p> <p>Command mode: Router OSPF3</p> |
| <pre>exit-overflow-interval <0-4294967295></pre> | <p>Configures the number of seconds that a router takes to exit Overflow State. The default value is 0 (zero).</p> <p>Command mode: Router OSPF3</p> |
| <pre>neighbor <I-256> {address <IPv6 address> enable interface <I-126> priority <0-255>}</pre> | <p>Configures directly reachable routers over non-broadcast networks. This is required for non-broadcast multiple access (NBMA) networks and optional for Point-to-Multipoint networks.</p> <ul style="list-style-type: none"> – <code>address</code> configures the neighbor's IPv6 address – <code>enable</code> activates a previously disabled neighbor – <code>interface</code> configures the OSPFv3 interface used for the neighbor entry – <code>priority</code> configures the priority value used for the neighbor entry. A priority value of 255 is the highest and 1 is the lowest. A priority value of 0 specifies that the neighbor cannot be used as Designated Router. The default value is 1. <p>Command mode: Router OSPF3</p> |
| <pre>no neighbor <I-256> [enable]</pre> | <p>Deletes the neighbor entry.</p> <p>Using the <code>enable</code> option only disables the neighbor, while preserving its settings.</p> <p>Command mode: Router OSPF3</p> |
| <pre>reference-bandwidth <0-4294967295></pre> | <p>Configures the reference bandwidth, in kilobits per second, used to calculate the default interface metric. The default value is 100,000.</p> <p>Command mode: Router OSPF3</p> |
| <pre>timers spf {<SPF delay (0-65535)>} {<SPF hold time (0-65535)>}</pre> | <p>Configures the number of seconds that SPF calculation is delayed after a topology change message is received. The default value is 5.</p> <p>Configures the number of seconds between SPF calculations. The default value is 10.</p> <p>Command mode: Router OSPF3</p> |
| <pre>router-id <IPv4 address></pre> | <p>Defines the router ID.</p> <p>Command mode: Router OSPF3</p> |

Table 323. OSPFv3 Configuration Commands (continued)

| Command Syntax and Usage |
|--|
| <pre>[no] nssaAsbrDfRtTrans</pre> <p>Enables or disables setting of the P-bit in the default Type 7 LSA generated by an NSSA internal ASBR. The default setting is <code>disabled</code>.</p> <p>Command mode: Router OSPF3</p> |
| <pre>enable</pre> <p>Enables OSPFv3 on the switch.</p> <p>Command mode: Router OSPF3</p> |
| <pre>no enable</pre> <p>Disables OSPFv3 on the switch.</p> <p>Command mode: Router OSPF3</p> |
| <pre>show ipv6 ospf</pre> <p>Displays the current OSPF configuration settings.</p> <p>Command mode: All</p> |

OSPFv3 Area Index Configuration

Table 324. OSPFv3 Area Index Configuration Options

| Command Syntax and Usage |
|---|
| <pre>area <area index> area-id <IP address></pre> <p>Defines the IP address of the OSPFv3 area number.</p> <p>Command mode: Router OSPF3</p> |
| <pre>area <area index> type {transit stub nssa} {no-summary}</pre> <p>Defines the type of area. For example, when a virtual link has to be established with the backbone, the area type must be defined as transit.</p> <p>Transit area: allows area summary information to be exchanged between routing devices. Any area that is not a stub area or NSSA is considered to be transit area.</p> <p>Stub area: is an area where external routing information is not distributed. Typically, a stub area is connected to only one other area.</p> <p>NSSA: Not-So-Stubby Area (NSSA) is similar to stub area with additional capabilities. For example, routes originating from within the NSSA can be propagated to adjacent transit and backbone areas. External routes from outside the Autonomous System (AS) can be advertised within the NSSA but are not distributed into other areas.</p> <p>Enables or disables the no-summary option. When enabled, the area-border router neither originates nor propagates Inter-Area-Prefix LSAs into stub/NSSA areas. Instead it generates a default Inter-Area-Prefix LSA.</p> <p>The default setting is <code>disabled</code>.</p> <p>Command mode: Router OSPF3</p> |

Table 324. OSPFv3 Area Index Configuration Options (continued)

| Command Syntax and Usage | |
|---|--|
| <pre>area <area index> default-metric <metric value (1-16777215)></pre> | <p>Configures the cost for the default summary route in a stub area or NSSA.</p> <p>Command mode: Router OSPF3</p> |
| <pre>area <area index> default-metric type <1-3></pre> | <p>Configures the default metric type applied to the route.</p> <p>This command applies only to area type of Stub/NSSA.</p> <p>Command mode: Router OSPF3</p> |
| <pre>area <area index> stability-interval <1-255></pre> | <p>Configures the stability interval for an NSSA, in seconds. When the interval expires, an elected translator determines that its services are no longer required. The default value is 40.</p> <p>Command mode: Router OSPF3</p> |
| <pre>area <area index> translation-role always candidate</pre> | <p>Configures the translation role for an NSSA area, as follows:</p> <ul style="list-style-type: none"> – Always: Type 7 LSAs are always translated into Type 5 LSAs. – Candidate: An NSSA border router participates in the translator election process. <p>The default setting is <code>candidate</code>.</p> <p>Command mode: Router OSPF3</p> |
| <pre>area <area index> enable</pre> | <p>Enables the OSPF area.</p> <p>Command mode: Router OSPF3</p> |
| <pre>area <area index> no enable</pre> | <p>Disables the OSPF area.</p> <p>Command mode: Router OSPF3</p> |
| <pre>no area <area index></pre> | <p>Deletes the OSPF area.</p> <p>Command mode: Router OSPF3</p> |
| <pre>show ipv6 ospf areas</pre> | <p>Displays the current OSPFv3 area configuration.</p> <p>Command mode: All</p> |

OSPFv3 Summary Range Configuration

Table 325. OSPFv3 Summary Range Configuration Options

| Command Syntax and Usage |
|---|
| <pre>area-range <1-16> address <IPv6 address> <prefix length (1-128)></pre> <p>Configures the base IPv6 address and subnet prefix length for the range. Command mode: Router OSPF3</p> |
| <pre>area-range <1-16> area <area index (0-2)></pre> <p>Configures the area index used by the switch. Command mode: Router OSPF3</p> |
| <pre>area-range <1-16> lsa-type summary Type7</pre> <p>Configures the LSA type, as follows:</p> <ul style="list-style-type: none"> – Summary LSA – Type7 LSA <p>Command mode: Router OSPF3</p> |
| <pre>area-range <1-16> tag <0-4294967295></pre> <p>Configures the route tag. Command mode: Router OSPF3</p> |
| <pre>[no] area-range <1-16> hide</pre> <p>Hides the OSPFv3 summary range. Command mode: Router OSPF3</p> |
| <pre>area-range <1-16> enable</pre> <p>Enables the OSPFv3 summary range. Command mode: Router OSPF3</p> |
| <pre>area-range <1-16> no enable</pre> <p>Disables the OSPFv3 summary range. Command mode: Router OSPF3</p> |
| <pre>no area-range <1-16></pre> <p>Deletes the OSPFv3 summary range. Command mode: Router OSPF3</p> |
| <pre>show ipv6 ospf area-range</pre> <p>Displays the current OSPFv3 summary range. Command mode: All</p> |

OSPFv3 AS-External Range Configuration

Table 326. OSPFv3 AS-External Range Configuration Options

| Command Syntax and Usage |
|--|
| <pre>summary-prefix <1-16> address <IPv6 address> <IPv6 prefix length (1-128)></pre> <p>Configures the base IPv6 address and the subnet prefix length for the range. Command mode: Router OSPF3</p> |
| <pre>summary-prefix <1-16> area <area index (0-2)></pre> <p>Configures the area index used by the switch. Command mode: Router OSPF3</p> |
| <pre>summary-prefix <1-16> aggregation-effect {allowAll denyAll advertise not-advertise}</pre> <p>Configures the aggregation effect, as follows:</p> <ul style="list-style-type: none"> – allowAll: If the area ID is 0.0.0.0, aggregated Type-5 LSAs are generated. Aggregated Type-7 LSAs are generated in all the attached NSSAs for the range. – denyAll: Type-5 and Type-7 LSAs are not generated. – advertise: If the area ID is 0.0.0.0, aggregated Type-5 LSAs are generated. For other area IDs, aggregated Type-7 LSAs are generated in the NSSA area. – not-advertise: If the area ID is 0.0.0.0, Type-5 LSAs are not generated, while all NSSA LSAs within the range are cleared and aggregated Type-7 LSAs are generated for all NSSAs. For other area IDs, aggregated Type-7 LSAs are not generated in the NSSA area. <p>Command mode: Router OSPF3</p> |
| <pre>[no] summary-prefix <1-16> translation</pre> <p>When enabled, the P-bit is set in the generated Type-7 LSA. When disabled, the P-bit is cleared. The default setting is disabled. Command mode: Router OSPF3</p> |
| <pre>summary-prefix <1-16> enable</pre> <p>Enables the OSPFv3 AS-external range. Command mode: Router OSPF3</p> |
| <pre>summary-prefix <1-16> no enable</pre> <p>Disables the OSPFv3 AS-external range. Command mode: Router OSPF3</p> |
| <pre>no summary-prefix <1-16></pre> <p>Deletes the OSPFv3 AS-external range. Command mode: Router OSPF3</p> |
| <pre>show ipv6 ospf summary-prefix <1-16></pre> <p>Displays the current OSPFv3 AS-external range. Command mode: All</p> |

OSPFv3 Interface Configuration

Table 327. OSPFv3 Interface Configuration Options

| Command Syntax and Usage |
|--|
| <pre>interface ip <interface number></pre> <p>Enter Interface IP mode, from Global Configuration mode. Command mode: Global configuration</p> |
| <pre>ipv6 ospf area <area index (0-2)></pre> <p>Configures the OSPFv3 area index. Command mode: Interface IP</p> |
| <pre>[no] ipsec dynamic-policy <I-10></pre> <p>Adds an IP security dynamic policy to the OSPFv3 interface. Command mode: Interface IP</p> |
| <pre>ipsec manual-policy <I-10></pre> <p>Adds an IP security manual policy to the OSPFv3 interface. Command mode: Interface IP</p> |
| <pre>ipv6 ospf area <area index (0-2)> instance <0-255></pre> <p>Configures the instance ID for the interface. Command mode: Interface IP</p> |
| <pre>[no] ipv6 ospf priority <priority value (0-255)></pre> <p>Configures the priority value for the switch's OSPFv3 interface. A priority value of 255 is the highest and 1 is the lowest. A priority value of 0 specifies that the interface cannot be used as Designated Router (DR). Command mode: Interface IP</p> |
| <pre>[no] ipv6 ospf cost <I-65535></pre> <p>Configures the metric value for sending a packet on the interface. Command mode: Interface IP</p> |
| <pre>[no] ipv6 ospf hello-interval <I-65535></pre> <p>Configures the indicated interval, in seconds, between the hello packets, that the router sends on the interface. Command mode: Interface IP</p> |
| <pre>[no] ipv6 ospf linklsasuppress</pre> <p>Enables or disables Link LSA suppression. When suppressed, no Link LSAs are originated. Default setting is disabled. Command mode: Interface IP</p> |

Table 327. OSPFv3 Interface Configuration Options (continued)

| Command Syntax and Usage | |
|--|--|
| <pre>ipv6 ospf network {broadcast non-broadcast point-to-multipoint point-to-point}</pre> | <p>Configures the network type for the OSPFv3 interface:</p> <ul style="list-style-type: none"> – broadcast: network where all routers use the broadcast capability – non-broadcast: non-broadcast multiple access (NBMA) network supporting pseudo-broadcast (multicast and broadcast traffic is configured manually) – point-to-multipoint: network where multiple point-to-point links are set up on the same interface – point-to-point: network that joins a single pair of routers <p>The default value is broadcast.</p> <p>Command mode: Interface IP</p> |
| <pre>ipv6 ospf poll-interval <0-4294967295></pre> | <p>Configures the poll interval in seconds for neighbors in NBMA networks. Default value is 120.</p> <p>Command mode: Interface IP</p> |
| <pre>no ipv6 ospf poll-interval</pre> | <p>Configures the poll interval in seconds for neighbors in NBMA and point-to-multipoint networks to its default 120 seconds value.</p> <p>Command mode: Interface IP</p> |
| <pre>[no] ipv6 ospf dead-interval <1-65535></pre> | <p>Configures the health parameters of a hello packet, in seconds, before declaring a silent router to be down.</p> <p>Command mode: Interface IP</p> |
| <pre>[no] ipv6 ospf transmit-delay <1-1800></pre> | <p>Configures the estimated time, in seconds, taken to transmit LS update packet over this interface.</p> <p>Command mode: Interface IP</p> |
| <pre>[no] ipv6 ospf retransmit-interval <1-1800></pre> | <p>Configures the interval in seconds, between LSA retransmissions for adjacencies belonging to interface.</p> <p>Command mode: Interface IP</p> |
| <pre>[no] ipv6 ospf passive-interface</pre> | <p>Enables or disables the <code>passive</code> setting on the interface. On a passive interface, OSPFv3 protocol packets are suppressed.</p> <p>Command mode: Interface IP</p> |
| <pre>ipv6 ospf enable</pre> | <p>Enables OSPFv3 on the interface.</p> <p>Command mode: Interface IP</p> |

Table 327. OSPFv3 Interface Configuration Options (continued)

| Command Syntax and Usage |
|--|
| <pre>ipv6 ospf no enable</pre> <p>Disables OSPFv3 on the interface. Command mode: Interface IP</p> |
| <pre>no ipv6 ospf</pre> <p>Deletes OSPFv3 from interface. Command mode: Interface IP</p> |
| <pre>show ipv6 ospf interface</pre> <p>Displays the current settings for OSPFv3 interface. Command mode: Interface IP</p> |

OSPFv3 over IPsec Configuration

The following table describes the OSPFv3 over IPsec Configuration commands.

Table 328. Layer 3 IPsec Configuration Options

| Command Syntax and Usage |
|--|
| <pre>ipv6 ospf authentication ipsec spi <256-4294967295> {md5 sha1} <authentication key (hexadecimal)></pre> <p>Configures the Security Parameters Index (SPI), algorithm, and authentication key for the Authentication Header (AH). The algorithms supported are:</p> <ul style="list-style-type: none"> – MD5 (hexadecimal key length is 32) – SHA1 (hexadecimal key length is 40) <p>Command mode: Interface IP</p> |
| <pre>[no] ipv6 ospf authentication ipsec enable</pre> <p>Enables or disables IPsec. Command mode: Interface IP</p> |
| <pre>no ipv6 ospf authentication ipsec spi <256-4294967295></pre> <p>Disables the specified Authentication Header (AH) SPI. Command mode: Interface IP</p> |
| <pre>ipv6 ospf authentication ipsec default</pre> <p>Resets the Authentication Header (AH) configuration to default values. Command mode: Interface IP</p> |

Table 328. Layer 3 IPsec Configuration Options (continued)

| Command Syntax and Usage | |
|--|---|
| <pre>ipv6 ospf encryption ipsec spi <256-4294967295> esp {3des aes-cbc des null} <encryption key (hexadecimal)>[null] {md5 sha1 none} <authentication key (hexadecimal)></pre> | <p>Configures the Security Parameters Index (SPI), encryption algorithm, authentication algorithm, and authentication key for the Encapsulating Security Payload (ESP). The ESP algorithms supported are:</p> <ul style="list-style-type: none"> – 3DES (hexadecimal key length is 48) – AES-CBC (hexadecimal key length is 32) – DES (hexadecimal key length is 16) <p>The authentication algorithms supported are:</p> <ul style="list-style-type: none"> – MD5 (hexadecimal key length is 32) – SHA1 (hexadecimal key length is 40) – none <p>Note: If the encryption algorithm is null, the authentication algorithm must be either MD5 or SHA1. (hexadecimal key length is 40). If an encryption algorithm is specified (3DES, AES-CBC, or DES), the authentication algorithm can be none.</p> <p>Command mode: Interface IP</p> |
| <pre>ipv6 ospf encryption ipsec enable</pre> | <p>Enables OSPFv3 encryption for this interface.</p> <p>Command mode: Interface IP</p> |
| <pre>no ipv6 ospf encryption ipsec spi <256-4294967295></pre> | <p>Disables the specified Encapsulating Security Payload (ESP) SPI.</p> <p>Command mode: Interface IP</p> |
| <pre>ipv6 ospf encryption ipsec default</pre> | <p>Resets the Encapsulating Security Payload (ESP) configuration to default values.</p> <p>Command mode: Interface IP</p> |

OSPFv3 Virtual Link Configuration

Table 329. OSPFv3 Virtual Link Configuration Options

| Command Syntax and Usage | |
|--|---|
| area-virtual-link <I-3> area <area index (0-2)> | Configures the OSPF area index. Command mode: Router OSPF3 |
| area-virtual-link <I-3> hello-interval <I-65535> | Configures the indicated interval, in seconds, between the hello packets, that the router sends on the interface. Command mode: Router OSPF3 |
| area-virtual-link <I-3> dead-interval <I-65535> | Configures the time period, in seconds, for which the router waits for hello packet from the neighbor before declaring this neighbor down. Command mode: Router OSPF3 |
| area-virtual-link <I-3> transmit-delay <I-1800> | Configures the estimated time, in seconds, taken to transmit LS update packet over this interface. Command mode: Router OSPF3 |
| area-virtual-link <I-3> retransmit-interval <I-1800> | Configures the interval, in seconds, between link-state advertisement (LSA) retransmissions for adjacencies belonging to the OSPFv3 virtual link interface. The default value is five seconds. Command mode: Router OSPF3 |
| area-virtual-link <I-3> neighbor-router <NBR router ID (IP address)> | Configures the router ID of the virtual neighbor. The default setting is 0.0.0.0 Command mode: Router OSPF3 |
| area-virtual-link <I-3> enable | Enables OSPF virtual link. Command mode: Router OSPF3 |
| area-virtual-link <I-3> no enable | Disables OSPF virtual link. Command mode: Router OSPF3 |
| no area-virtual-link <I-3> | Deletes OSPF virtual link. Command mode: Router OSPF3 |
| show ipv6 ospf area-virtual-link | Displays the current OSPFv3 virtual link settings. Command mode: All |

OSPFv3 Host Entry Configuration

Table 330. OSPFv3 Host Entry Configuration Options

| Command Syntax and Usage | |
|--|---|
| <pre>host <1-128> address <IPv6 address> <prefix length (1-128)></pre> | <p>Configures the base IPv6 address and the subnet prefix length for the host entry.</p> <p>Command mode: Router OSPF3</p> |
| <pre>host <1-128> area <area index (0-2)></pre> | <p>Configures the area index of the host.</p> <p>Command mode: Router OSPF3</p> |
| <pre>host <1-128> cost <1-65535></pre> | <p>Configures the cost value of the host.</p> <p>Command mode: Router OSPF3</p> |
| <pre>host <1-128> enable</pre> | <p>Enables the host entry.</p> <p>Command mode: Router OSPF3</p> |
| <pre>no host <1-128> enable</pre> | <p>Disables the host entry.</p> <p>Command mode: Router OSPF3</p> |
| <pre>no host <1-128></pre> | <p>Deletes the host entry.</p> <p>Command mode: Router OSPF3</p> |
| <pre>show ipv6 ospf host [<1-128>]</pre> | <p>Displays the current OSPFv3 host entries.</p> <p>Command mode: All</p> |

OSPFv3 Redist Entry Configuration

Table 331. OSPFv3 Redist Entry Configuration Options

| Command Syntax and Usage |
|--|
| <pre>redist-config <1-128> address <IPv6 address> <IPv6 prefix length (1-128)></pre> <p>Configures the base IPv6 address and the subnet prefix length for the redistribution entry.</p> <p>Command mode: Router OSPF3</p> |
| <pre>redist-config <1-128> metric-value <1-16777215></pre> <p>Configures the route metric value applied to the route before it is advertised into the OSPFv3 domain.</p> <p>Command mode: Router OSPF3</p> |
| <pre>redist-config <1-128> metric-type asExtttype1 asExtttype2</pre> <p>Configures the metric type applied to the route before it is advertised into the OSPFv3 domain.</p> <p>Command mode: Router OSPF3</p> |
| <pre>[no] redist-config <1-128> tag <0-4294967295></pre> <p>Configures the route tag.</p> <p>Command mode: Router OSPF3</p> |
| <pre>redist-config <1-128> enable</pre> <p>Enables the OSPFv3 redistribution entry.</p> <p>Command mode: Router OSPF3</p> |
| <pre>no redist-config <1-128> enable</pre> <p>Disables the OSPFv3 redistribution entry.</p> <p>Command mode: Router OSPF3</p> |
| <pre>no redist-config <1-128></pre> <p>Deletes the OSPFv3 redistribution entry.</p> <p>Command mode: Router OSPF3</p> |
| <pre>show ipv6 ospf redist-config</pre> <p>Displays the current OSPFv3 redistribution configuration entries.</p> <p>Command mode: Router OSPF3</p> |

OSPFv3 Redistribute Configuration

Table 332. OSPFv3 Redistribute Configuration Options

| Command Syntax and Usage |
|---|
| <pre>[no] redistribute {connected static} export <metric value (1-16777215)> <metric type (1-2)> <tag (0-4294967295)></pre> <p>Exports the routes of this protocol as external OSPFv3 AS-external LSAs in which the metric, metric type, and route tag are specified. To remove a previous configuration and stop exporting the routes of the protocol, use the <code>no</code> form of the command.</p> <p>Command mode: Router OSPF3</p> |
| <pre>show ipv6 ospf</pre> <p>Displays the current OSPFv3 route redistribution settings.</p> <p>Command mode: All</p> |

IP Loopback Interface Configuration

An IP loopback interface is not connected to any physical port. A loopback interface is always accessible over the network.

Table 333. IP Loopback Interface Commands

| Command Syntax and Usage |
|---|
| <pre>interface loopback <I-5></pre> <p>Enter Interface Loopback mode. Command mode: Global configuration</p> |
| <pre>no interface loopback <I-5></pre> <p>Deletes the selected loopback interface. Command mode: Global configuration</p> |
| <pre>ip address <IP address></pre> <p>Defines the loopback interface IP address. Command mode: Interface loopback</p> |
| <pre>ip netmask <subnet mask></pre> <p>Defines the loopback interface subnet mask. Command mode: Interface loopback</p> |
| <pre>ip ospf area <area number></pre> <p>Configures the OSPF area index used by the loopback interface. Command mode: Interface loopback</p> |
| <pre>[no] ip ospf enable</pre> <p>Enables or disables OSPF for the loopback interface. Command mode: Interface loopback</p> |
| <pre>enable</pre> <p>Enables the loopback interface. Command mode: Interface loopback</p> |
| <pre>no enable</pre> <p>Disables the loopback interface. Command mode: Interface loopback</p> |
| <pre>show interface loopback <I-5></pre> <p>Displays the current IP loopback interface parameters. Command mode: All</p> |

Converged Enhanced Ethernet Configuration

Table 334 describes the Converged Enhanced Ethernet (CEE) configuration commands.

Table 334. CEE Commands

| Command Syntax and Usage |
|---|
| <code>cee enable</code> Globally turns CEE on. Command mode: Global configuration |
| <code>no cee enable</code> Globally turns CEE off. Command mode: Global configuration |
| <code>cee iscsi enable</code> Enables or disables ISCSI TLV advertisements. Command mode: Global configuration |
| <code>show cee iscsi</code> Displays the current ISCSI TLV parameters. Command mode: All |
| <code>show cee</code> Displays the current CEE parameters. Command mode: All |

ETS Global Configuration

Enhanced Transmission Selection (ETS) allows you to allocate bandwidth to different traffic types, based on 802.1p priority.

Note: ETS configuration supersedes the QoS 802.1p menu. When ETS is enabled, you cannot configure the 802.1p menu options.

ETS Global Priority Group Configuration

[Table 335](#) describes the global ETS Priority Group configuration options.

Table 335. Global ETS Priority Group Commands

| Command Syntax and Usage |
|---|
| <pre>cee global ets priority-group pgid <0-7, 15> bandwidth <802.1p priority (0-7)> <bandwidth percentage (0, 10-100)></pre> <p>Allows you to configure Priority Group parameters. You can enter the link bandwidth percentage allocated to the Priority Group, and also assign one or more 802.1p values to the Priority Group.</p> <p>Command mode: Global configuration</p> |
| <pre>cee global ets priority-group pgid <0-7, 15> description <1-31 characters></pre> <p>Enter text that describes this Priority Group.</p> <p>Command mode: Global configuration</p> |
| <pre>no cee global ets priority-group <0-7, 15> description</pre> <p>Removes the description for the specified Priority Group.</p> <p>Command mode: Global configuration</p> |
| <pre>[no] cee global ets mcast-priority-group mcpgid <0-3> [bandwidth percentage <0, 10-100>] [priority <0-7>]</pre> <p>Configures Multicast Priority Group parameters. You can enter the link bandwidth percentage allocated to the Multicast Priority Group, and assign one or more 802.1p values to the Multicast Priority Group.</p> <p>Command mode: Global configuration</p> |
| <pre>cee global ets mcast-priority-group mcpgid <0-3> description <1-31 characters></pre> <p>Enter text that describes the multicast priority group.</p> <p>Command mode: Global configuration</p> |
| <pre>no cee global ets mcast-priority-group mcpgid <0-3> description</pre> <p>Removes the description for the specified multicast priority group.</p> <p>Command mode: Global configuration</p> |
| <pre>cee global ets priority-group pgid <0-7, 15> priority <0-7></pre> <p>Adds one or more 802.1p priority values to the Priority Group. Enter one value per line, null to end.</p> <p>Command mode: Global configuration</p> |

Table 335. Global ETS Priority Group Commands

| Command Syntax and Usage |
|---|
| <pre>show cee global ets priority-group <0-7, 15></pre> <p>Displays the current global ETS Priority Group parameters.</p> <p>Command mode: All</p> |
| <pre>show cee global ets</pre> <p>Displays the current global ETS Priority Group parameters.</p> <p>Command mode: All</p> |
| <pre>show cee global ets mcast-priority-group <0-3></pre> <p>Displays the current global ETS Multicast Priority Group parameters.</p> <p>Command mode: All</p> |

Priority Flow Control Configuration

Priority-based Flow Control (PFC) enhances flow control by allowing the switch to pause traffic based on its 802.1p priority value, while allowing traffic at other priority levels to continue.

Port-level 802.1p PFC Configuration

Table 336 describes the 802.1p Priority Flow Control (PFC) configuration options for the selected port.

Table 336. Port 802.1p PFC Options

| Command Syntax and Usage |
|--|
| <pre>cee port <port alias or number> pfc enable</pre> <p>Enables Priority Flow Control on the selected port.</p> <p>Command mode: Global configuration</p> |
| <pre>no cee port <port alias or number> pfc enable</pre> <p>Disables Priority Flow Control on the selected port.</p> <p>Command mode: Global configuration</p> |
| <pre>cee port <port alias or number> pfc priority <0-7> enable</pre> <p>Enables Priority Flow Control on the selected 802.1p priority.</p> <p>Note: PFC can be enabled on 802.1p priority 3 and one other priority only.</p> <p>Command mode: Global configuration</p> |
| <pre>no cee port <port alias or number> pfc priority <0-7> enable</pre> <p>Disables Priority Flow Control on the selected 802.1p priority.</p> <p>Command mode: Global configuration</p> |
| <pre>[no] cee port <port alias or number> pfc priority <0-7> description <1-31 characters></pre> <p>Enter text to describe the priority value.</p> <p>Command mode: Global configuration</p> |

Table 336. Port 802.1p PFC Options (continued)

| Command Syntax and Usage |
|---|
| <pre>show cee port <port alias or number> pfc priority <0-7></pre> <p>Displays the current 802.1p PFC parameters for the selected port.</p> <p>Command mode: All</p> |
| <pre>show cee port <port alias or number> pfc</pre> <p>Displays the current PFC parameters for the selected port.</p> <p>Command mode: All</p> |

DCBX Port Configuration

[Table 337](#) describes the port DCB Capability Exchange Protocol (DCBX) configuration options.

Table 337. Port DCBX Commands

| Command Syntax and Usage |
|---|
| <pre>[no] cee port <port alias or number> dcbx app_proto advertise</pre> <p>Enables or disables DCBX Application Protocol advertisements of configuration data. When enabled, the Advertisement flag is set to 1 (advertise data to the peer device).</p> <p>Command mode: Global configuration</p> |
| <pre>[no] cee port <port alias or number> dcbx app_proto willing</pre> <p>Enables or disables Application Protocol willingness to accept configuration data from the peer device. When enabled, the Willing flag is set to 1 (willing to accept data).</p> <p>Command mode: Global configuration</p> |
| <pre>[no] cee port <port alias or number> dcbx ets advertise</pre> <p>Enables or disables DCBX ETS advertisements of configuration data. When enabled, the Advertisement flag is set to 1 (advertise data to the peer device).</p> <p>Command mode: Global configuration</p> |
| <pre>[no] cee port <port alias or number> dcbx ets willing</pre> <p>Enables or disables ETS willingness to accept configuration data from the peer device. When enabled, the Willing flag is set to 1 (willing to accept data).</p> <p>Command mode: Global configuration</p> |
| <pre>[no] cee port <port alias or number> dcbx pfc advertise</pre> <p>Enables or disables DCBX PFC advertisements of configuration data. When enabled, the Advertisement flag is set to 1 (advertise data to the peer device).</p> <p>Command mode: Global configuration</p> |
| <pre>[no] cee port <port alias or number> dcbx pfc willing</pre> <p>Enables or disables PFC willingness to accept configuration data from the peer device. When enabled, the Willing flag is set to 1 (willing to accept data).</p> <p>Command mode: Global configuration</p> |

Table 337. Port DCBX Commands (continued)

| Command Syntax and Usage |
|---|
| <pre>no cee port <port alias or number> dcbx enable</pre> <p>Disables DCBX on the port. Command mode: Global configuration</p> |
| <pre>cee port <port alias or number> dcbx enable</pre> <p>Enables DCBX on the port. Command mode: Global configuration</p> |
| <pre>show cee port <port alias or number> dcbx</pre> <p>Displays the current port DCBX parameters. Command mode: All</p> |

Fibre Channel over Ethernet Configuration

Fibre Channel over Ethernet (FCoE) transports Fibre Channel frames over an Ethernet fabric. The CEE features and FCoE features allow you to create a lossless Ethernet transport mechanism.

Note: On EN4093 models, FCoE is not supported in stacking mode.

[Table 338](#) describes the FCoE configuration options.

Table 338. FCoE Configuration Commands

| Command Syntax and Usage |
|---|
| <pre>fcoe fips enable</pre> <p>Globally turns FIP Snooping on.</p> <p>Command mode: Global configuration</p> |
| <pre>no fcoe fips enable</pre> <p>Globally turns FIP Snooping off.</p> <p>Command mode: Global configuration</p> |
| <pre>[no] fcoe fips timeout-acl</pre> <p>Enables or disables ACL time-out removal. When enabled, ACLs associated with expired FCFs and FCoE connections are removed from the system.</p> <p>Command mode: Global configuration</p> |
| <pre>[no] fcoe fips automatic-vlan</pre> <p>Enables or disables automatic VLAN creation, based on response received from the connected device.</p> <p>Command mode: Global configuration</p> |
| <pre>show fcoe information</pre> <p>Displays the current FCoE parameters.</p> <p>Command mode: All</p> |

FIPS Port Configuration

FIP Snooping allows the switch to monitor FCoE Initialization Protocol (FIP) frames to gather discovery, initialization, and maintenance data. This data is used to automatically configure ACLs that provide FCoE connections and data security.

[Table 339](#) describes the port Fibre Channel over Ethernet Initialization Protocol (FIP) Snooping configuration options.

Table 339. Port FIP Snooping Commands

| Command Syntax and Usage |
|---|
| <pre>fcoe fips port <port alias or number> fcf-mode [auto on off]</pre> <p>Configures FCoE Forwarding (FCF) on the port, as follows:</p> <ul style="list-style-type: none">– on: Configures the port as a Fibre Channel Forwarding (FCF) port.– off: Configures the port as an FCoE node (ENode).– auto: Automatically detect the configuration of the connected device, and configure this port to match. <p>Command mode: Global configuration</p> |
| <pre>fcoe fips port <port alias or number> enable</pre> <p>Enables FIP Snooping on the port. The default setting is enabled.</p> <p>Note: If IPv6 ACLs are assigned to the port, you cannot enable FCoE.</p> <p>Command mode: Global configuration</p> |
| <pre>no fcoe fips port <port alias or number> enable</pre> <p>Disables FIP Snooping on the port.</p> <p>Command mode: Global configuration</p> |

Remote Monitoring Configuration

Remote Monitoring (RMON) allows you to monitor traffic flowing through the switch. The RMON MIB is described in RFC 1757.

The following sections describe the Remote Monitoring (RMON) configuration options.

- [“RMON History Configuration” on page 468](#)
- [“RMON Event Configuration” on page 469](#)
- [“RMON Alarm Configuration” on page 470](#)

RMON History Configuration

[Table 340](#) describes the RMON History commands.

Table 340. RMON History Commands

| Command Syntax and Usage |
|---|
| <pre>rmon history <1-65535> interface-oid <1-127 characters></pre> <p>Configures the interface MIB Object Identifier. The IFOID must correspond to the standard interface OID, as follows:</p> <pre>1.3.6.1.2.1.2.2.1.1.x</pre> <p>where x is the ifIndex</p> <p>Command mode: Global configuration</p> |
| <pre>rmon history <1-65535> requested-buckets <1-65535></pre> <p>Configures the requested number of buckets, which is the number of discrete time intervals over which data is to be saved. The default value is 30.</p> <p>The maximum number of buckets that can be granted is 50.</p> <p>Command mode: Global configuration</p> |
| <pre>rmon history <1-65535> polling-interval <1-3600></pre> <p>Configures the time interval over which the data is sampled for each bucket.</p> <p>The default value is 1800.</p> <p>Command mode: Global configuration</p> |
| <pre>rmon history <1-65535> owner <1-127 characters></pre> <p>Enter a text string that identifies the person or entity that uses this History index.</p> <p>Command mode: Global configuration</p> |
| <pre>no rmon history <1-65535></pre> <p>Deletes the selected History index.</p> <p>Command mode: Global configuration</p> |
| <pre>show rmon history</pre> <p>Displays the current RMON History parameters.</p> <p>Command mode: All</p> |

RMON Event Configuration

Table 341 describes the RMON Event commands.

Table 341. RMON Event Commands

| Command Syntax and Usage |
|---|
| <pre>rmon event <1-65535> description <1-127 characters></pre> <p>Enter a text string to describe the event. Command mode: Global configuration</p> |
| <pre>[no] rmon event <1-65535> type log trap both</pre> <p>Selects the type of notification provided for this event. For log events, an entry is made in the log table and sent to the configured syslog host. For trap events, an SNMP trap is sent to the management station. Command mode: Global configuration</p> |
| <pre>rmon event <1-65535> owner <1-127 characters></pre> <p>Enter a text string that identifies the person or entity that uses this event index. Command mode: Global configuration</p> |
| <pre>no rmon event <1-65535></pre> <p>Deletes the selected RMON Event index. Command mode: Global configuration</p> |
| <pre>show rmon event</pre> <p>Displays the current RMON Event parameters. Command mode: All</p> |

RMON Alarm Configuration

The Alarm RMON group can track rising or falling values for a MIB object. The MIB object must be a counter, gauge, integer, or time interval. Each alarm index must correspond to an event index that triggers once the alarm threshold is crossed.

[Table 342](#) describes the RMON Alarm commands.

Table 342. RMON Alarm Commands

| Command Syntax and Usage |
|---|
| <pre>rmon alarm <1-65535> oid <1-127 characters></pre> <p>Configures an alarm MIB Object Identifier.</p> <p>Command mode: Global configuration</p> |
| <pre>rmon alarm <1-65535> interval <1-65535></pre> <p>Configures the time interval over which data is sampled and compared with the rising and falling thresholds. The default value is 1800.</p> <p>Command mode: Global configuration</p> |
| <pre>rmon alarm <1-65535> sample abs delta</pre> <p>Configures the method of sampling the selected variable and calculating the value to be compared against the thresholds, as follows:</p> <ul style="list-style-type: none"> – <code>abs</code>—absolute value, the value of the selected variable is compared directly with the thresholds at the end of the sampling interval. – <code>delta</code>—delta value, the value of the selected variable at the last sample is subtracted from the current value, and the difference compared with the thresholds. <p>Command mode: Global configuration</p> |
| <pre>rmon alarm <1-65535> alarm-type rising falling either</pre> <p>Configures the alarm type as rising, falling, or either (rising or falling).</p> <p>Command mode: Global configuration</p> |
| <pre>rmon alarm <1-65535> rising-limit <-2147483647 - 2147483647></pre> <p>Configures the rising threshold for the sampled statistic. When the current sampled value is greater than or equal to this threshold, and the value at the last sampling interval was less than this threshold, a single event is generated.</p> <p>Command mode: Global configuration</p> |
| <pre>rmon alarm <1-65535> falling-limit <-2147483647 - 2147483647></pre> <p>Configures the falling threshold for the sampled statistic. When the current sampled value is less than or equal to this threshold, and the value at the last sampling interval was greater than this threshold, a single event is generated.</p> <p>Command mode: Global configuration</p> |
| <pre>rmon alarm <1-65535> rising-crossing-index <1-65535></pre> <p>Configures the rising alarm event index that is triggered when a rising threshold is crossed.</p> <p>Command mode: Global configuration</p> |

Table 342. RMON Alarm Commands (continued)

| Command Syntax and Usage | |
|--|---|
| <pre>rmon alarm <1-65535> falling-crossing-index <1-65535></pre> | <p>Configures the falling alarm event index that is triggered when a falling threshold is crossed.</p> <p>Command mode: Global configuration</p> |
| <pre>rmon alarm <1-65535> owner <1-127 characters></pre> | <p>Enter a text string that identifies the person or entity that uses this alarm index.</p> <p>Command mode: Global configuration</p> |
| <pre>no rmon alarm <1-65535></pre> | <p>Deletes the selected RMON Alarm index.</p> <p>Command mode: Global configuration</p> |
| <pre>show rmon alarm</pre> | <p>Displays the current RMON Alarm parameters.</p> <p>Command mode: All</p> |

Virtualization Configuration

Table 343 describes the virtualization configuration options.

Table 343. Virtualization Configurations Options

| Command Syntax and Usage |
|--|
| <pre>virt enable</pre> <p>Enables VMready.</p> <p>Command mode: Global configuration</p> |
| <pre>no virt enable</pre> <p>Disables VMready.</p> <p>Note: This command deletes all configured VM groups.</p> <p>Command mode: Global configuration</p> |
| <pre>show virt</pre> <p>Displays the current virtualization parameters.</p> <p>Command mode: All</p> |

VM Policy Bandwidth Management

Table 344 describes the bandwidth management options for the selected VM. Use these commands to limit the bandwidth used by each VM.

Table 344. VM Bandwidth Management Options

| Command Syntax and Usage |
|--|
| <pre>virt vmpolicy vmbwidth [<MAC address> <UUID> <name> <IP address> <index number>] txrate <64-10000000> <max. burst (32-4096)> <ACL number></pre> <p>The first value configures Committed Rate—the amount of bandwidth available to traffic transmitted from the VM to the switch, in kilobits per second. Enter the value in multiples of 64.</p> <p>The second values configures the maximum burst size, in kilobits. Enter one of the following values: 32, 64, 128, 256, 512, 1024, 2048, 4096.</p> <p>The third value represents the ACL assigned to the transmission rate. The ACL is automatically, in sequential order, if not specified by the user. If there are no available ACLs, the TXrate cannot be configured. Each TXrate configuration reduces the number of available ACLs by one.</p> <p>Command mode: Global configuration</p> |
| <pre>virt vmpolicy vmbwidth [<MAC address> <UUID> <name> <IP address> <index number>] rxrate <64-10000000></pre> <p>The first value configures Committed Rate—the amount of bandwidth available to traffic transmitted from the switch to the VM, in kilobits per second. Enter the value in multiples of 64.</p> <p>The second values configures the maximum burst size, in kilobits. Enter one of the following values: 32, 64, 128, 256, 512, 1024, 2048, 4096.</p> <p>Command mode: Global configuration</p> |

Table 344. VM Bandwidth Management Options (continued)

| Command Syntax and Usage |
|---|
| <pre>[no] virt vmpolicy vmbwidth [<MAC address> <UUID> <name> <IP address> <index number>] bwctrl</pre> <p>Enables or disables bandwidth control on the VM policy.</p> <p>Command mode: Global configuration</p> |
| <pre>[no] virt vmpolicy vmbwidth [<MAC address> <UUID> <name> <IP address> <index number>]</pre> <p>Deletes the bandwidth management settings from this VM policy.</p> <p>Command mode: Global configuration</p> |
| <pre>show virt vmpolicy vmbandwidth [<MAC address> <UUID> <name> <IP address> <index number>]</pre> <p>Displays the current VM bandwidth management parameters.</p> <p>Command mode: All</p> |

Virtual NIC Configuration

Table 345 describes the Virtual NIC (vNIC) configuration options.

Table 345. Virtual NIC options

| Command Syntax and Usage |
|--|
| <pre>vnic enable</pre> <p>Globally turns vNIC on.</p> <p>Command mode: Global configuration</p> |
| <pre>no vnic enable</pre> <p>Globally turns vNIC off.</p> <p>Command mode: Global configuration</p> |
| <pre>[no] vnic egress-bw-meter</pre> <p>Enables or disables vNIC bandwidth metering. When enabled, any bandwidth which is not used by the vNIC to which it is allocated is shared with other vNICs. In all cases, the configured values for minimum bandwidth are honored. Only the excess bandwidth is shared.</p> <p>Command mode: Global configuration</p> |
| <pre>[no] vnic uplink-share</pre> <p>Enable or disable vNIC shared mode. When enabled, multiple vNIC groups can be assigned to the same uplink port.</p> <p>Command mode: Global configuration</p> |
| <pre>show vnic</pre> <p>Displays the current vNIC parameters.</p> <p>Command mode: All</p> |

vNIC Port Configuration

Table 346 describes the Virtual NIC (vNIC) port configuration options.

Table 346. vNIC Port Commands

| Command Syntax and Usage |
|---|
| <pre>vnic port <port alias or number> index <1-4></pre> <p>Enters vNIC Configuration mode.</p> <p>Note: This command is valid for internal server ports only.</p> <p>Command mode: Global configuration</p> |
| <pre>bandwidth <1-100></pre> <p>Configures the maximum bandwidth allocated to this vNIC, in increments of 100 Mbps. For example:</p> <ul style="list-style-type: none">– 1 = 100 Mbps– 10 = 1000 Mbps <p>Command mode: vNIC configuration</p> |
| <pre>enable</pre> <p>Enables the vNIC.</p> <p>Command mode: vNIC configuration</p> |
| <pre>no enable</pre> <p>Disables the vNIC.</p> <p>Command mode: vNIC configuration</p> |

Virtual NIC Group Configuration

Table 347 describes the Virtual NIC (vNIC) Group configuration options.

Table 347. vNIC Group Commands

| Command Syntax and Usage |
|---|
| <pre>vnic vnicgroup <1-32></pre> <p>Enters vNIC Group Configuration mode.</p> <p>Command mode: Global Configuration</p> |
| <pre>vlan <VLAN number></pre> <p>Assigns a VLAN to the vNIC Group.</p> <p>Command mode: vNIC Group configuration</p> |
| <pre>[no] key <LACP key></pre> <p>Adds or removes the selected LACP trunk group from the vNIC Group.</p> <p>Command mode: vNIC Group configuration</p> |

Table 347. vNIC Group Commands (continued)

| Command Syntax and Usage | |
|--------------------------------|--|
| [no] failover | <p>Enables or disables uplink failover for the vNIC Group. Uplink Failover for the vNIC Group will disable all vNIC and non-vNIC ports in the group. Other port functions continue to operate normally.</p> <p>The default setting is disabled.</p> <p>Command mode: vNIC Group configuration</p> |
| member <vNIC number> | <p>Adds a vNIC to the vNIC Group. The vNIC ID is comprised of the port number and the vNIC number. For example: 1.1</p> <p>Command mode: vNIC Group configuration</p> |
| no member <vNIC number> | <p>Removes the selected vNIC from the vNIC Group.</p> <p>Command mode: vNIC Group configuration</p> |
| port <port number or alias> | <p>Adds the non-vNIC port or uplink port to the vNIC Group.</p> <p>Command mode: vNIC Group configuration</p> |
| no port <port number or alias> | <p>Removes the non-vNIC port or uplink port from the vNIC Group.</p> <p>Command mode: vNIC Group configuration</p> |
| trunk <trunk number> | <p>Adds the uplink trunk group to the vNIC Group.</p> <p>Command mode: vNIC Group configuration</p> |
| no trunk <trunk number> | <p>Removes the uplink trunk group from the vNIC Group.</p> <p>Command mode: vNIC Group configuration</p> |
| key <trunk number> | <p>Adds the uplink LACP trunk to the vNIC Group.</p> <p>Command mode: vNIC Group configuration</p> |
| no key <trunk number> | <p>Removes the uplink LACP trunk from the vNIC Group.</p> <p>Command mode: vNIC Group configuration</p> |
| enable | <p>Enables the vNIC Group.</p> <p>Command mode: vNIC Group configuration</p> |
| no enable | <p>Disables the vNIC Group.</p> <p>Command mode: vNIC Group configuration</p> |

Table 347. vNIC Group Commands (continued)

| Command Syntax and Usage |
|--|
| <pre>no vnic vnicgroup <1-32></pre> <p>Deletes the selected vNIC Group. Command mode: Global configuration</p> |
| <pre>show vnicgroup</pre> <p>Displays the current vNIC Group parameters. Command mode: All</p> |

UFP Configuration

Table 348 describes the Unified Fabric Port (UFP) configuration options. UFP allows defining up to 4 virtual ports per physical port. Each virtual port can be set up to operate in a specific mode (access, trunk, tunnel, FCoE) and within predefined bandwidth limits.

Note: vNIC and UFP are mutually exclusive. Only one of them can be globally enabled at any point in time.

Table 348. UFP Commands

| Command Syntax and Usage |
|--|
| <pre>[no] ufp enable</pre> <p>Globally enables or disables UFP. Command mode: Global configuration</p> |
| <pre>[no] ufp port <port_no.> enable</pre> <p>Enables or disables UFP on the specified physical ports. Command mode: Global configuration</p> |
| <pre>ufp port <port_no.> vport <1-4></pre> <p>Enters UFP Virtual Port Configuration mode. Command mode: Global configuration</p> |
| <pre>no ufp port <port_no.> [vport <1-4>]</pre> <p>Disables UFP settings on the specified physical or virtual port. Command mode: Global configuration</p> |
| <pre>[no] enable</pre> <p>Enables or disables the virtual port. Command mode: UFP Virtual Port Configuration</p> |

Table 348. UFP Commands (continued)

| Command Syntax and Usage |
|---|
| <pre>network {mode [access trunk tunnel fcoe auto] default-vlan <2-4094> default-tag}</pre> <p>Configures the virtual port network configuration settings:</p> <ul style="list-style-type: none"> – mode configures the virtual port's operating mode: <ul style="list-style-type: none"> • access allows the virtual port to associate only with the default customer VLAN, as defined by the default-vlan option. • trunk allows the virtual port to associate with up to 32 customer VLANs. • tunnel makes the virtual port VLAN agnostic. This is the default setting. • fcoe configures the virtual port to carry Fibre Channel over Ethernet traffic when linked to a Fibre Channel virtual Host Bus Adapter. Setting a virtual port in fcoe mode enables Priority Flow Control on the physical port. • auto chooses the operating mode automatically – default-vlan configures the default VLAN ID for the virtual port. The default value is automatically assigned (408x, where x is the SPAR ID). This option provides an override if conflicts arise with a customer VLAN ID on the upstream network. – default-tag enables tagging egress frames with the default VLAN ID when the virtual port is in access or trunk mode and default-vlan is defined. Default setting is disabled. <p>Note: VLANs 4002-4005 cannot be used as customer VLANs</p> <p>Note: A customer VLAN cannot be configured on multiple virtual ports of the same physical port.</p> <p>Command mode: UFP Virtual Port Configuration</p> |
| <pre>no network default-tag</pre> <p>Disables default VLAN ID tagging on the virtual port.</p> <p>Command mode: UFP Virtual Port Configuration</p> |
| <pre>qos bandwidth {max <10-100> min <10-100>}</pre> <p>Configures bandwidth allocation for the virtual port:</p> <ul style="list-style-type: none"> – Configures the minimum bandwidth guaranteed for the virtual port as a percentage of the physical port's bandwidth. The default value is 25. – Configures the maximum bandwidth allowed for this virtual port as a percentage of the physical port's bandwidth. The default value is 100. <p>Note: The aggregated minimum bandwidth guaranteed for all the virtual ports within a physical port cannot exceed 100.</p> <p>Command mode: UFP Virtual Port Configuration</p> |

VM Group Configuration

Table 349 describes the VM group configuration options. A VM group is a collection of members, such as VMs, ports, or trunk groups. Members of a VM group share certain properties, including VLAN membership, ACLs (VMAP), and VM profiles.

Table 349. VM Group Commands

| Command Syntax and Usage |
|--|
| <pre>virt vmgroup <I-4069> cpu</pre> <p>Enables or disables sending unregistered IPMC to CPU.</p> <p>Command mode: Global configuration</p> |
| <pre>virt vmgroup <I-4069> flood</pre> <p>Enables or disables flooding unregistered IPMC.</p> <p>Command mode: Global configuration</p> |
| <pre>virt vmgroup <I-4069> optflood</pre> <p>Enables or disables optimized flooding.</p> <p>Command mode: Global configuration</p> |
| <pre>virt vmgroup <I-4069> vlan <VLAN number></pre> <p>Assigns a VLAN to this VM group. If you do not assign a VLAN to the VM group, the switch automatically assigns an unused VLAN when adding a port or a VM to the VM Group.</p> <p>Note: If you add a VM profile to this group, the group will use the VLAN assigned to the profile.</p> <p>Command mode: Global configuration</p> |
| <pre>[no] virt vmgroup <I-4069> vmap <VMAP number> intports extports</pre> <p>Assigns the selected VLAN Map to this group. You can choose to limit operation of the VLAN Map to internal ports only or external ports only. If you do not select a port type, the VMAP is applied to the entire VM Group.</p> <p>For more information about configuring VLAN Maps, see “VMAP Configuration” on page 313.</p> <p>Command mode: Global configuration</p> |
| <pre>[no] virt vmgroup <I-4069> tag</pre> <p>Enables or disables VLAN tagging on ports in this VM group.</p> <p>Command mode: Global configuration</p> |
| <pre>virt vmgroup <I-4069> vm [<MAC address> <UUID> <name> <IP address> <index number>]</pre> <p>Adds a VM to the VM group. Enter a unique identifier to select a VM. The UUID and name parameters apply only if Virtual Center information is configured (virt vmware vcspec).</p> <p>The VM index number is found in the VM information dump (show virt vm).</p> <p>Note: If the VM is connected to a port that is contained within the VM group, do not add the VM to the VM group.</p> <p>Command mode: Global configuration</p> |

Table 349. VM Group Commands (continued)

| Command Syntax and Usage | |
|--|---|
| <pre>no virt vmgroup <I-4069> vm [<MAC address> <UUID> <name> <IP address> <index number>]</pre> | <p>Removes a VM from the VM group. Enter a unique identifier to select a VM. The UUID and name parameters apply only if Virtual Center information is configured (virt vmware vcspec). The VM index number is found in the VM information dump (show virt vm).</p> <p>Command mode: Global configuration</p> |
| <pre>virt vmgroup <I-4069> profile <profile name (1-39 characters)></pre> | <p>Adds the selected VM profile to the VM group.</p> <p>Command mode: Global configuration</p> |
| <pre>no virt vmgroup <I-4069> profile</pre> | <p>Removes the VM profile assigned to the VM group.</p> <p>Note: This command can only be used if the VM group is empty (only has the profile assigned).</p> <p>Command mode: Global configuration</p> |
| <pre>virt vmgroup <I-4069> port <port number or alias></pre> | <p>Adds the selected port to the VM group.</p> <p>Note: A port can be added to a VM group only if no VMs on that port are members of the VM group.</p> <p>Command mode: Global configuration</p> |
| <pre>no virt vmgroup <I-4069> port <port number or alias></pre> | <p>Removes the selected port from the VM group.</p> <p>Command mode: Global configuration</p> |
| <pre>virt vmgroup <I-4096> vport <port alias or number></pre> | <p>Adds the selected virtual port to the VM group.</p> <p>Command mode: Global configuration</p> |
| <pre>no virt vmgroup <I-4096> vport <port alias or number></pre> | <p>Removes the selected virtual port from the VM group.</p> <p>Command mode: Global configuration</p> |
| <pre>virt vmgroup <I-4069> portchannel <trunk number></pre> | <p>Adds the selected trunk group to the VM group.</p> <p>Command mode: Global configuration</p> |
| <pre>no virt vmgroup <I-4069> portchannel <trunk number></pre> | <p>Removes the selected trunk group from the VM group.</p> <p>Command mode: Global configuration</p> |

Table 349. VM Group Commands (continued)

| Command Syntax and Usage | |
|--|--|
| <pre>virt vmgroup <I-4069> key <I-65535></pre> | <p>Adds an LACP <i>admin key</i> to the VM group. LACP trunks formed with this <i>admin key</i> will be included in the VM group.</p> <p>Command mode: Global configuration</p> |
| <pre>no virt vmgroup <I-4069> key <I-65535></pre> | <p>Removes an LACP <i>admin key</i> from the VM group.</p> <p>Command mode: Global configuration</p> |
| <pre>virt vmgroup <I-4069> stg <STG number></pre> | <p>Assigns the VM group VLAN to a Spanning Tree Group (STG).</p> <p>Command mode: Global configuration</p> |
| <pre>virt vmgroup <I-4069> validate [basic advanced]</pre> | <p>Enables MAC address spoof prevention for the specified VM group. Default setting is disabled.</p> <ul style="list-style-type: none"> – <i>basic</i> validation ensures lightweight port-based protection by cross-checking the VM MAC address, switch port and switch ID between the switch and the hypervisor. Applicable for “trusted” hypervisors, which are not susceptible to duplicating or reusing MAC addresses on virtual machines. – <i>advanced</i> validation ensures heavyweight VM-based protection by cross-checking the VM MAC address, VM UUID, switch port and switch ID between the switch and the hypervisor. Applicable for “untrusted” hypervisors, which are susceptible to duplicating or reusing MAC addresses on virtual machines. <p>Command mode: Global configuration</p> |
| <pre>no virt vmgroup <I-4069> validate</pre> | <p>Disables MAC address spoof prevention for the specified VM group.</p> <p>Command mode: Global configuration</p> |
| <pre>no virt vmgroup <I-4069></pre> | <p>Deletes the VM group.</p> <p>Command mode: Global configuration</p> |
| <pre>show virt vmgroup <I-4069></pre> | <p>Displays the current VM group parameters.</p> <p>Command mode: All</p> |

VM Check Configuration

[Table 350](#) describes the VM Check validation options used for MAC address spoof prevention.

Table 350. VM Check Configuration Options

| Command Syntax and Usage | |
|--|--|
| <pre>virt vmcheck acls max <1-640></pre> | <p>Configures the maximum number of ACLs that can be set up for MAC address spoofing prevention in advanced validation mode. Default value is 50.</p> <p>Command mode: Global configuration</p> |
| <pre>no virt vmcheck acls</pre> | <p>Disables ACL-based MAC address spoofing prevention in advanced validation mode.</p> <p>Command mode: Global configuration</p> |
| <pre>virt vmcheck action basic {link log}</pre> | <p>Sets up action taken when detecting MAC address spoofing in basic validation mode:</p> <ul style="list-style-type: none"> – link registers a syslog entry and disables the corresponding switch port – log registers a syslog entry <p>Default setting is link.</p> <p>Command mode: Global configuration</p> |
| <pre>virt vmcheck action advanced {acl link log}</pre> | <p>Sets up action taken when detecting MAC address spoofing in advanced validation mode:</p> <ul style="list-style-type: none"> – acl registers a syslog entry and installs an ACL to drop traffic incoming on the corresponding switch port originating from the spoofed MAC address – link registers a syslog entry and disables the corresponding switch port – log registers a syslog entry <p>Default setting is acl.</p> <p>Command mode: Global configuration</p> |
| <pre>[no] virt vmcheck trust <ports></pre> | <p>Enables or disables trusted ports for VM communication. By default, all ports are disabled.</p> <p>Command mode: Global configuration</p> |
| <pre>show virt vmcheck</pre> | <p>Displays the current VM Check settings. See page 119 for sample output.</p> <p>Command mode: Global configuration</p> |

VM Profile Configuration

Table 351 describes the VM Profiles configuration options.

Table 351. VM Profiles Commands

| Command Syntax and Usage |
|---|
| <pre>virt vmprofile <profile name (1-39 characters)></pre> <p>Defines a name for the VM profile.</p> <p>Command mode: Global configuration</p> |
| <pre>no virt vmprofile <profile name (1-39 characters)></pre> <p>Deletes the selected VM profile.</p> <p>Command mode: Global configuration</p> |
| <pre>virt vmprofile edit <profile name (1-39 characters)> vlan <VLAN number></pre> <p>Assigns a VLAN to the VM profile.</p> <p>Command mode: Global configuration</p> |
| <pre>[no] virt vmprofile edit <profile name (1-39 characters)> shaping [<average (1-1000000000)> <burst (1-1000000000)> <peak (1-1000000000)>]</pre> <p>Configures traffic shaping parameters implemented in the hypervisor, as follows:</p> <ul style="list-style-type: none"> – Average traffic, in Kilobits per second – Maximum burst size, in Kilobytes – Peak traffic, in Kilobits per second – Delete traffic shaping parameters. <p>Command mode: Global configuration</p> |
| <pre>[no] virt vmprofile edit <profile name (1-39 characters)> eshaping [<average (1-1000000000)> <burst (1-1000000000)> <peak (1-1000000000)>]</pre> <p>Configures traffic egress shaping parameters implemented in the hypervisor, as follows:</p> <ul style="list-style-type: none"> – Average traffic, in Kilobits per second – Maximum burst size, in Kilobytes – Peak traffic, in Kilobits per second – Delete traffic shaping parameters. <p>Command mode: Global configuration</p> |
| <pre>show virt vmprofile [<profile name>]</pre> <p>Displays the current VM Profile parameters.</p> <p>Command mode: All</p> |

VMWare Configuration

Table 352 describes the VMware configuration options. When the user configures the VMware Virtual Center, the VM Agent module in the switch can perform advanced functionality by communicating with the VMware management console. The Virtual Center provides VM and Host names, IP addresses, Virtual Switch and port group information. The VM Agent on the switch communicates with the Virtual Center to synchronize VM profiles between the switch and the VMware virtual switch.

Table 352. VM Ware Commands

| Command Syntax and Usage | |
|--|---|
| <pre>virt vmware hbport <I-65535></pre> | <p>Configures the UDP port number used for heartbeat communication from the VM host to the Virtual Center. The default value is port 902.</p> <p>Command mode: Global configuration</p> |
| <pre>[no] virt vmware vcspec [<IP address> [<username> noauth]</pre> | <p>Defines the Virtual Center credentials on the switch. Once you configure the Virtual Center, VM Agent functionality is enabled across the system. You are prompted for the following information:</p> <ul style="list-style-type: none"> – IP address of the Virtual Center – User name and password for the Virtual Center – Whether to authenticate the SSL security certificate (yes or no) <p>Command mode: Global configuration</p> |
| <pre>virt vmware hello [enable haddr <IP_address> hport <port_no> htimer <I-60>]</pre> | <p>Configures CDP (Cisco Discovery Protocol) advertisements sent periodically to VMware ESX hypervisors. Exchanging CDP message with ESX hypervisors facilitates MAC address spoof prevention. Default setting is disabled.</p> <ul style="list-style-type: none"> – <code>enable</code> enables CDP advertisements transmission. – <code>haddr</code> advertises a specific IP address instead of the default 0.0.0.0 IP. – <code>hport</code> enables ports on which CDP advertisements are sent. – <code>htimer</code> sets the number of seconds between successive CDP advertisements. Default value is 30. <p>Command mode: Global configuration</p> |
| <pre>no virt vmware hello [enable hport <port_no>]</pre> | <p>Disables CDP advertisement transmissions completely or only on specific ports.</p> <p>Command mode: Global configuration</p> |
| <pre>show virt vmware</pre> | <p>Displays the current VMware parameters.</p> <p>Command mode: All</p> |

Miscellaneous VMready Configuration

You can pre-configure MAC addresses as VM Organization Unique Identifiers (OUIs). These configuration commands are only available using the Networking OS CLI and the Miscellaneous VMready Configuration Menu. [Table 352](#) describes the VMready configuration options.

Table 353. VMware Miscellaneous Options

| Command Syntax and Usage |
|---|
| <pre>virt vmrmisc oui < 3 byte VM MAC OUI> <Vendor Name></pre> <p>Adds a MAC OUI.</p> |
| <pre>no virt vmrmisc oui < 3 byte VM MAC OUI></pre> <p>Removes a MAC OUI.</p> |
| <pre>show virt oui</pre> <p>Displays all the configured MAC OUIs.</p> |
| <pre>virt vmrmisc lmac</pre> <p>Enables the switch to treat locally administered MAC addresses as VMs.</p> |
| <pre>no virt vmrmisc lmac</pre> <p>Disables the switch from treating locally administered MAC addresses as VMs.</p> |

Edge Virtual Bridge Configuration

You can configure your switch to use Edge Virtual Bridging (EVB). [Table 354](#) describes the EVB configuration options.

Table 354. Edge Virtual Bridge Configuration Options

| Command Syntax and Usage |
|--|
| <pre>virt evb vsidb <VSIDB_number></pre> <p>Enter Virtual Station Interface Database configuration mode. Command mode: Global configuration</p> |
| <pre>virt evb update vsidb <VSIDB_number></pre> <p>Update VSI types from the VSI database. Command mode: All</p> |
| <pre>clear virt evb vsidb <VSIDB_number></pre> <p>Clears local VSI types cache. Command mode: Privileged EXEC</p> |
| <pre>clear virt evb vsi</pre> <p>Clears VSI database associations. Command mode: Privileged EXEC</p> |
| <pre>host <IP address> [mgt-port data-port]</pre> <p>Sets the Virtual Station Interface Type database manager IPv4/IPv6 address and the port used for the connection. By default, the management port is used. Command mode: VSI Database</p> |
| <pre>port <I-65534></pre> <p>Sets the Virtual Station Interface Type database manager port. Command mode: VSI Database</p> |
| <pre>filename <URI path></pre> <p>Sets the Virtual Station Interface Type database document name. Command mode: VSI Database</p> |
| <pre>filepath <URI path></pre> <p>Sets the Virtual Station Interface Type database document path. Command mode: VSI Database</p> |
| <pre>update-interval <5-300></pre> <p>Sets the Virtual Station Interface Type database update interval in seconds. A value of "0" disables periodic updates. Command mode: VSI Database</p> |
| <pre>show virt evb vsitypes [mgrid <0-255> typeid <I-16777215> version <0-255></pre> <p>Displays the current Virtual Station Interface Type database parameters. Command mode: All</p> |

Table 354. Edge Virtual Bridge Configuration Options

| Command Syntax and Usage |
|---|
| <pre>show virt evb vsidb <VSIDB_number></pre> <p>Displays the current Virtual Station Interface database information.</p> <p>Command mode: All</p> |
| <pre>no virt evb vsidb <VSIDB_number></pre> <p>Resets the Virtual Station Interface Type database information to the default values.</p> <p>Command mode: Global configuration</p> |

Edge Virtual Bridge Profile Configuration

Table 355 describes the Edge Virtual Bridge profile configuration options.

Table 355. Edge Virtual Bridge VSI Type Profile Configuration Options

| Command Syntax and Usage |
|---|
| <pre>virt evb profile <profile_number></pre> <p>Enter Virtual Station Interface type profile configuration mode.</p> <p>Command mode: Global configuration</p> |
| <pre>[no] reflective-relay</pre> <p>Enables or disables VEPA mode (Reflective Relay capability).</p> <p>Command mode: EVB Profile</p> |
| <pre>[no] vsi-discovery</pre> <p>Enables or disables VSI Discovery (ECP and VDP).</p> <p>Command mode: EVB Profile</p> |
| <pre>no virt evb profile <profile_number></pre> <p>Deletes the specified EVB profile.</p> <p>Command mode: Global configuration</p> |
| <pre>show virt evb profile [<1-16>]</pre> <p>Displays the current EVB profile parameters.</p> <p>Command mode: All</p> |
| <pre>evb profile <1-16></pre> <p>Applies the specified EVB profile for the port. Automatically enables LLDP EVB TLV on the corresponding port.</p> <p>Command mode: Interface port</p> |
| <pre>no evb profile</pre> <p>Resets EVB profile for the port. Automatically disables LLDP, EVB, and TLV on the corresponding port.</p> <p>Command mode: Interface port</p> |

OpenFlow Configuration

OpenFlow is an open interface used to control the forwarding plane in compatible switches and routers remotely, from an external controller. The EN4093 and EN4093R 10Gb Scalable Switch can function as either a Hybrid or OpenFlow-only switch:

- In Hybrid mode (default), an OpenFlow pipeline can be set up to run in parallel to the normal Ethernet switching pipeline. The two pipelines are completely separate, each with its own dedicated ports and confined packet flows.
- In OpenFlow-only mode, the normal Ethernet switching capabilities are disabled, and the EN4093 and EN4093R 10Gb Scalable Switch behaves as a pure OpenFlow switch.

Table 356 describes the OpenFlow configuration options.

Table 356.

| Command Syntax and Usage |
|--|
| <pre>boot profile openflow</pre> <p>Starts the switch in OpenFlow-only mode on reboot.</p> <p>Command mode: Global configuration</p> |
| <pre>boot profile default</pre> <p>Starts the switch in Hybrid mode on reboot. This is the default setting.</p> <p>Command mode: Global configuration</p> |
| <pre>[no] openflow enable</pre> <p>Enables or disables OpenFlow.</p> <p>Note: The following features are not supported when OpenFlow is enabled: ACL, VNIC egress, VMready VMAP, FCOE, IPv6, IPMC, ECN, PVID and MACL.</p> <p>Command mode: Global configuration</p> |
| <pre>[no] openflow edgeport <port_numbers></pre> <p>Enables or disables the selected port as an OpenFlow edge port (outside port). Edge ports are usually connected to servers. The default setting is disabled.</p> <p>Note: Learning is turned on and flood blocking is turned on in OpenFlow edge ports.</p> <p>Command mode: Global configuration</p> |
| <pre>openflow fdb-priority <1-65535></pre> <p>Configures a priority value to map flows with matching priority to FDB entries, if the flow uses destination MAC address and VLAN as the matching qualifier and single port as the action. The default value is 1000.</p> <p>Note: When you issue this command, all registered flow entries are cleared.</p> <p>Command mode: Global configuration</p> |

Table 356.

| Command Syntax and Usage | |
|---|---|
| <code>no openflow fdb-priority</code> | Resets priority value required for FDB flows to the default value of 1000. Command mode: Global configuration |
| <code>openflow fdb-timeout <1-300></code> | Configures a time interval in seconds for periodically clearing dynamically learned FDB entries on edge ports. Default value is disabled. Command mode: Global configuration |
| <code>no openflow fdb-timeout</code> | Disables periodical clearing of dynamically learned FDB entries on edge ports. Command mode: Global configuration |
| <code>[no] openflow fdb-aging</code> | Enables or disables periodical clearing of dynamically learned FDB entries on a specific port. Default value is disabled on OpenFlow edge ports. Command mode: Interface port |
| <code>[no] openflow static-station-move</code> | Enables or disables forwarding frames that have source MAC addresses conflicting with entries in the static FDB table. This enables equal cost multi-path routing and use cases where IPS and Firewall devices forward packets without changing the source MAC address. Default value is disabled. Command mode: Interface port |
| <code>openflow instance <1-2></code> | Enters OpenFlow Instance command mode for the specified instance ID. Command mode: Global configuration, OpenFlow Instance |
| <code>no openflow instance <1-2></code> | Deletes the instance and clears flow table and statistics for the specified instance ID. Command mode: Global configuration, OpenFlow Instance |
| <code>[no] openflow mgmtport <ports></code> | Enables or disables OpenFlow management for the selected port. Use OpenFlow management ports to communicate with an OpenFlow Controller. In Hybrid mode, controllers can also connect to the switch using legacy ports. The default setting is disabled. Command mode: Global configuration |

Table 356.

| Command Syntax and Usage |
|--|
| <pre>show openflow [flow-allocation information statistics table]</pre> <p>Displays the current OpenFlow configuration. For more information, see page 104.</p> <ul style="list-style-type: none"> – <code>flow-allocation</code> displays the configured, current and maximum number of flows for each OpenFlow instance. For more information, see page 104. – <code>information</code> displays the configuration for each OpenFlow instance. For more information, see page 104. – <code>statistics</code> displays traffic statistics for each OpenFlow instance. For more information see page 105. – <code>table</code> displays the basic and emergency flow tables for each OpenFlow instance. For more information, see page 106 <p>Command mode: All</p> |
| <pre>show openflow instance <I-2> [information statistics table]</pre> <p>Displays OpenFlow information for the specified instance ID:</p> <ul style="list-style-type: none"> – <code>information</code> displays the instance configuration – <code>statistics</code> displays traffic statistics – <code>table</code> displays the basic and emergency flow tables <p>Command mode: All</p> |
| <pre>clear openflow {statistics table [basic emergency]}</pre> <p>Clears OpenFlow data for all instances:</p> <ul style="list-style-type: none"> – The <code>statistics</code> option clears traffic statistics. – The <code>table</code> option clears all basic and emergency OpenFlow tables. <ul style="list-style-type: none"> • The <code>basic</code> option clears only the basic OpenFlow tables. • The <code>emergency</code> option clears only the emergency OpenFlow tables. <p>Command mode: Privileged EXEC</p> |
| <pre>clear openflow instance <I-2> {statistics table [basic emergency]}</pre> <p>Clears OpenFlow data for the specified instance ID:</p> <ul style="list-style-type: none"> – The <code>statistics</code> option clears traffic statistics. – The <code>table</code> option clears all basic and emergency OpenFlow tables. <ul style="list-style-type: none"> • The <code>basic</code> option clears only the basic OpenFlow table. • The <code>emergency</code> option clears only the emergency OpenFlow table. <p>Command mode: Privileged EXEC</p> |
| <pre>[no] buffer</pre> <p>Enables or disables buffering support for OpenFlow packets. The default setting is disabled.</p> <p>Command mode: OpenFlow Instance</p> |

Table 356.

| Command Syntax and Usage | |
|---|--|
| <code>connect-retry <1-8></code> | <p>Configures the maximum number of attempts to establish connection to a controller, before assuming the controller is down. The default value is 4.</p> <p>Command mode: OpenFlow Instance</p> |
| <code>no connect-retry</code> | <p>Resets the <code>connect-retry</code> value to 4.</p> <p>Command mode: OpenFlow Instance</p> |
| <code>controller <1-4> address <ip_address> [data-port mgt-port extm-port]</code> | <p>Configures the IP address of the OpenFlow Controller. You may specify the port to use for data transfer: data port (<code>data-port</code>), management port (<code>mgt-port</code>) or external management port (<code>extm-port</code>). By default, the system uses the management port.</p> <p>Command mode: OpenFlow Instance</p> |
| <code>controller <1-4> port <TCP port number (1-65535)></code> | <p>Configures the TCP port used for communication with the Controller. The default port is 6633.</p> <p>Command mode: OpenFlow Instance</p> |
| <code>no controller <1-4></code> | <p>Deletes the selected controller from the specified instance ID.</p> <p>Command mode: OpenFlow Instance</p> |
| <code>dpid <hex string></code> | <p>Applies an 8 byte Datapath ID to the instance, which enables equal cost multi-path routing in an OpenFlow environment. The default value is the instance ID followed by the switch MAC.</p> <p>Command mode: OpenFlow Instance</p> |
| <code>no dpid</code> | <p>Resets the instance's Datapath ID to the default value (instance ID followed by the switch MAC).</p> <p>Command mode: OpenFlow Instance</p> |
| <code>echo-reply-timeout <2-65535></code> | <p>Configures the duration in seconds the switch will wait to receive an echo reply from the controller, before assuming failure. The default value is 15.</p> <p>Note: The <code>echo-reply-timeout</code> value must be lower than the <code>echo-request-interval</code> value.</p> <p>Command mode: OpenFlow Instance</p> |
| <code>no echo-reply-timeout</code> | <p>Resets the <code>echo-reply-timeout</code> to the default value of 15.</p> <p>Command mode: OpenFlow Instance</p> |

Table 356.

| Command Syntax and Usage | |
|--|--|
| <pre>echo-request-interval <5-65535></pre> | <p>Configures the maximum duration in seconds the switch will keep sending echo requests to a non-responsive controller. The default value is 30.</p> <p>Note: The <code>echo-request-interval</code> value must be higher than the <code>echo-reply-timeout</code> value.</p> <p>Command mode: OpenFlow Instance</p> |
| <pre>no echo-request-interval</pre> | <p>Resets the <code>echo-request-interval</code> value to the default value of 30.</p> <p>Command mode: OpenFlow Instance</p> |
| <pre>emergency [timeout <0-3600>]</pre> | <p>Forces the instance in emergency mode.</p> <p>The <code>timeout</code> parameter configures the duration in seconds after which the emergency mode expires. The default value is 30.</p> <p>Command mode: OpenFlow Instance</p> |
| <pre>no emergency [timeout]</pre> | <p>Brings the instance out of emergency mode.</p> <p>The <code>timeout</code> parameter resets the emergency mode duration to the default value of 30.</p> <p>Command mode: OpenFlow Instance</p> |
| <pre>[no] enable</pre> | <p>Enables or disables the instance. When disabling an instance, its flow tables and statistics are cleared.</p> <p>Command mode: OpenFlow Instance</p> |
| <pre>max-flow-acl <0-750/1000></pre> | <p>Enables or disables the maximum flow ACL option, which ensures a dedicated maximum number of ACL flows are available for the instance. The maximum number of entries is 750 in Hybrid mode and 1000 in OpenFlow Only mode. The total number of 750/1000 entries is shared between instances. By default, <code>max-flow-acl</code> is set to 0, allowing instances to dynamically access the available ACL flow slots until depletion. Setting <code>max-flow-acl</code> manually limits the number of ACL flow slots available for other instances by the corresponding value.</p> <p>Command mode: OpenFlow Instance</p> |
| <pre>max-flow-mcast-fdb <0-4096></pre> | <p>Enables or disables the maximum flow multicast FDB option, which ensures a dedicated maximum number of FDB multicast flows are available for the instance. The total number of 4096 entries is shared between instances. By default, <code>max-flow-mcast-fdb</code> is set to 0, allowing instances to dynamically access the available FDB multicast flow slots until depletion. Setting <code>max-flow-mcast-fdb</code> manually limits the number of FDB multicast flow slots available for other instances by the corresponding value.</p> <p>Command mode: OpenFlow Instance</p> |

Table 356.

| Command Syntax and Usage | |
|--|--|
| <code>max-flow-ucast-fdb <0-123904></code> | <p>Enables or disables the maximum flow unicast FDB option, which ensures a dedicated maximum number of FDB unicast flows available for the instance. The total number of 123904 entries is shared between instances. By default, <code>max-flow-ucast-fdb</code> is set to 0, allowing instances to dynamically access the available FDB unicast flow slots until depletion. Setting <code>max-flow-ucast-fdb</code> manually limits the number of FDB unicast flow slots available for other instances by the corresponding value.</p> <p>Command mode: OpenFlow Instance</p> |
| <code>no max-flow-acl</code> | <p>Sets the instance's maximum number of ACL based flows to the default value of 0 (dynamic allocation).</p> <p>Command mode: OpenFlow Instance</p> |
| <code>no max-flow-mcast-fdb</code> | <p>Sets the instance's maximum number of FDB based multicast flows to the default value of 0 (dynamic allocation).</p> <p>Command mode: OpenFlow Instance</p> |
| <code>no max-flow-ucast-fdb</code> | <p>Sets the instance's maximum number of FDB based unicast flows to the default value of 0 (dynamic allocation).</p> <p>Command mode: OpenFlow Instance</p> |
| <code>[no] member <ports></code> | <p>Enables or disables port usage by the OpenFlow instance for data traffic.</p> <p>Command mode: OpenFlow Instance</p> |
| <code>min-flow-timeout <0-300></code> | <p>Sets the minimum number of seconds after which a flow can be cleared from the instance's tables. Default value is 0, meaning controller provided values are used instead.</p> <p>Command mode: OpenFlow Instance</p> |
| <code>no min-flow-timeout</code> | <p>Sets the number of seconds after which a flow can be cleared from the instance's tables to the default value of 0 (controller provided values).</p> <p>Command mode: OpenFlow Instance</p> |

Static Flows Configuration

Static flows are ACL OpenFlow entries set up manually from the CLI by the administrator. Static flows cannot be deleted/modified by OpenFlow controllers and will continue to function when the switch goes into emergency mode. Even if they

qualify as FDB entries based on their settings, static flows are always stored as ACL entries. A total of maximum 750 static flows pool is shared between all OpenFlow instances.

[Table 357](#) describes the static flow configuration options.

Table 357. Static Flows

| Command Syntax and Usage |
|---|
| <pre>static-table add index <1-750> match WORD actions WORD [options WORD] priority <0-65535></pre> <p>Adds a static flow entry to the instance. Command mode: OpenFlow Instance</p> |
| <pre>static-table modify index <1-750> match WORD actions WORD [options WORD] priority <0-65535></pre> <p>Overwrites a static flow entry. Command mode: OpenFlow Instance</p> |
| <pre>static-table remove index <1-750></pre> <p>Deletes a static flow entry. Command mode: OpenFlow Instance</p> |
| <pre>clear openflow table static</pre> <p>Deletes all static flow entries. Command mode: Global configuration</p> |

The following table describes the available matching qualifiers

Table 358. Static Flow Matching Qualifiers

| Qualifier | Value |
|------------------|---|
| ingress-port | Port of instance |
| src-mac | Source MAC address |
| dst-mac | Destination MAC address |
| vlan-id | VLAN identifier (0-4095 + 65535 (untagged)) |
| vlan-priority | 802.1p Priority Code Point (0-7) |
| src-ip | Source IP address |
| dst-ip | Destination IP address |
| src-port | L4 source port (0-65536) |
| dst-port | L4 destination port (0-65535) |
| ether-type | "arp"/"0806" or "ip"/"0800" or (hex-value <= 65535) |
| protocol | "tcp" or "udp" or 0-255 |
| tos | IP Type of Service (0-255) |

Table 358. Static Flow Matching Qualifiers

| Qualifier | Value |
|-----------|---|
| type | "request" or "reply" (can be set only if ether type is ARP) |
| all | Applicable to all traffic |

The following table describes the available actions

Table 359. Static Flow Actions

| Action | Value |
|-------------------|---|
| out-put | "all", "in-port", "flood", "controller" or a valid port |
| set-src-mac | Change source MAC address |
| set-dst-mac | Change destination MAC address |
| strip-vlan-id | Remove VLAN identifier |
| set-vlan-priority | Set 802.1p priority code point value (0-7) |
| set-nw-tos | Set IP Type of Service (0-255) |
| drop | Drop packet |
| max-len | Maximum length to send to controller |

Switch Partition (SPAR) Configuration

Switch partitions (SPARs) divide the data plane inside a physical switch into independent switching domains. Switch partitions do not communicate with each other, forcing hosts on different SPARs to bridge traffic over an upstream link, even if they belong to the same VLAN.

Up to 8 SPARs can be defined on a switch. Each SPAR supports up to 256 local VLANs, for further partitioning flexibility

Table 360. SPAR Configuration Options

| Command Syntax and Usage | |
|---|---|
| spar <1-8> | Enters SPAR Configuration mode Command mode: Global configuration |
| no spar <1-8> | Deletes the specified SPAR. Command mode: Global configuration |
| [no] enable | Enables or disables the SPAR. Command mode: SPAR Configuration |
| name | Configures the SPAR name. Command mode: SPAR Configuration |
| [no] uplink {port <port no.> portchannel <1-64> adminkey <1-65535>} | Enables or disables uplink connectivity for the SPAR. A single external port, portchannel, or LACP channel can be used for uplink. All uplinks within a SPAR are automatically assigned to the SPAR domain's default VLAN and to any SPAR local VLANs. Command mode: SPAR Configuration |
| domain default {vlan <2-4094> member <port no.>} | Configures the SPAR's default domain settings: <ul style="list-style-type: none"> – vlan configures the default SPAR VLAN ID. A unique factory default VLAN ID is assigned to each SPAR as "408x", where x is the SPAR ID <1-8>. This option provides an override if conflicts arise with a customer VLAN ID on the upstream network. – member adds server ports to the SPAR. Command mode: SPAR Configuration |
| no domain default member <port no.> | Removes server ports from the SPAR. Command mode: SPAR Configuration |

Table 360. SPAR Configuration Options (continued)

| Command Syntax and Usage |
|---|
| <p>domain local <1-32> {enable member <port no.> name <text> vlan <2-4094>}</p> <p>Configures the SPAR's local domains:</p> <ul style="list-style-type: none"> - enable enables the SPAR local domains - member adds server ports to the SPAR local domains - name configures the SPAR local domains names - vlan applies a VLAN ID to the SPAR local domains. The default value is 0. <p>Command mode: SPAR Configuration</p> |
| <p>no domain local <1-32> [enable member <port no.>]</p> <p>Deletes the SPAR local VLAN domains:</p> <ul style="list-style-type: none"> - enable disables the SPAR local domains - member deletes SPAR local domains server ports <p>Command mode: SPAR Configuration</p> |
| <p>domain mode {passthrough local}</p> <p>Configures the SPAR domain mode:</p> <ul style="list-style-type: none"> - passthrough references member ports only by the SPAR default VLAN. This provides VLAN-unaware uplink connectivity via pass-through tunnel domain switching for SPAR member ports. The default value is passthrough. - local references member ports by both SPAR default VLAN and SPAR local domain VLANs. This provides VLAN-aware uplink connectivity via local domain switching for SPAR member ports <p>Command mode: SPAR Configuration</p> |
| <p>show spar <1-8> [domain [default local <1-32>] uplink]</p> <p>Displays the SPAR settings:</p> <ul style="list-style-type: none"> - domain filters only the SPAR domain related settings <ul style="list-style-type: none"> • default filters only SPAR default domain settings • local <1-32> filters only SPAR local domains settings - uplink filters only SPAR uplink settings <p>Command mode: All</p> |

Precision Time Protocol Configuration

Precision Time Protocol (PTP) allows high accuracy clock synchronization between a networked master clock and compliant network hosts. The IBM Flex System Fabric EN4093 and EN4093R 10Gb Scalable Switch supports two PTP modes:

- Ordinary slave clock - Synchronizes the Real Time Clock (RTC) with PTP master clocks detected on the network.
- End-to-End transparent clock - Allows PTP traffic to pass through without affecting the RTC, while updating the correction fields for event packets.

Table 361. Precision Time Protocol Configuration Options

| Command Syntax and Usage | |
|---|--|
| <pre>[no] ptp ordinary enable</pre> | <p>Enables or disables PTP ordinary slave clock mode. In this mode, if a PTP master clock is detected on the network, the RTC is synchronized with it. If no master clock is detected, the RTC is not affected. Default setting is disabled.</p> <p>Note: Enabling PTP ordinary slave clock mode disables NTP settings and system time clock manual settings.</p> <p>Command mode: Global configuration</p> |
| <pre>[no] ptp transparent enable</pre> | <p>Enables or disables PTP End-to-End transparent clock mode. In this mode, incoming PTP packets are forwarded based on routing rules currently in place for the PTP domain's multicast address (within the 224.0.1.129 - 224.0.1.132 range). On egress, PTP packet timestamps are updated based on the time spent between ingress and egress. Default setting is disabled.</p> <p>Command mode: Global configuration</p> |
| <pre>no ptp</pre> | <p>Disables both PTP ordinary slave clock mode and PTP End-to-End transparent clock mode.</p> <p>Command mode: Global configuration</p> |
| <pre>ip ptp source-interface loopback <1-5></pre> | <p>Loopback interface used as source IP address for delay-request packets sent during synchronization with the master clock in ordinary slave mode. By default, the interface with the lowest index from the master clock's VLAN is used.</p> <p>Command mode: Global configuration</p> |
| <pre>no ip ptp source-interface loopback</pre> | <p>Sets the source IP address for delay-request packets sent during synchronization with the master clock in ordinary slave mode to the interface with the lowest index from the master clock's VLAN.</p> <p>Command mode: Global configuration</p> |

Table 361. Precision Time Protocol Configuration Options (continued)

| Command Syntax and Usage |
|---|
| <pre>[no] ptp</pre> <p>Enables or disables PTP on the current port. Disabled ports will not support PTP even if PTP is globally enabled. Default setting is enabled.</p> <p>Note: PTP is not supported on management ports.</p> <p>Command mode: Interface port</p> |
| <pre>show ptp [counters]</pre> <p>Displays current PTP settings.</p> <p>The <code>counters</code> option displays PTP packet counters. See page 239 for details.</p> <p>Command mode: All</p> |
| <pre>show interface port <port alias or number> ptp-counters</pre> <p>Displays Precision Time Protocol statistics for the port. See page 239 for details.</p> <p>Command mode: All</p> |
| <pre>clear ptp counters</pre> <p>Resets PTP packet counters.</p> <p>Command mode: Privileged EXEC</p> |

Service Location Protocol Configuration

Service Location Protocol (SLP) enables networked devices to request/announce services over a local area network without prior configuration. In an SLP environment, devices may have the following roles:

- User Agents (UA) are devices requesting services.
- Service Agents (SA) are devices providing services.
- Directory Agents (DA) are devices caching services provided by SAs. When present in an SLA setup, DAs mediate all communication between UAs and SAs.

When SLP is enabled, the EN4093 and EN4093R 10Gb Scalable Switch behaves as a Service Agent providing systems management services.

Table 362. Service Location Protocol

| Command Syntax and Usage |
|--|
| <pre>[no] ip slp enable</pre> <p>Enables or disables SLP. Default value is disabled.</p> <p>Command mode: Global configuration</p> |
| <pre>[no] ip slp active-da-discovery enable</pre> <p>Enables or disables active directory agent discovery. Default value is disabled.</p> <p>Command mode: Global configuration</p> |

Table 362. Service Location Protocol (continued)

| Command Syntax and Usage |
|---|
| <pre>ip slp active-da-discovery-start-wait-time <1-10></pre> <p>Number of seconds to wait after enabling SLP before attempting active DA discovery, if active DA discovery is enabled. Default value is 3.</p> <p>Command mode: Global configuration</p> |
| <pre>clear ip slp directory-agents</pre> <p>Clears directory agents discovered.</p> <p>Command mode: Privileged EXEC</p> |

Configuration Dump

The dump program writes the current switch configuration to the terminal screen. To start the dump program, at the prompt, enter:

```
Router(config)# show running-config
```

The configuration is displayed with parameters that have been changed from the default values. The screen display can be captured, edited, and placed in a script file, which can be used to configure other switches through a Telnet connection. When using Telnet to configure a new switch, paste the configuration commands from the script file at the command line prompt of the switch. The active configuration can also be saved or loaded via FTP/TFTP, as described on [page 502](#).

Saving the Active Switch Configuration

When the `copy running-config {ftp|tftp|sftp}` command is used, the switch's active configuration commands (as displayed using `show running-config`) will be uploaded to the specified script configuration file on the FTP/TFTP/SFTP server. To start the switch configuration upload, at the prompt, enter:

```
Router(config)# copy running-config ftp [data-port|extm-port|mgt-port]
    or
Router(config)# copy running-config tftp [data-port|extm-port|mgt-port]
    or
Router(config)# copy running-config sftp [data-port|extm-port|mgt-port]
```

Select a port, or press **Enter** to use the default (management port). The switch prompts you for the server address and filename.

Notes:

- The output file is formatted with line-breaks but no carriage returns—the file cannot be viewed with editors that require carriage returns (such as Microsoft Notepad).
- If the FTP/TFTP server is running SunOS or the Solaris operating system, the specified configuration file must exist prior to executing the `copy running-config` command and must be writable (set with proper permission, and not locked by any application). The contents of the specified file will be replaced with the current configuration data.

Restoring the Active Switch Configuration

When the `copy {ftp|tftp|sftp} running-config` command is used, the active configuration will be replaced with the commands found in the specified configuration file. The file can contain a full switch configuration or a partial switch configuration.

To start the switch configuration download, at the prompt, enter:

```
Router(config)# copy ftp running-config [extm-port|mgt-port|data-port]
    or
Router(config)# copy tftp running-config [extm-port|mgt-port|data-port]
    or
Router(config)# copy sftp running-config [extm-port|mgt-port|data-port]
```

Select a port, or press **Enter** to use the default (management port). The switch prompts you for the server address and filename.

Chapter 5. Operations Commands

Operations commands generally affect switch performance immediately, but do not alter permanent switch configurations. For example, you can use Operations commands to immediately disable a port (without the need to apply or save the change), with the understanding that when the switch is reset, the port returns to its normally configured operation.

These commands enable you to alter switch operational characteristics without affecting switch configuration.

Table 363. General Operations Commands

| Command Syntax and Usage |
|--|
| <pre>password <1-128 characters></pre> <p>Allows the user to change the password. You must enter the current password in use for validation. The switch prompts for a new password between 1-128 characters.</p> <p>Command Mode: Privileged EXEC</p> |
| <pre>clear logging</pre> <p>Clears all Syslog messages.</p> <p>Command Mode: Privileged EXEC</p> |
| <pre>ntp send</pre> <p>Allows the user to send requests to the NTP server.</p> <p>Command Mode: Privileged EXEC</p> |

Operations-Level Port Commands

Operations-level port options are used for temporarily disabling or enabling a port, and for re-setting the port.

Table 364. Port Operations Commands

| Command Syntax and Usage |
|--|
| <pre>no interface port <port number or alias> shutdown</pre> <p>Temporarily enables the port. The port will be returned to its configured operation mode when the switch is reset.</p> <p>Command Mode: Privileged EXEC</p> |
| <pre>interface port <port number or alias> shutdown</pre> <p>Temporarily disables the port. The port will be returned to its configured operation mode when the switch is reset.</p> <p>Command Mode: Privileged EXEC</p> |
| <pre>show interface port <port number or alias> operation</pre> <p>Displays the port interface operational state.</p> <p>Command Mode: Privileged EXEC</p> |

Operations-Level Port 802.1X Commands

Operations-level port 802.1X options are used to temporarily set 802.1X parameters for a port.

Table 365. 802.1X Operations Commands

| Command Syntax and Usage |
|---|
| <pre>interface port <port number or alias> dot1x init</pre> <p>Re-initializes the 802.1X access-control parameters for the port. The following actions take place, depending on the 802.1X port configuration:</p> <ul style="list-style-type: none">– <code>force unauth</code>: the port is placed in unauthorized state, and traffic is blocked.– <code>auto</code>: the port is placed in unauthorized state, then authentication is initiated.– <code>force auth</code>: the port is placed in authorized state, and authentication is not required. <p>Command Mode: Privileged EXEC</p> |
| <pre>interface port <port number or alias> dot1x re-authenticate</pre> <p>Re-authenticates the supplicant (client) attached to the port. This command only applies if the port's 802.1X mode is configured as <code>auto</code>.</p> <p>Command Mode: Privileged EXEC</p> |

Operations-Level FCoE Commands

Fibre Channel over Ethernet (FCoE) operations commands are listed in the following table.

Table 366. FCoE Operations Commands

| Command Syntax and Usage |
|--|
| <pre>no fcoe fips fcf <MAC address></pre> <p>Deletes the selected FCoE Forwarder (FCF), and any associated ACLs.</p> <p>Command Mode: Privileged EXEC</p> |

Operations-Level VRRP Commands

Table 367. Virtual Router Redundancy Operations Commands

| Command Syntax and Usage |
|--|
| <pre>router vrrp backup <virtual router number (1-255)></pre> <p>Forces the specified master virtual router on this switch into backup mode. This is generally used for passing master control back to a preferred switch once the preferred switch has been returned to service after a failure. When this command is executed, the current master gives up control and initiates a new election by temporarily advertising its own priority level as 0 (lowest). After the new election, the virtual router forced into backup mode by this command will resume master control in the following cases:</p> <ul style="list-style-type: none">– This switch owns the virtual router (the IP addresses of the virtual router and its IP interface are the same)– This switch's virtual router has a higher priority and preemption is enabled.– There are no other virtual routers available to take master control. <p>Command Mode: Privileged EXEC</p> |

Operations-Level BGP Commands

Table 368. IP BGP Operations Commands

| Command Syntax and Usage |
|---|
| <pre>router bgp start <1-12></pre> <p>Starts the peer session.</p> <p>Command Mode: Privileged EXEC</p> |
| <pre>router bgp stop <1-12></pre> <p>Stops the peer session.</p> <p>Command Mode: Privileged EXEC</p> |
| <pre>show ip bgp state</pre> <p>Displays the current BGP operational state.</p> <p>Command Mode: Privileged EXEC</p> |

Protected Mode Options

Protected Mode is used to secure certain switch management options, so they cannot be changed by the management module.

Table 369. Protected Mode Options

| Command Syntax and Usage |
|--|
| <pre>[no] protected-mode external-management</pre> <p>Enables exclusive local control of switch management. When Protected Mode is set to <code>on</code>, the management module cannot be used to disable external management on the switch. The default value is <code>enabled</code>.</p> <p>Note: Due to current management module implementation, this setting cannot be disabled.</p> <p>Command Mode: Global Configuration</p> |
| <pre>[no] protected-mode external-ports</pre> <p>Enables exclusive local control of external ports. When Protected Mode is set to <code>on</code>, the management module cannot be used to disable external ports on the switch. The default value is <code>enabled</code>.</p> <p>Note: Due to current management module implementation, this setting cannot be disabled.</p> <p>Command Mode: Global Configuration</p> |
| <pre>[no] protected-mode factory-default</pre> <p>Enables exclusive local control of factory default resets. When Protected Mode is set to <code>on</code>, the management module cannot be used to reset the switch software to factory default values. The default value is <code>enabled</code>.</p> <p>Note: Due to current management module implementation, this setting cannot be disabled.</p> <p>Command Mode: Global Configuration</p> |
| <pre>[no] protected-mode management-vlan-interface</pre> <p>Enables exclusive local control of the management interface. When Protected Mode is set to <code>on</code>, the management module cannot be used to configure parameters for the management interface. The default value is <code>enabled</code>.</p> <p>Note: Due to current management module implementation, this setting cannot be disabled.</p> <p>Command Mode: Global Configuration</p> |
| <pre>protected-mode enable</pre> <p>Turns Protected Mode <code>on</code>. When Protected Mode is turned on, the switch takes exclusive local control of all enabled options.</p> <p>Command Mode: Global Configuration</p> |

Table 369. Protected Mode Options (continued)

| Command Syntax and Usage |
|---|
| <pre>no protected-mode enable</pre> <p>Turns Protected Mode <code>off</code>. When Protected Mode is turned off, the switch relinquishes exclusive local control of all enabled options.</p> <p>Command Mode: Global Configuration</p> |
| <pre>show protected-mode</pre> <p>Displays the current Protected Mode configuration.</p> <p>Command Mode: Global Configuration</p> |

VMware Operations

Use these commands to perform minor adjustments to the VMware operation. Use these commands to perform Virtual Switch operations directly from the switch. Note that these commands require the configuration of Virtual Center access information (`virt vmware vcspec`).

Table 370. VMware Operations Commands

| Command Syntax and Usage |
|---|
| <pre>virt vmware pg [<Port Group name> <host ID> <VSwitch name> <VLAN number> <shaping-enabled> <average-Kbps> <burst-KB> <peak-Kbps>]</pre> <p>Adds a Port Group to a VMware host. You are prompted for the following information:</p> <ul style="list-style-type: none"> – Port Group name – VMware host ID (Use host UUID, host IP address, or host name.) – Virtual Switch name – VLAN ID of the Port Group – Whether to enable the traffic-shaping profile (1 or 0). If you choose 1 (yes), you are prompted to enter the traffic shaping parameters. <p>Command Mode: Privileged EXEC</p> |
| <pre>virt vmware vsw <host ID> <Virtual Switch name></pre> <p>Adds a Virtual Switch to a VMware host. Use one of the following identifiers to specify the host:</p> <ul style="list-style-type: none"> – UUID – IP address – Host name <p>Command Mode: Privileged EXEC</p> |
| <pre>no virt vmware pg <Port Group name> <host ID></pre> <p>Removes a Port Group from a VMware host. Use one of the following identifiers to specify the host:</p> <ul style="list-style-type: none"> – UUID – IP address – Host name <p>Command Mode: Privileged EXEC</p> |
| <pre>no virt vmware vsw <host ID> <Virtual Switch name></pre> <p>Removes a Virtual Switch from a VMware host. Use one of the following identifiers to specify the host:</p> <ul style="list-style-type: none"> – UUID – IP address – Host name <p>Command Mode: Privileged EXEC</p> |

Table 370. VMware Operations Commands (continued)

| Command Syntax and Usage |
|--|
| <pre>virt vmware export <VM profile name> <VMware host ID> <Virtual Switch name></pre> <p>Exports a VM Profile to a VMware host.</p> <p>Use one of the following identifiers to specify each host:</p> <ul style="list-style-type: none"> – UUID – IP address – Host name <p>You may enter a Virtual Switch name, or enter a new name to create a new Virtual Switch.</p> <p>Command Mode: Privileged EXEC</p> |
| <pre>virt vmware scan</pre> <p>Performs a scan of the VM Agent, and updates VM information.</p> <p>Command Mode: Privileged EXEC</p> |
| <pre>virt vmware vmacpg <MAC address> <Port Group name></pre> <p>Changes a VM NIC's configured Port Group.</p> <p>Command Mode: Privileged EXEC</p> |
| <pre>virt vmware updpg <Port Group name> <host ID> <VLAN number> [<shaping enabled> <average Kbps> <burst KB> <peak Kbps>]</pre> <p>Updates a VMware host's Port Group parameters.</p> <p>Command Mode: Privileged EXEC</p> |

VMware Distributed Virtual Switch Operations

Use these commands to administer a VMware Distributed Virtual Switch (dvSwitch).

Table 371. VMware dvSwitch Operations (/oper/virt/vmware/dvswitch)

| Command Syntax and Usage |
|---|
| <pre>virt vmware dvswitch add <datacenter name> <dvSwitch name> <dvSwitch version></pre> <p>Adds the specified dvSwitch to the specified DataCenter.</p> <p>Command Mode: Privileged EXEC</p> |
| <pre>virt vmware dvswitch del <datacenter name> <dvSwitch name></pre> <p>Removes the specified dvSwitch from the specified DataCenter.</p> <p>Command Mode: Privileged EXEC</p> |
| <pre>virt vmware dvswitch addhost <dvSwitch name> <host UUID IP address host name></pre> <p>Adds the specified host to the specified dvSwitch. Use one of the following identifiers to specify the host:</p> <ul style="list-style-type: none"> – UUID – IP address – Host name <p>Command Mode: Privileged EXEC</p> |
| <pre>virt vmware dvswitch remhost <dvSwitch name> <host UUID IP address host name></pre> <p>Removes the specified host from the specified dvSwitch. Use one of the following identifiers to specify the host:</p> <ul style="list-style-type: none"> – UUID – IP address – Host name <p>Command Mode: Privileged EXEC</p> |
| <pre>virt vmware dvswitch addUplink <dvSwitch name> <host ID> <uplink name></pre> <p>Adds the specified physical NIC to the specified dvSwitch uplink ports.</p> <p>Command Mode: Privileged EXEC</p> |
| <pre>virt vmware dvswitch remUplink <dvSwitch name> <host ID> <uplink name></pre> <p>Removes the specified physical NIC from the specified dvSwitch uplink ports.</p> <p>Command Mode: Privileged EXEC</p> |

VMware Distributed Port Group Operations

Use these commands to administer a VMware distributed port group.

Table 372. VMware Distributed Port Group Operations (/oper/virt/vmware/dpg)

| Command Syntax and Usage |
|--|
| <pre>virt vmware dpg add <port group name> <dvSwitch name> <VLAN ID> [ishaping <bandwidth> <burst size> <peak bandwidth>] [eshaping <bandwidth> <burst size> <peak bandwidth>]</pre> <p>Adds the specified port group to the specified dvSwitch. You may enter the following parameters:</p> <ul style="list-style-type: none">– <code>ishaping</code>: Enables ingress shaping. Supply the following information:<ul style="list-style-type: none">• average bandwidth in KB per second• burst size in KB• peak bandwidth in KB per second– <code>eshaping</code>: Enables egress shaping. Supply the following information:<ul style="list-style-type: none">• average bandwidth in KB per second• burst size in KB• peak bandwidth in KB per second <p>Command Mode: Privileged EXEC</p> |
| <pre>virt vmware dpg vmac <VNIC MAC> <port group name></pre> <p>Adds the specified VM NIC to the specified port group.</p> <p>Command Mode: Privileged EXEC</p> |
| <pre>virt vmware dpg update <port group name> <dvSwitch name> <VLAN ID (1-4094)> [ishaping <bandwidth> <burst size> <peak bandwidth>] [eshaping <bandwidth> <burst size> <peak bandwidth>]</pre> <p>Updates the specified port group on the specified dvSwitch. You may enter the following parameters:</p> <ul style="list-style-type: none">– <code>ishaping</code>: Enables ingress shaping. Supply the following information:<ul style="list-style-type: none">• average bandwidth in KB per second• burst size in KB• peak bandwidth in KB per second– <code>eshaping</code>: Enables egress shaping. Supply the following information:<ul style="list-style-type: none">• average bandwidth in KB per second• burst size in KB• peak bandwidth in KB per second <p>Command Mode: Privileged EXEC</p> |
| <pre>virt vmware dpg del <port group name> <dvSwitch name></pre> <p>Removes the specified port group from the specified dvSwitch.</p> <p>Command Mode: Privileged EXEC</p> |

Edge Virtual Bridge Operations

Edge Virtual Bridge operations commands are listed in the following table:

Table 373. Edge Virtual Bridge Operations Commands

| Command Syntax and Usage |
|--|
| <pre>virt evb update vsidb <VSIDB_number></pre> <p>Update VSI types from the VSI database. Command mode: All</p> |
| <pre>clear virt evb vsidb <VSIDB_number></pre> <p>Clears local VSI types cache. Command mode: Privileged EXEC</p> |
| <pre>clear virt evb vsi</pre> <p>Clears VSI database associations. Command mode: Privileged EXEC</p> |

Chapter 6. Boot Options

To use the Boot Options commands, you must be logged in to the switch as the administrator. The Boot Options commands provide options for:

- Selecting a switch software image to be used when the switch is next reset
- Selecting a configuration block to be used when the switch is next reset
- Downloading or uploading a new software image to the switch via FTP/TFTP

In addition to the Boot commands, you can use a Web browser or SNMP to work with switch image and configuration files. To use SNMP, refer to “Working with Switch Images and Configuration Files” in the *Command Reference*.

The boot options are discussed in the following sections.

Stacking Boot Options

The Stacking Boot options are used to define the role of the switch in a stack: either as the Master that controls the stack, or as a participating Member switch. Options are available for loading stack software to individual Member switches, and to configure the VLAN that is reserved for inter-switch stacking communications.

You must enable Stacking and reset the switch to enter Stacking mode. When the switch enters Stacking mode, the Stacking configuration menu appears. For more information, see “Stacking Configuration” on page 295.

Table 374 lists the Boot Stacking command options.

Table 374. Boot Stacking Options

| Command Syntax and Usage |
|--|
| <pre>boot stack mode [master member]</pre> <p>Configures the Stacking mode for the selected switch.</p> <p>Command mode: Global configuration</p> |
| <pre>boot stack hlgig-trunk <list of ports></pre> <p>Configures the ports used to connect the switch to the stack. Enter only 10Gb external ports.</p> <p>Command mode: Global configuration</p> |
| <pre>boot stack vlan <VLAN number> [<1-16> all backup master]</pre> <p>Configures the VLAN used for Stacking control communication. This can be applied for:</p> <ul style="list-style-type: none">– a specific unit <1-16>– all units– backup unit– master unit <p>Command mode: Global configuration</p> |
| <pre>default boot stack [master backup <cnum (1-16)> all]</pre> <p>Resets the Stacking boot parameters to their default values.</p> <p>Command mode: Global configuration</p> |

Table 374. Boot Stacking Options (continued)

| Command Syntax and Usage | |
|--|--|
| <code>boot stack push-image {image1 image2 boot} <csnum (1-16)></code> | Pushes the selected software file from the master to the selected switch. Command mode: Global configuration |
| <code>boot stack enable</code> | Enables the switch stack. Command mode: Global configuration |
| <code>no boot stack enable</code> | Disables the switch stack. Command mode: Global configuration |
| <code>show boot stack [master backup <csnum (1-8)> all]</code> | Displays current Stacking boot parameters. Command mode: All |

When in stacking mode, the following stand-alone features are not supported:

- Active Multi-Path Protocol (AMP)
- SFD
- sFlow port monitoring
- Uni-Directional Link Detection (UDLD)
- Port flood blocking
- BCM rate control
- Link Layer Detection Protocol (LLDP)
- Private VLANs
- RIP
- OSPF and OSPFv3
- IPv6
- Virtual Router Redundancy Protocol (VRRP)
- Loopback Interfaces
- Router IDs
- Route maps
- Border Gateway Protocol (BGP)
- MAC address notification
- Static MAC address adding
- Static multicast
- Converged Enhanced Ethernet (CEE) and Fibre Channel over Ethernet (FCOE)
- MSTP and RSTP settings for CIST, Name, Rev, and Maxhop
- IGMP Relay and IGMPv3
- Static multicast routes
- IGMP Querier
- Microburst detection

Switch menus and commands for unsupported features may be unavailable, or may have no effect on switch operation.

Scheduled Reboot

This feature allows you to schedule a reboot to occur at a particular time in the future. This feature is particularly helpful if the user needs to perform switch upgrades during off-peak hours. You can set the reboot time, cancel a previously scheduled reboot, and check the time of the currently set reboot schedule.

Table 375. Boot Scheduling Options

| Command Syntax and Usage |
|--|
| <pre>boot schedule <day of week> <time of day></pre> <p>Defines the reboot schedule. Enter the day of the week, followed by the time of day (in hh:mm format). For example:</p> <pre>boot schedule monday 11:30</pre> <p>Command mode: Global configuration</p> |
| <pre>no boot schedule</pre> <p>Cancels the next pending scheduled reboot.</p> <p>Command mode: Global configuration</p> |
| <pre>show boot</pre> <p>Displays the current reboot scheduling parameters.</p> <p>Command mode: All</p> |

Netboot Configuration

Netboot allows the switch to automatically download its configuration file over the network during switch reboot, and apply the new configuration. Upon reboot, the switch includes the following options in its DHCP requests:

- Option 66 (TFTP server address)
- Option 67 (file path)

If the DHCP server returns the information, the switch initiates a TFTP file transfer, and loads the configuration file into the active configuration block. As the switch boots up, it applies the new configuration file. Note that the option 66 TFTP server address must be specified in IP-address format (host name is not supported).

If DHCP is not enabled, or the DHCP server does not return the required information, the switch uses the manually-configured TFTP server address and file path.

Table 376. Netboot Options (/boot/netboot)

| Command Syntax and Usage | |
|--|--|
| <code>boot netboot enable</code> | Enables Netboot. When enabled, the switch boots into factory-default configuration, and attempts to download a new configuration file. Command mode: Global configuration |
| <code>no boot netboot enable</code> | Disables Netboot. Command mode: Global configuration |
| <code>[no] boot netboot tftp <IP address></code> | Configures the IP address of the TFTP server used for manual configuration. This server is used if DHCP is not enabled, or if the DHCP server does not return the required information. Command mode: Global configuration |
| <code>[no] boot netboot cfgfile <1-31 characters></code> | Defines the file path for the configuration file on the TFTP server. For example: <code>/directory/sub/config.cfg</code> Command mode: Global configuration |
| <code>show boot</code> | Displays the current Netboot parameters. Command mode: All |

QSFP Port Configuration

Quad Small Form-factor Pluggable Plus (QSFP+) ports are designed to handle high-intensity traffic. Use the following commands to configure QSFP+ ports.

Table 377. Netboot Options (/boot/qsfp-40Gports)

| Command Syntax and Usage |
|---|
| <pre>[no] boot qsfp-40Gports <ports></pre> <p>Enables or disables 40GbE mode on the selected QSFP+ ports. When enabled, each QSFP+ port is set as a single 40GbE port. When disabled, each QSFP+ port is configured to breakout into four 10GbE ports.</p> <p>You must reboot the switch for this change to take effect.</p> <p>Command mode: Global configuration</p> |
| <pre>show boot qsfp-port-modes</pre> <p>Displays the current QSFP port settings.</p> <p>Command mode: All</p> |

Updating the Switch Software Image

The switch software image is the executable code running on the EN4093 and EN4093R 10Gb Scalable Switch. A version of the image ships with the switch, and comes pre-installed on the device. As new versions of the image are released, you can upgrade the software running on your switch. To get the latest version of software available for your EN4093 and EN4093R, go to:

<http://www-304.ibm.com/jct01004c/systems/support>

Click on software updates. Use the following command to determine the current software version: `show boot`

Upgrading the software image on your switch requires the following:

- Loading the new image onto a FTP or TFTP server on your network
- Transferring the new image from the FTP or TFTP server to your switch
- Selecting the new software image to be loaded into switch memory the next time the switch is reset

Loading New Software to Your Switch

The switch can store up to two different software images, called `image1` and `image2`, as well as boot software, called `boot`. When you load new software, you must specify where it should be placed: either into `image1`, `image2`, or `boot`.

For example, if your active image is currently loaded into `image1`, you would probably load the new image software into `image2`. This lets you test the new software and reload the original active image (stored in `image1`), if needed.

Note: EN4093R models do not support image releases prior to 7.5.

To load a new software image to your switch, you need the following:

- The image or boot software loaded on an FTP/TFTP server on your network
- The hostname or IP address of the FTP/TFTP server
- The name of the new software image or boot file

Note: The DNS parameters must be configured if specifying hostnames.

When the above requirements are met, use the following procedure to download the new software to your switch.

1. In Privileged EXEC mode, enter the following command:

```
Router# copy {ftp|tftp} {image1 | image2 | boot-image[extm-port |  
mgt-port | data-port]}
```

Select a port, or press <Enter> to use the default (management port).

2. Enter the hostname or IP address of the FTP or TFTP server.

```
Address or name of remote host: <IP address or hostname>
```

3. Enter the name of the new software file on the server.

```
Source file name: <filename>
```

The exact form of the name will vary by server. However, the file location is normally relative to the FTP or TFTP directory (usually `tftpboot`).

4. Enter your username and password for the server, if applicable.

```
User name: {<username> | <Enter>}
```

5. The system prompts you to confirm your request.

Next, select a software image to run, as described in the following section.

Selecting a Software Image to Run

You can select which software image (`image1` or `image2`) you want to run in switch memory for the next reboot.

1. In Global Configuration mode, enter:

```
Router(config)# boot image {image1 | image2}
```

2. Enter the name of the image you want the switch to use upon the next boot. The system informs you of which image set to be loaded at the next reset:

```
Next boot will use switch software image1 instead of image2.
```

Uploading a Software Image from Your Switch

You can upload a software image from the switch to a FTP or TFTP server.

1. In Privileged EXEC mode, enter:

```
Router# copy {image1 | image2 | boot-image} {ftp|tftp[extm-port |  
mgt-port | data-port]}
```

Select a port, or press `<Enter>` to use the default (management port).

2. Enter the name or the IP address of the FTP or TFTP server:

```
Address or name of remote host: <IP address or hostname>
```

3. Enter the name of the file into which the image will be uploaded on the FTP or TFTP server:

```
Destination file name: <filename>
```

4. Enter your username and password for the server, if applicable.

```
User name: {<username> | <Enter>}
```

5. The system then requests confirmation of what you have entered. To have the file uploaded, enter `y`.

```
image2 currently contains Software Version 6.5.0
that was downloaded at 0:23:39 Thu Jan 1, 2010
Upload will transfer image2 (2788535 bytes) to file "image1"
on FTP/TFTP server 1.90.90.95.
Confirm upload operation (y/n) ? y
```

Selecting a Configuration Block

When you make configuration changes to the EN4093 and EN4093R 10Gb Scalable Switch, you must save the changes so that they are retained beyond the next time the switch is reset. When you perform a save operation (`copy running-config startup-config`), your new configuration changes are placed in the *active* configuration block. The previous configuration is copied into the *backup* configuration block.

There is also a *factory* configuration block. This holds the default configuration set by the factory when your EN4093 and EN4093R 10Gb Scalable Switch was manufactured. Under certain circumstances, it may be desirable to reset the switch configuration to the default. This can be useful when a custom-configured EN4093 and EN4093R 10Gb Scalable Switch is moved to a network environment where it will be re-configured for a different purpose.

In Global Configuration mode, use the following command to set which configuration block you want the switch to load the next time it is reset:

```
Router (config)# boot configuration-block {active | backup | factory}
```

Resetting the Switch

You can reset the switch to make your software image file and configuration block changes occur.

Note: Resetting the switch causes the Spanning Tree Group to restart. This process can be lengthy, depending on the topology of your network.

Enter the following command to reset (reload) the switch:

```
>> Router# reload
```

You are prompted to confirm your request.

```
Reset will use software "image2" and the active config block.  
>> Note that this will RESTART the Spanning Tree,  
>> which will likely cause an interruption in network service.  
Confirm reload (y/n) ?
```

Accessing the Networking OS CLI

To access the Networking OS CLI, enter the following command from the ISCLI:

```
Router(config)# boot cli-mode ibmnos-cli
```

The default command-line interface for the EN4093 and EN4093R is the Networking OS CLI. To access the ISCLI, enter the following command and reset the EN4093 and EN4093R:

```
Main# boot/mode iscli
```

Users can select the CLI mode upon login, if the following ISCLI command is enabled:

```
Router(config)# boot cli-mode prompt
```

Only an administrator connected through the CLI can view and enable the `prompt` command. When `prompt` is enabled, the first user to log in can select the CLI mode. Subsequent users must use the selected CLI mode, until all users have logged out.

Changing the Switch Profile

The Networking OS software for the EN4093 and EN4093R can be configured to operate in different modes for different deployment scenarios. The deployment profile changes some of the basic switch behavior, shifting switch resources to optimize capacity levels to meet the needs of different types of networks. For more information about deployment profiles, see the *Networking OS 7.7 Application Guide*.

To change the deployment profile, select the new profile and reset the EN4093 and EN4093R. Use the following command to select a new profile:

```
Router(config)# boot profile {default | acl | ipmc-opt | openflow}
```

Using the Boot Management Menu

The Boot Management menu allows you to switch the software image, reset the switch to factory defaults, or to recover from a failed software download.

You can interrupt the boot process and enter the Boot Management menu from the serial console port. When the system displays Memory Test, press **<Shift B>**. The Boot Management menu appears.

```
Resetting the System ...
Memory Test .....

Boot Management Menu
1 - Change booting image
2 - Change configuration block
3 - Xmodem download
4 - Exit

Please choose your menu option: 1
Current boot image is 1. Enter image to boot: 1 or 2: 2
Booting from image 2
```

The Boot Management menu allows you to perform the following actions:

- To change the booting image, press 1 and follow the screen prompts.
- To change the configuration block, press 2, and follow the screen prompts.
- To perform an Xmodem download, press 3 and follow the screen prompts.
- To exit the Boot Management menu, press 4. The booting process continues.

Recovering from a Failed Software Upgrade

Use the following procedure to recover from a failed software upgrade.

1. Connect a PC to the serial port of the switch.
2. Open a terminal emulator program that supports XModem Download (for example, HyperTerminal, CRT, PuTTY) and select the following serial port characteristics:
 - Speed: 9600 bps
 - Data Bits: 8
 - Stop Bits: 1
 - Parity: None
 - Flow Control: None
3. Boot the switch and access the Boot Management menu by pressing **<Shift B>** while the Memory Test is in progress and the dots are being displayed.
4. Select **3** for **Xmodem download**. When you see the following message, change the Serial Port characteristics to 115200 bps:

```
## Switch baudrate to 115200 bps and press ENTER ...
```

5. Press **<Enter>** to set the system into download accept mode. When the readiness meter displays (a series of “C” characters), start XModem on your terminal emulator.

6. Select the Boot Image to download. The XModem initiates the file transfer. When the download is complete, a message similar to the following is displayed:

```
yzModem - CRC mode, 62494(SOH)/0(STX)/0(CAN) packets, 6 retries

Extracting images ... Do *NOT* power cycle the switch.

**** VMLINUX ****

Un-Protected 10 sectors

Erasing Flash..... done

Writing to Flash.....done

Protected 10 sectors

**** RAMDISK ****

Un-Protected 44 sectors

Erasing Flash..... done

Writing to Flash.....done

Protected 44 sectors

**** BOOT CODE ****

Un-Protected 8 sectors

Erasing Flash..... done

Writing to Flash.....done

Protected 8 sectors
```

7. When you see the following message, change the Serial Port characteristics to 9600 bps:

```
## Switch baudrate to 9600 bps and press ESC ...
```

8. Press the Escape key (<Esc>) to re-display the Boot Management menu.
9. Select **3** to start a new **XModem Download**. When you see the following message, change the Serial Port characteristics to 115200 bps:

```
## Switch baudrate to 115200 bps and press ENTER ...
```

10. Press <Enter> to continue the download.

11. Select the OS Image to download. The XModem initiates the file transfer. When the download is complete, a message similar to the following is displayed:

```
yzModem - CRC mode, 27186(SOH)/0(STX)/0(CAN) packets, 6 retries
Extracting images ... Do *NOT* power cycle the switch.
**** Switch OS ****
Please choose the Switch OS Image to upgrade [1|2|n] :
```

12. Select the image number to load the new image (1 or 2). It is recommended that you select 1. A message similar to the following is displayed:

```
Switch OS Image 1 ...
Un-Protected 27 sectors
Erasing Flash..... done
Writing to Flash.....done
Protected 27 sectors
```

13. When you see the following message, change the Serial Port characteristics to 9600 bps:

```
## Switch baudrate to 9600 bps and press ESC ...
```

14. Press the Escape key (<Esc>) to re-display the Boot Management menu. Select **4** to exit and boot the new image.

Recovering a Failed Boot Image

Use the following procedure to recover from a failed boot image upgrade.

1. Connect a PC to the serial port of the switch.
2. Open a terminal emulator program that supports Xmodem download (for example, HyperTerminal, CRT, PuTTY) and select the following serial port characteristics:
 - Speed: 9600 bps
 - Data Bits: 8
 - Stop Bits: 1
 - Parity: None
 - Flow Control: None
3. Boot the switch and access the Boot Management menu by pressing <Shift B> while the Memory Test is in progress and the dots are being displayed.
4. Select **4** for **Xmodem download**. You will see the following display:

```
Perform xmodem download
To download an image use 1K xmodem at 115200 bps.
```

5. When you see the following message, change the Serial Port characteristics to 115200 bps:

Change the baud rate to 115200 bps and hit the <ENTER> key before initiating the download.

- a. Press <Enter> to set the system into download accept mode. When the readiness meter displays (a series of "C" characters), start Xmodem on your terminal emulator. You will see a display similar to the following:

```
Extracting images ... Do *NOT* power cycle the switch.
**** RAMDISK ****
Un-Protected 38 sectors
Erasing Flash...
..... done
Erased 38 sectors
Writing to
Flash...9...8...7...6...5...4...3...2...1...done
Protected 38 sectors
**** KERNEL ****
Un-Protected 24 sectors
Erasing Flash...
..... done
Erased 24 sectors
writing to Flash...9...8...7...6...5...4...3...2...1...
```

- b. When you see the following message, change the Serial Port characteristics to 9600 bps:

Change the baud rate back to 9600 bps, hit the <ESC> key.

Boot image recovery is complete.

Chapter 7. Maintenance Commands

The maintenance commands are used to manage dump information and forward database information. They also include debugging commands to help with troubleshooting.

Dump information contains internal switch state data that is written to flash memory on the EN4093 and EN4093R 10Gb Scalable Switch after any one of the following occurs:

- The watchdog timer forces a switch reset. The purpose of the watchdog timer is to reboot the switch if the switch software freezes.
- The switch detects a hardware or software problem that requires a reboot.

To use the maintenance commands, you must be logged in to the switch as the administrator.

Table 378. General Maintenance Commands

| Command Syntax and Usage |
|--|
| <pre>show flash-dump-uuencode</pre> <p>Displays dump information in uuencoded format. For details, see page 548.</p> <p>Command mode: All</p> |
| <pre>copy flash-dump tftp</pre> <p>Saves the system dump information via TFTP. For details, see page 549.</p> <p>Command mode: All except User EXEC</p> |
| <pre>copy flash-dump ftp</pre> <p>Saves the system dump information via FTP. For details, see page 549.</p> <p>Command mode: All except User EXEC</p> |
| <pre>copy flash-dump sftp</pre> <p>Saves the system dump information via SFTP. For details, see page 549.</p> <p>Command mode: All except User EXEC</p> |
| <pre>clear flash-dump</pre> <p>Clears dump information from flash memory.</p> <p>Command mode: All except User EXEC</p> |
| <pre>show tech-support [l2 l3 link port]</pre> <p>Dumps all EN4093 and EN4093R information, statistics, and configuration. You can log the output (<code>tsdmp</code>) into a file. To filter the information, use the following options:</p> <ul style="list-style-type: none"> – <code>l2</code> displays only Layer 2-related information – <code>l3</code> displays only Layer 3-related information – <code>link</code> displays only link status-related information – <code>port</code> displays only port-related information <p>Command mode: All except User EXEC</p> |

Table 378. General Maintenance Commands

| Command Syntax and Usage |
|--|
| <pre>copy tech-support tftp</pre> <p>Redirects the technical support dump (tsdmp) to an external TFTP server.</p> <p>Command mode: All except User EXEC</p> |
| <pre>copy tech-support ftp</pre> <p>Redirects the technical support dump (tsdmp) to an external FTP server.</p> <p>Command mode: All except User EXEC</p> |

Forwarding Database Maintenance

The Forwarding Database commands can be used to view information and to delete a MAC address from the forwarding database or to clear the entire forwarding database. This is helpful in identifying problems associated with MAC address learning and packet forwarding decisions.

Table 379. FDB Manipulation Commands

| Command Syntax and Usage |
|---|
| <pre>show mac-address-table address <MAC address></pre> <p>Displays a single database entry by its MAC address. If not specified, you are prompted for the MAC address of the device. Enter the MAC address using one of the following formats:</p> <ul style="list-style-type: none"> – xx:xx:xx:xx:xx:xx (such as 08:00:20:12:34:56) – xxxxxxxxxxxxxx (such as 080020123456) <p>Command mode: All except User EXEC</p> |
| <pre>show mac-address-table interface port <port number or alias></pre> <p>Displays all FDB entries for a particular port.</p> <p>Command mode: All except User EXEC</p> |
| <pre>show mac-address-table portchannel <trunk group number></pre> <p>Displays all FDB entries for a particular trunk group.</p> <p>Command mode: All</p> |
| <pre>show mac-address-table vlan <VLAN number></pre> <p>Displays all FDB entries on a single VLAN.</p> <p>Command mode: All except User EXEC</p> |
| <pre>show mac-address-table state {forward trunk unknown}</pre> <p>Displays all FDB entries of a particular state.</p> <p>Command mode: All except User EXEC</p> |
| <pre>show mac-address-table static</pre> <p>Displays static entries in the FDB.</p> <p>Command mode: All except User EXEC</p> |
| <pre>no mac-address-table static {<MAC address> all}</pre> <p>Removes static FDB entries.</p> <p>Command mode: All except User EXEC</p> |
| <pre>no mac-address-table multicast {<MAC address> all}</pre> <p>Removes static multicast FDB entries.</p> <p>Command mode: All except User EXEC</p> |
| <pre>clear mac-address-table static</pre> <p>Clears all static entries from the Forwarding Database.</p> <p>Command mode: All except User EXEC</p> |

Table 379. FDB Manipulation Commands (continued)

| Command Syntax and Usage |
|--|
| <pre>clear mac-address-table</pre> <p>Clears the entire Forwarding Database from switch memory.</p> <p>Command mode: All except User EXEC</p> |

Debugging Commands

The Miscellaneous Debug Commands display trace buffer information about events that can be helpful in understanding switch operation. You can view the following information using the debug commands:

- Events traced by the Management Processor (MP)
- Events traced to a buffer area when a reset occurs

Note: IBM Networking OS debug commands are intended for advanced users. Use debug commands with caution as they can disrupt the operation of the switch under high load conditions. When debug is running under high load conditions, the CLI prompt may appear unresponsive. Before debugging, check the MP utilization to verify there is sufficient processing capacity available to perform the debug operation.

If the switch resets for any reason, the MP trace buffer is saved into the snap trace buffer area. The output from these commands can be interpreted by Technical Support personnel.

Table 380. Miscellaneous Debug Commands

| Command Syntax and Usage |
|---|
| <code>debug debug-flags</code> This command sets the flags that are used for debugging purposes. Command mode: All except User EXEC |
| <code>debug mp-trace</code> Displays the Management Processor trace buffer. Header information similar to the following is shown: MP trace buffer at 13:28:15 Fri May 25, 2001; mask: 0x2ffdf748 The buffer information is displayed after the header. Command mode: All except User EXEC |
| <code>debug dumpbt</code> Displays the backtrace log. Command mode: All except User EXEC |
| <code>debug mp-snap</code> Displays the Management Processor snap (or post-mortem) trace buffer. This buffer contains information traced at the time that a reset occurred. Command mode: All except User EXEC |
| <code>clear flash-config</code> Deletes all flash configuration blocks. Command mode: All except User EXEC |

Table 380. Miscellaneous Debug Commands

| Command Syntax and Usage |
|---|
| <p>[no] debug lacp packet [receive transmit both] [port <port numbers>]</p> <p>Enables/disables debugging for Link Aggregation Control Protocol (LACP) packets on all ports running LACP.</p> <p>The following parameters are available:</p> <ul style="list-style-type: none"> – receive filters only LACP packets received – transmit filters only LACP packets sent – both filters LACP packets either sent or received – port filters LACP packets sent/received on specific ports <p>By default, LACP debugging is disabled.</p> <p>Command mode: Privileged EXEC</p> |
| <p>[no] debug spanning-tree bpdu [receive transmit]</p> <p>Enables/disables debugging for Spanning Tree Protocol (STP) Bridge Protocol Data Unit (BPDU) frames sent or received.</p> <p>The following parameters are available:</p> <ul style="list-style-type: none"> – receive filters only BPDU frames received – transmit filters only BPDU frames sent <p>By default, STP BPDU debugging is disabled.</p> <p>Command mode: Privileged EXEC</p> |

IP Security Debugging

The following table describes the options available.

Table 381. IP Security Debug Options

| Command Syntax and Usage |
|---|
| <p>[no] debug sec all</p> <p>Enables or disables all IP security debug messages.</p> |
| <p>[no] debug sec crypto</p> <p>Enables or disables all IP security cryptographic debug messages.</p> |
| <p>[no] debug sec ike</p> <p>Enables or disables all IP security IKEv2 debug messages.</p> |
| <p>[no] debug sec ipsec</p> <p>Enables or disables all IPsec debug messages.</p> |
| <p>[no] debug sec info</p> <p>Displays the current security debug settings.</p> |

DCBX Debugging Commands

Table 382. DCBX Maintenance Commands

| Command Syntax and Usage |
|--|
| <pre>show dcbx transmit <port alias or number></pre> <p>Displays the Type-Length-Value (TLV) list transmitted in the DCBX TLV. Command mode: All except User EXEC</p> |
| <pre>show dcbx receive <port alias or number></pre> <p>Displays the Type-Length-Value (TLV) list received in the DCBX TLV. Command mode: All except User EXEC</p> |

ARP Cache Maintenance

Table 383. Address Resolution Protocol Maintenance Commands

| Command Syntax and Usage |
|---|
| <pre>show ip arp find <IP address></pre> <p>Shows a single ARP entry by IP address. Command mode: All except User EXEC</p> |
| <pre>show ip arp interface port <port number or alias></pre> <p>Shows ARP entries on selected ports. Command mode: All except User EXEC</p> |
| <pre>show ip arp vlan <VLAN number></pre> <p>Shows ARP entries on a single VLAN. Command mode: All except User EXEC</p> |
| <pre>show ip arp reply</pre> <p>Shows the list of IP addresses which the switch will respond to for ARP requests. Command mode: All except User EXEC</p> |
| <pre>show ip arp</pre> <p>Shows all ARP entries. Command mode: All except User EXEC</p> |
| <pre>clear arp</pre> <p>Clears the entire ARP list from switch memory. Command mode: All except User EXEC</p> |

Note: To display all or a portion of ARP entries currently held in the switch, you can also refer to “ARP Information” on [page 64](#).

IP Route Manipulation

Table 384. IP Route Manipulation Commands

| Command Syntax and Usage |
|--|
| <pre>show ip route address <IP address></pre> <p>Shows a single route by destination IP address.</p> <p>Command mode: All except User EXEC</p> |
| <pre>show ip route gateway <IP address></pre> <p>Shows routes to a default gateway.</p> <p>Command mode: All except User EXEC</p> |
| <pre>show ip route type {indirect direct local broadcast martian multicast}</pre> <p>Shows routes of a single type.</p> <p>Command mode: All except User EXEC</p> <p>For a description of IP routing types, see Table 39 on page 63</p> |
| <pre>show ip route tag {fixed static address rip ospf bgp broadcast martian multicast}</pre> <p>Shows routes of a single tag.</p> <p>Command mode: All except User EXEC</p> <p>For a description of IP routing tags, see Table 40 on page 63</p> |
| <pre>show ip route interface <IP interface></pre> <p>Shows routes on a single interface.</p> <p>Command mode: All except User EXEC</p> |
| <pre>show ip route</pre> <p>Shows all routes.</p> <p>Command mode: All except User EXEC</p> |
| <pre>clear ip route</pre> <p>Clears the route table from switch memory.</p> <p>Command mode: All except User EXEC</p> |

Note: To display all routes, you can also refer to [“IP Routing Information” on page 62](#).

LLDP Cache Manipulation

[Table 385](#) describes the LLDP cache manipulation commands.

Table 385. LLDP Cache Manipulation commands

| Command Syntax and Usage |
|---|
| <pre>show lldp port <port alias or number></pre> <p>Displays Link Layer Discovery Protocol (LLDP) port information.</p> <p>Command mode: All</p> |
| <pre>show lldp receive</pre> <p>Displays information about the LLDP receive state machine.</p> <p>Command mode: All</p> |
| <pre>show lldp transmit</pre> <p>Displays information about the LLDP transmit state machine.</p> <p>Command mode: All</p> |
| <pre>show lldp remote-device [<I-256> detail]</pre> <p>Displays information received from LLDP -capable devices. For more information, see page 44.</p> <p>Command mode: All</p> |
| <pre>show lldp</pre> <p>Displays all LLDP information.</p> <p>Command mode: All</p> |
| <pre>clear lldp</pre> <p>Clears the LLDP cache.</p> <p>Command mode: All</p> |

IGMP Group Maintenance

Table 386 describes the IGMP group maintenance commands.

Table 386. IGMP Multicast Group Maintenance Commands

| Command Syntax and Usage |
|---|
| <pre>show ip igmp groups address <IP address></pre> <p>Displays a single IGMP multicast group by its IP address.</p> <p>Command mode: All</p> |
| <pre>show ip igmp groups vlan <VLAN number></pre> <p>Displays all IGMP multicast groups on a single VLAN.</p> <p>Command mode: All</p> |
| <pre>show ip igmp groups interface port <port number or alias></pre> <p>Displays all IGMP multicast groups on selected ports.</p> <p>Command mode: All</p> |
| <pre>show ip igmp groups portchannel <trunk number></pre> <p>Displays all IGMP multicast groups on a single trunk group.</p> <p>Command mode: All</p> |
| <pre>show ip igmp groups detail <IP address></pre> <p>Displays detailed information about a single IGMP multicast group.</p> <p>Command mode: All</p> |
| <pre>show ip igmp groups</pre> <p>Displays information for all multicast groups.</p> <p>Command mode: All</p> |
| <pre>clear ip igmp groups</pre> <p>Clears the IGMP group table.</p> <p>Command mode: All except User EXEC</p> |

IGMP Multicast Routers Maintenance

The following table describes the maintenance commands for IGMP multicast routers (Mrouters).

Table 387. IGMP Multicast Router Maintenance Commands

| Command Syntax and Usage |
|--|
| <pre>show ip igmp mrouter vlan <VLAN number></pre> <p>Displays IGMP Mrouter information for a single VLAN.</p> <p>Command mode: All</p> |
| <pre>show ip igmp mrouter</pre> <p>Displays information for all Mrouters.</p> <p>Command mode: All</p> |
| <pre>show ip igmp mrouter dynamic</pre> <p>Displays all dynamic multicast router ports installed.</p> <p>Command mode: All</p> |
| <pre>show ip igmp mrouter static</pre> <p>Displays all static multicast router ports installed.</p> <p>Command mode: All</p> |
| <pre>show ip igmp mrouter interface port <port alias or number></pre> <p>Displays all multicast router ports installed on a specific port.</p> <p>Command mode: All</p> |
| <pre>show ip igmp mrouter portchannel <trunk number></pre> <p>Displays all multicast router ports installed on a specific portchannel group.</p> <p>Command mode: All</p> |
| <pre>show ip igmp mrouter information</pre> <p>Displays IGMP snooping information for all Mrouters.</p> <p>Command mode: All</p> |
| <pre>show ip igmp snoop igmpv3</pre> <p>Displays IGMPv3 snooping information.</p> <p>Command mode: All</p> |
| <pre>show ip igmp relay</pre> <p>Displays IGMP relay information.</p> <p>Command mode: All</p> |
| <pre>clear ip igmp mrouter</pre> <p>Clears the IGMP Mrouter port table.</p> <p>Command mode: All except User EXEC</p> |

MLD Multicast Group Manipulation

Table 388 describes the Multicast Listener Discovery (MLD) manipulation options.

Table 388. MLD Maintenance

| Command Syntax and Usage |
|--|
| <pre>show ipv6 mld groups</pre> <p>Shows all MLD groups. Command mode: All</p> |
| <pre>show ipv6 mld interface <interface number></pre> <p>Shows MLD groups on the specified interface. Command mode: All</p> |
| <pre>clear ipv6 mld mrouter</pre> <p>Clears all dynamic MLD multicast router group tables. Command mode: All except User EXEC</p> |
| <pre>clear ipv6 mld groups</pre> <p>Clears all dynamic MLD registered group tables. Command mode: All except User EXEC</p> |
| <pre>clear ipv6 mld dynamic</pre> <p>Clears all dynamic MLD group tables. Command mode: All except User EXEC</p> |

IPv6 Neighbor Discovery Cache Manipulation

Table 389 describes the IPv6 Neighbor Discovery cache manipulation commands.

Table 389. IPv6 Neighbor Discovery cache manipulation commands

| Command Syntax and Usage |
|---|
| <pre>show ipv6 neighbors find <IPv6 address></pre> <p>Shows a single IPv6 Neighbor Discovery cache entry by IP address.</p> <p>Command mode: All</p> |
| <pre>show ipv6 neighbors interface port <port number or alias></pre> <p>Shows IPv6 Neighbor Discovery cache entries on a single port.</p> <p>Command mode: All</p> |
| <pre>show ipv6 neighbors vlan <VLAN number></pre> <p>Shows IPv6 Neighbor Discovery cache entries on a single VLAN.</p> <p>Command mode: All</p> |
| <pre>show ipv6 neighbors static</pre> <p>Shows static IPv6 Neighbor Discovery cache entries.</p> <p>Command mode: All</p> |
| <pre>show ipv6 neighbors</pre> <p>Shows all IPv6 Neighbor Discovery cache entries.</p> <p>Command mode: All</p> |
| <pre>clear ipv6 neighbors</pre> <p>Clears all IPv6 Neighbor Discovery cache entries from switch memory.</p> <p>Command mode: All except User EXEC</p> |

IPv6 Route Maintenance

Table 390 describes the IPv6 route maintenance commands.

Table 390. IPv6 Route Maintenance Options

| Command Syntax and Usage |
|---|
| <pre>show ipv6 route address <IPv6 address></pre> <p>Show a single route by destination IP address.</p> <p>Command mode: All</p> |
| <pre>show ipv6 route gateway <IPv6 gateway number></pre> <p>Show routes to a single gateway.</p> <p>Command mode: All</p> |
| <pre>show ipv6 route interface <interface number></pre> <p>Show routes on a single IP interface.</p> <p>Command mode: All</p> |
| <pre>show ipv6 route type {connected static ospf}</pre> <p>Show routes of a single type.</p> <p>Command mode: All</p> |
| <pre>show ipv6 route static</pre> <p>Show static IPv6 routes.</p> <p>Command mode: All</p> |
| <pre>show ipv6 route summary</pre> <p>Shows a summary of IPv6 route information.</p> <p>Command mode: All</p> |
| <pre>show ipv6 route</pre> <p>Shows all IPv6 routes.</p> <p>Command mode: All</p> |
| <pre>clear ipv6 route</pre> <p>Clears all IPv6 routes.</p> <p>Command mode: Privileged EXEC</p> |

Uuencode Flash Dump

Using this command, dump information is presented in uuencoded format. This format makes it easy to capture the dump information as a file or a string of characters.

If you want to capture dump information to a file, set your communication software on your workstation to capture session data prior to issuing the `show flash-dump-uuencode` command. This will ensure that you do not lose any information. Once entered, the `show flash-dump-uuencode` command will cause approximately 23,300 lines of data to be displayed on your screen and copied into the file.

Using the `show flash-dump-uuencode` command, dump information can be read multiple times. The command does not cause the information to be updated or cleared from flash memory.

Note: Dump information is not cleared automatically. In order for any subsequent dump information to be written to flash memory, you must manually clear the dump region. For more information on clearing the dump region, see [page 550](#).

To access dump information, enter:

```
Router# show flash-dump-uuencode
```

The dump information is displayed on your screen and, if you have configured your communication software to do so, captured to a file. If the dump region is empty, the following appears:

```
No FLASH dump available.
```

TFTP, SFTP or FTP System Dump Put

Use these commands to `put` (save) the system dump to a TFTP or FTP server.

Note: If the TFTP/FTP server is running SunOS or the Solaris operating system, the specified `copy flash-dump tftp` (or `ftp`) file must exist *prior* to executing the `copy flash-dump tftp` command (or `copy flash-dump ftp`), and must be writable (set with proper permission, and not locked by any application). The contents of the specified file will be replaced with the current dump data.

To save dump information via TFTP, enter:

```
Router# copy flash-dump tftp [data-port|extm-port|mgt-port] <server filename>
```

You are prompted for the TFTP server IP address or hostname, and the *filename* of the target dump file.

To save dump information via SFTP, enter:

```
Router# copy flash-dump sftp [data-port|extm-port|mgt-port] <server filename>
```

You are prompted for the SFTP server IP address or hostname, your *username* and *password*, and the *filename* of the target dump file.

To save dump information via FTP, enter:

```
Router# copy flash-dump ftp [data-port|extm-port|mgt-port] <server filename>
```

You are prompted for the FTP server IP address or hostname, your *username* and *password*, and the *filename* of the target dump file.

Clearing Dump Information

To clear dump information from flash memory, enter:

```
Router# clear flash-dump
```

The switch clears the dump region of flash memory and displays the following message:

```
FLASH dump region cleared.
```

If the flash dump region is already clear, the switch displays the following message:

```
FLASH dump region is already clear.
```

Unscheduled System Dumps

If there is an unscheduled system dump to flash memory, the following message is displayed when you log on to the switch:

```
Note: A system dump exists in FLASH. The dump was saved
      at 13:43:22 Wednesday January 30, 2010. Use show flash-dump
      uuencode to
      extract the dump for analysis and clear flash-dump to
      clear the FLASH region. The region must be cleared
      before another dump can be saved.
```

Appendix A. Networking OS System Log Messages

The EN4093 and EN4093R 10Gb Scalable Switch (EN4093 and EN4093R) uses the following syntax when outputting system log (syslog) messages:

<Time stamp><Log Label>IBMOS<Thread ID> : <Message>

The following parameters are used:

- *<Timestamp>*

The time of the message event is displayed in the following format:

<month (3 characters)> <day> <hour (1-24)> : <minute> : <second>

For example: Aug 19 14 : 20 : 30

- *<Log Label>*

The following types of log messages are recorded: LOG_CRIT, LOG_WARNING, LOG_ALERT, LOG_ERR, LOG_NOTICE, and LOG_INFO

- *<Thread ID>*

This is the software thread that reports the log message. For example:

stg, ip, console, telnet, vrrp, system, web server, ssh, bgp

- *<Message>*: The log message

Following is a list of potential syslog messages. To keep this list as short as possible, only the *<Thread ID>* and *<Message>* are shown. The messages are sorted by *<Log Label>*.

Where the *<Thread ID>* is listed as *mgmt*, one of the following may be shown: console, telnet, web server, or ssh.

LOG_ALERT

| Thread | LOG_ALERT Message |
|----------|---|
| | Possible buffer overrun attack detected! |
| BGP | session with <IP address> failed (bad event:<event>) |
| BGP | session with <IP address> failed <reason> Reasons: <ul style="list-style-type: none"> • Connect Retry Expire • Holdtime Expire • Invalid • Keepalive Expire • Receive KEEPALIVE • Receive NOTIFICATION • Receive OPEN • Receive UPDATE • Start • Stop • Transport Conn Closed • Transport Conn Failed • Transport Conn Open • Transport Fatal Error |
| HOTLINKS | LACP trunk <trunk ID> and <trunk ID> formed with admin key <key> |
| IP | cannot contact default gateway <IP address> |
| IP | Route table full |
| MGMT | Maximum number of login failures (<threshold>) has been exceeded. |
| OSPF | Interface IP <IP address>, Interface State {Down Loopback Waiting P To P DR BackupDR DR Other}: Interface down detached |
| OSPF | LS Database full: likely incorrect/missing routes or failed neighbors |
| OSPF | Neighbor Router ID <router ID>, Neighbor State {Down Attempt Init 2 Way ExStart Exchange Loading Full Loopback Waiting P To P DR BackupDR DR Other} |
| OSPF | OSPF Route table full: likely incorrect/missing routes |
| STP | CIST new root bridge |
| STP | CIST topology change detected |
| STP | Fast Forward port <port> active, putting port into forwarding state |
| STP | New preferred Fast Uplink port <port> active for STG <STG>, {restarting canceling} timer |
| STP | own BPDU received from port <port> |
| STP | Port <port>, putting port into blocking state |
| STP | Preferred STG <STG> Fast Uplink port has gone down. Putting secondary Fast Uplink port <port> into forwarding |

| Thread | LOG_ALERT Message (continued) |
|--------|---|
| STP | Setting STG <STG> Fast Uplink primary port <port> forwarding and backup port <port> blocking |
| STP | STG <STG> preferred Fast Uplink port <port> active. Waiting <seconds> seconds before switching from port <port> |
| STP | STG <STG> root port <port> has gone down. Putting backup Fast Uplink port <port> into forwarding |
| STP | STG <STG>, new root bridge |
| STP | STG <STG>, topology change detected |
| SYSTEM | LACP trunk <trunk ID> and <trunk ID> formed with admin key <key> |
| VRRP | Received <x> virtual routers instead of <y> |
| VRRP | received errored advertisement from <IP address> |
| VRRP | received incorrect addresses from <IP address> |
| VRRP | received incorrect advertisement interval <interval> from <IP address> |
| VRRP | received incorrect VRRP authentication type from <IP address> |
| VRRP | received incorrect VRRP password from <IP address> |
| VRRP | VRRP : received incorrect IP addresses list from <IP address> |

LOG_CRIT

| Thread | LOG_CRIT Message |
|--------|--|
| SSH | can't allocate memory in load_MP_INT() |
| SSH | currently not enough resource for loading RSA {private public key} |
| SYSTEM | System memory is at <n> percent |

LOG_ERR

| Thread | LOG_ERR Message |
|--------|---|
| CFG | Configuration file is EMPTY |
| CFG | Configuration is too large |
| CFG | Default VLAN cannot be a private-VLAN. |
| CFG | Error writing active config to FLASH! Configuration is too large |
| CFG | Error writing active config to FLASH! Unknown error |
| CFG | TFTP {Copy cfgRcv} attempting to redirect a previously redirected output |
| MGMT | Apply is issued by another user. Try later |
| MGMT | Critical Error. Failed to add Interface <interface> |
| MGMT | Diff is issued by another user. Try later |
| MGMT | Dump is issued by another user. Try later |
| MGMT | Error: Apply not done |
| MGMT | Error: Save not done. |
| MGMT | Firmware download failed (insufficient memory |
| MGMT | Revert Apply is issued by another user. Try later |
| MGMT | Revert is issued by another user. Try later. |
| MGMT | Save is issued by another user. Try later |
| NTP | unable to listen to NTP port |
| STP | Cannot set "{Hello Time Max Age Forward Delay Aging}" (Switch is in MSTP mode) |
| SYSTEM | Error: BOOTP Offer was found incompatible with the other IP interfaces |
| SYSTEM | I2C device <ID> <description> set to access state <state> [from CLI] |
| SYSTEM | Not enough memory! |

LOG_INFO

| Thread | LOG_INFO Message |
|----------|--|
| | System log cleared by user <i><username></i> . |
| | System log cleared via SNMP. |
| HOTLINKS | "Error" is set to "{Active Standby}" |
| HOTLINKS | "Learning" is set to "{Active Standby}" |
| HOTLINKS | "None" is set to "{Active Standby}" |
| HOTLINKS | "Side Max" is set to "{Active Standby}" |
| HOTLINKS | has no "{Side Max None Learning Error}" interface |
| MGMT | <i>/* Config changes at <time> by <username> */ <config diff> /* Done */</i> |
| MGMT | <i><username></i> ejected from BBI |
| MGMT | <i><username></i> (<i><user type></i>) {logout ejected idle timeout connection closed} from {Console Telnet/SSH} |
| MGMT | <i><username></i> (<i><user type></i>) login {on Console from host <i><IP address></i> } |
| MGMT | boot kernel download completed. Now writing to flash. |
| MGMT | boot kernel downloaded {from host <i><hostname></i> via browser}, filename too long to be displayed, software version <i><version></i> |
| MGMT | boot kernel downloaded from host <i><hostname></i> , file' <i><filename></i> ', software version <i><version></i> |
| MGMT | Can't downgrade to image with only single flash support |
| MGMT | Could not revert unsaved changes |
| MGMT | Download already currently in progress. Try again later via {Browser BBI} |
| MGMT | Error in setting the new config |
| MGMT | Failed to allocate buffer for diff track. |
| MGMT | Firmware download failed to {invalid image image1 image2 boot kernel undefined SP boot kernel} |
| MGMT | Firmware downloaded to {invalid image image1 image2 boot kernel undefined SP boot kernel}. |
| MGMT | Flash dump successfully tftp'd to <i><hostname></i> : <i><filename></i> |
| MGMT | FLASH ERROR - invalid address used |
| MGMT | Flash Read Error. Failed to read flash into holding structure. Quitting |

| Thread | LOG_INFO Message (continued) |
|--------|---|
| MGMT | Flash Write Error |
| MGMT | Flash Write Error. Failed to allocate buffer. Quitting |
| MGMT | Flash Write Error. Trying again |
| MGMT | image1 2 download completed. Now writing to flash. |
| MGMT | image1 2 downloaded {from host <hostname> via browser}, filename too long to be displayed, software version <version> |
| MGMT | image1 2 downloaded from host <hostname>, file '<filename>', software version <version> |
| MGMT | Incorrect image being loaded |
| MGMT | Invalid diff track address. Continuing with apply() |
| MGMT | Invalid image being loaded for this switch type |
| MGMT | invalid image download completed. Now writing to flash. |
| MGMT | invalid image downloaded {from host <hostname> via browser}, filename too long to be displayed, software version <version> |
| MGMT | invalid image downloaded from host <hostname>, file '<filename>', software version <version> |
| MGMT | New config set |
| MGMT | new configuration applied [from BBI EM SCP SNMP Stacking Master] |
| MGMT | new configuration saved from {BBI ISCLI SNMP} |
| MGMT | scp<username>(<user type>) {logout ejected idle timeout connection closed} from {Console Telnet/SSH} |
| MGMT | scp<username>(<user type>) login {on Console from host <IP address>} |
| MGMT | SP boot kernel download completed. Now writing to flash. |
| MGMT | SP boot kernel downloaded {from host <hostname> via browser}, filename too long to be displayed, software version <version> |
| MGMT | SP boot kernel downloaded from host <hostname>, file '<filename>', software version <version> |
| MGMT | Starting Firmware download for {invalid image image1 image2 boot kernel undefined SP boot kernel}. |
| MGMT | Static FDB entry on disabled VLAN |
| MGMT | Tech support dump failed |
| MGMT | Tech support dump successfully tftp'd to <hostname>:<filename> |
| MGMT | Two Phase Apply Failed in Creating Backup Config Block. |

| Thread | LOG_INFO Message (continued) |
|--------|--|
| MGMT | undefined download completed. Now writing to flash. |
| MGMT | undefined downloaded {from host <hostname> via browser}, filename too long to be displayed, software version <version> |
| MGMT | undefined downloaded from host <hostname>, file '<filename>', software version <version> |
| MGMT | unsaved changes reverted [from BBI from SNMP] |
| MGMT | Unsupported GBIC {accepted refused} |
| MGMT | user {SNMP user <username>} ejected from BBI |
| MGMT | Watchdog has been {enabled disabled} |
| MGMT | Watchdog timeout interval is now <seconds> seconds) |
| MGMT | Wrong config file type |
| SSH | <username>(<user type>) {logout ejected idle timeout connection closed} from {Console Telnet/SSH} |
| SSH | <username>(<user type>) login {on Console from host <IP address>} |
| SSH | Error in setting the new config |
| SSH | New config set |
| SSH | scp<username>(<user type>) {logout ejected idle timeout connection closed} from {Console Telnet/SSH} |
| SSH | scp<username>(<user type>) login {on Console from host <IP address>} |
| SSH | server key autogen {starts completes} |
| SSH | Wrong config file type |
| SYSTEM | booted version <version> from Flash image <image>, {active backup factory} config block |

LOG_NOTICE

| Thread | LOG_NOTICE Message |
|----------|---|
| | ARP table is full. |
| | Current config successfully tftp'd <filename> from <hostname> |
| | Current config successfully tftp'd to <hostname>: <filename> |
| | Port <port> mode is changed to full duplex for 1000 Mbps operation. |
| CONSOLE | RADIUS: authentication timeout. Retrying... |
| CONSOLE | RADIUS: failed to contact primary secondary server |
| CONSOLE | RADIUS: No configured RADIUS server |
| CONSOLE | RADIUS: trying alternate server... |
| HOTLINKS | "Error" is set to "Standby Active" |
| HOTLINKS | "Learning" is set to "Standby Active" |
| HOTLINKS | "None" is set to "Standby Active" |
| HOTLINKS | "Side Max" is set to "Standby Active" |
| HOTLINKS | has no "{Side Max None Learning Error}" interface |
| MGMT | <username> automatically logged out from BBI because changing of authentication type |
| MGMT | <username>(<user type>) {logout ejected idle timeout connection closed} from {BBI Console Telnet/SSH} |
| MGMT | <username>(<user type>) login {on Console from host <IP address> from BBI} |
| MGMT | Authentication failed for backdoor. |
| MGMT | Authentication failed for backdoor. Password incorrect! |
| MGMT | Authentication failed for backdoor. Telnet disabled! |
| MGMT | boot config block changed |
| MGMT | boot image changed |
| MGMT | boot mode changed |
| MGMT | enable password changed |
| MGMT | Error in setting the new config |
| MGMT | Failed login attempt via {BBI TELNET} from host <IP address>. |
| MGMT | Failed login attempt via the CONSOLE |
| MGMT | FLASH Dump cleared from BBI |

| Thread | LOG_NOTICE Message (continued) |
|--------|---|
| MGMT | New config set |
| MGMT | packet-buffer statistics cleared |
| MGMT | PANIC command from CLI |
| MGMT | PASSWORD FIX-UP MODE IN USE |
| MGMT | Password for {oper operator} changed by {SNMP user <username>}, notifying admin to save. |
| MGMT | QSFP: Port <port> changed to {10G 40G}, from {BBI SNMP CLI}. |
| MGMT | RADIUS server timeouts |
| MGMT | RADIUS: authentication timeout. Retrying... |
| MGMT | RADIUS: failed to contact {primary secondary} server |
| MGMT | RADIUS: No configured RADIUS server |
| MGMT | RADIUS: trying alternate server... |
| MGMT | scp<username>(<user type>) {logout ejected idle timeout connection closed} from {Console Telnet/SSH} |
| MGMT | scp<username>(<user type>) login {on Console from host <IP address>} |
| MGMT | second syslog host changed to {this host <IP address>} |
| MGMT | selectable [boot] mode changed |
| MGMT | STP BPDU statistics cleared |
| MGMT | switch reset from CLI |
| MGMT | syslog host changed to {this host <IP address>} |
| MGMT | System clock set to <time>. |
| MGMT | System date set to <date>. |
| MGMT | Terminating BBI connection from host <IP address> |
| MGMT | User <username> deleted by {SNMP user <username>}. |
| MGMT | User <username> is {deleted disabled} and will be ejected by {SNMP user <username>} |
| MGMT | User {oper operator} is disabled and will be ejected by {SNMP user <username>}. |
| MGMT | Wrong config file type |
| NTP | System clock updated |
| OSPF | Neighbor Router ID <router ID>, Neighbor State {Down Loopback Waiting P To P DR BackupDR DR Other Attempt Init 2 Way ExStart Exchange Loading Full} |

| Thread | LOG_NOTICE Message (continued) | | |
|--|---|--|---|
| SERVER | link {down up} on port <port> | | |
| SSH | (remote disconnect msg) | | |
| SSH | <username>(<user type>) {logout ejected idle timeout connection closed} from {Console Telnet/SSH} | | |
| SSH | <username>(<user type>) login {on Console from host <IP address>} | | |
| SSH | Error in setting the new config | | |
| SSH | Failed login attempt via SSH | | |
| SSH | New config set | | |
| SSH | scp<username>(<user type>) {logout ejected idle timeout connection closed} from {Console Telnet/SSH} | | |
| SSH | scp<username>(<user type>) login {on Console from host <IP address>} | | |
| SSH | Wrong config file type | | |
| SYSTEM | Change fiber GIG port <port> mode to full duplex | | |
| SYSTEM | Change fiber GIG port <port> speed to 1000 | | |
| SYSTEM | Changed ARP entry for IP <IP address> to: MAC <MAC address>, Port <port>, VLAN <VLAN> | | |
| SYSTEM | Enable auto negotiation for copper GIG port: <port> | | |
| SYSTEM | I2C device <ID> <description> set to access state <state> [from CLI] | | |
| SYSTEM | Port <port> disabled | | |
| SYSTEM | Port <port> disabled due to reason code <reason code> | | |
| SYSTEM | rebooted (<reason>)[, administrator logged in] Reason: <table border="0" style="width: 100%;"> <tr> <td style="vertical-align: top;"> <ul style="list-style-type: none"> • Boot watchdog reset • console PANIC command • console RESET KEY • hard reset by SNMP • hard reset by WEB-UI • hard reset from console • hard reset from Telnet • low memory • MM Cycled Power Domain • power cycle • Reset Button was pushed • reset by SNMP • reset by WEB-UI </td> <td style="vertical-align: top;"> <ul style="list-style-type: none"> • reset from console • reset from EM • reset from Telnet/SSH • scheduled reboot • SMS-64 found an over-voltage • SMS-64 found an under-voltage • software ASSERT • software PANIC • software VERIFY • Telnet PANIC command • unknown reason • watchdog timer </td> </tr> </table> | <ul style="list-style-type: none"> • Boot watchdog reset • console PANIC command • console RESET KEY • hard reset by SNMP • hard reset by WEB-UI • hard reset from console • hard reset from Telnet • low memory • MM Cycled Power Domain • power cycle • Reset Button was pushed • reset by SNMP • reset by WEB-UI | <ul style="list-style-type: none"> • reset from console • reset from EM • reset from Telnet/SSH • scheduled reboot • SMS-64 found an over-voltage • SMS-64 found an under-voltage • software ASSERT • software PANIC • software VERIFY • Telnet PANIC command • unknown reason • watchdog timer |
| <ul style="list-style-type: none"> • Boot watchdog reset • console PANIC command • console RESET KEY • hard reset by SNMP • hard reset by WEB-UI • hard reset from console • hard reset from Telnet • low memory • MM Cycled Power Domain • power cycle • Reset Button was pushed • reset by SNMP • reset by WEB-UI | <ul style="list-style-type: none"> • reset from console • reset from EM • reset from Telnet/SSH • scheduled reboot • SMS-64 found an over-voltage • SMS-64 found an under-voltage • software ASSERT • software PANIC • software VERIFY • Telnet PANIC command • unknown reason • watchdog timer | | |

| Thread | LOG_NOTICE Message (continued) |
|---------|---|
| SYSTEM | Received BOOTP Offer: IP: <IP address>, Mask: <netmask>, Broadcast <IP address>, GW: <IP address> |
| SYSTEM | Watchdog threshold changed from <old value> to <new value> seconds |
| SYSTEM | Watchdog timer has been enabled |
| TEAMING | error, action is undefined |
| TEAMING | is down, but teardown is blocked |
| TEAMING | is down, control ports are auto disabled |
| TEAMING | is up, control ports are auto controlled |
| VLAN | Default VLAN can not be deleted |
| VRRP | virtual router <IP address> is now {BACKUP MASTER} |
| WEB | <username> ejected from BBI |
| WEB | RSA host key is being saved to Flash ROM, please don't reboot the box immediately. |

LOG_WARNING

| Thread | LOG_WARNING Message |
|----------|--|
| CFG | Authentication should be disabled to run RIPv2 in RIPv1 compatibility mode on interface <i><interface></i> . |
| CFG | Multicast should be disabled to run RIPv2 in RIPv1 compatibility mode on interface <i><interface></i> . |
| HOTLINKS | "Error" is set to "Standby Active" |
| HOTLINKS | "Learning" is set to "Standby Active" |
| HOTLINKS | "None" is set to "Standby Active" |
| HOTLINKS | "Side Max" is set to "Standby Active" |
| HOTLINKS | has no "{Side Max None Learning Error}" interface |
| NTP | cannot contact [primary secondary] NTP server <i><IP address></i> |
| SYSTEM | I2C device <i><ID></i> <i><description></i> set to access state <i><state></i> [from CLI] |
| TEAMING | error, action is undefined |
| TEAMING | is down, but teardown is blocked |
| TEAMING | is down, control ports are auto disabled |
| TEAMING | is up, control ports are auto controlled |

Appendix B. Getting help and technical assistance

If you need help, service, or technical assistance or just want more information about IBM products, you will find a wide variety of sources available from IBM to assist you. This section contains information about where to go for additional information about IBM and IBM products, what to do if you experience a problem with your system, and whom to call for service, if it is necessary.

Before you call

Before you call, make sure that you have taken these steps to try to solve the problem yourself:

- Check all cables to make sure that they are connected.
- Check the power switches to make sure that the system and any optional devices are turned on.
- Use the troubleshooting information in your system documentation, and use the diagnostic tools that come with your system. Information about diagnostic tools is in the *Problem Determination and Service Guide* on the *IBM Documentation CD* that comes with your system.
- Go to the IBM support website at <http://www.ibm.com/systems/support/> to check for technical information, hints, tips, and new device drivers or to submit a request for information.

You can solve many problems without outside assistance by following the troubleshooting procedures that IBM provides in the online help or in the documentation that is provided with your IBM product. The documentation that comes with IBM systems also describes the diagnostic tests that you can perform. Most systems, operating systems, and programs come with documentation that contains troubleshooting procedures and explanations of error messages and error codes. If you suspect a software problem, see the documentation for the operating system or program.

Using the documentation

Information about your IBM system and pre-installed software, if any, or optional device is available in the documentation that comes with the product. That documentation can include printed documents, online documents, ReadMe files, and Help files. See the troubleshooting information in your system documentation for instructions for using the diagnostic programs. The troubleshooting information or the diagnostic programs might tell you that you need additional or updated device drivers or other software. IBM maintains pages on the World Wide Web where you can get the latest technical information and download device drivers and updates. To access these pages, go to <http://www.ibm.com/systems/support/> and follow the instructions. Also, some documents are available through the IBM Publications Center at <http://www.ibm.com/shop/publications/order/>.

Getting help and information on the World Wide Web

On the World Wide Web, the IBM website has up-to-date information about IBM systems, optional devices, services, and support. The address for IBM System x[®] and xSeries[®] information is <http://www.ibm.com/systems/x/>. The address for IBM BladeCenter information is <http://www.ibm.com/systems/bladecenter/>. The address for IBM IntelliStation[®] information is <http://www.ibm.com/intellistation/>.

You can find service information for IBM systems and optional devices at <http://www.ibm.com/systems/support/>.

Software service and support

Through IBM Support Line, you can get telephone assistance, for a fee, with usage, configuration, and software problems with System x and x Series servers, BladeCenter products, IntelliStation workstations, and appliances. For information about which products are supported by Support Line in your country or region, see <http://www.ibm.com/services/sl/products/>.

For more information about Support Line and other IBM services, see <http://www.ibm.com/services/>, or see <http://www.ibm.com/planetwide/> for support telephone numbers. In the U.S. and Canada, call 1-800-IBM-SERV (1-800-426-7378).

Hardware service and support

You can receive hardware service through your IBM reseller or IBM Services. To locate a reseller authorized by IBM to provide warranty service, go to <http://www.ibm.com/partnerworld/> and click **Find Business Partners** on the right side of the page. For IBM support telephone numbers, see <http://www.ibm.com/planetwide/>. In the U.S. and Canada, call 1-800-IBM-SERV (1-800-426-7378).

In the U.S. and Canada, hardware service and support is available 24 hours a day, 7 days a week. In the U.K., these services are available Monday through Friday, from 9 a.m. to 6 p.m.

IBM Taiwan product service

台灣 IBM 產品服務聯絡方式：
台灣國際商業機器股份有限公司
台北市松仁路7號3樓
電話：0800-016-888

IBM Taiwan product service contact information:

IBM Taiwan Corporation
3F, No 7, Song Ren Rd.
Taipei, Taiwan
Telephone: 0800-016-888

Index

Numerics

802.1p
 and ETS 462
 configuration 297, 319
 DCBX PFC information 134
 information 99, 100, 137
 PFC configuration 463
 Priority Group mapping 137
 priority level 284, 303, 313
 IPv6 307
 priority value 321
 re-marking the value (IPv6) 310

802.1s
 information 50, 52

802.1w
 information 50, 52

802.1X
 configuration 325
 guest VLAN 327
 information 35, 48
 operations-level commands 505
 port configuration 328

A

abbreviating commands (CLI) 9

access control
 switch 277
 user 278

Access Control List (see ACL) 101

ACL
 add group 290
 and VMAP 313
 configuration 302
 delete 506
 Ethernet matching criteria 304
 filtering criteria 303
 groups 302
 information 101, 102
 IPv4 matching criteria 305
 IPv6 307
 list of FIPS ACLs 139, 140
 management ACL filtering 311
 metering configuration 318
 Packet Format matching criteria 307
 port ACL configuration 290
 port configuration commands 290
 QoS parameters 290
 re-marking 319
 re-marking (IPv6) 310, 321
 remove group 290
 statistics 230, 231
 TCP matching criteria 306
 UDP matching criteria 306

active

 configuration block 245, 525
 IP interface 435
 switch configuration
 ptcfg 501
 restoring 502
 saving and loading 502
 VLAN port 435

addr (IP route tag) 63

administrator account 10

aging (STP information) 51, 53

autonomous system filter path
 action 382
 as 382
 aspath 382

B

backup configuration block 525

bandwidth allocation, Priority Groups 462

BGP 63
 aggregation configuration 403
 configuration 397
 eBGP 397
 filters, aggregation configuration 403
 iBGP 397
 in route 400
 IP address, border router 399
 keep-alive time 399
 operations-level commands 508
 peer 397
 peer configuration 399
 redistribution configuration 402
 remote autonomous system 399
 route reflector client 399
 router hops 400

bgp (IP route tag) 63

boot
 options 517 to 531

Boot Management menu 529

BOOTP
 configuration 427
 relay broadcast domain configuration 427

Bootstrap Protocol (see BOOTP) 427

Border Gateway Protocol (see BGP) 4

BPDU
 how often transmitted 50

bridge priority 50, 55

Bridge Protocol Data Unit (BPDU) 55, 336

Bridge Protocol Data Unit (see BPDU) 50

Bridge Spanning-Tree parameters 336

broadcast (IP route tag) 64

broadcast (IP route type) 63

C

capture dump information to a file 548

CEE

- and stacking 518
- configuration 461
- DCBX 539
- information 130

Cisco Ether Channel 345

CIST information 54

clear

- ACL statistics 230
- all defined management networks 277
- all IP statistics 172
- all IPv4 statistics 170, 173
- all IPv6 statistics 176
- ARP statistics 171
- DNS statistics 172
- dump information 550
- FCoE statistics 232
- Hot Links statistics 163
- ICMP statistics 172
- IGMP statistics 172
- LACP statistics 163
- MLD statistics 190
- OSPF statistics 172
- RIP statistics 172
- static route 373
- statistics for specific ports 145
- statistics on a specific trunk group 162
- TCP statistics 172
- UDP statistics 172
- VRRP statistics 172

commands

- abbreviations 9
- conventions used in this manual xvi
- help with 7
- shortcuts 9
- tab completion 9

configuration

- 802.1X 325
- CIST 333
- commands 243 to 502
- default gateway interval, for health checks 372
- default gateway IP address 372
- dump command 500
- failover 353
- flow control 288, 294
- IGMP 406
- IP static route 373
- port link speed 287
- port mirroring 323
- port trunking 345
- RIP 383
- RIP commands 384
- save changes 245
- SNMP 263
- switch IP address 368
- TACACS+ 255

VLAN default (PVID) 284

VLAN IP interface 368

VLAN tagging 285

VMware 483

VRRP 429

configuration block

- active 525
- backup 525
- factory 525
- selection 525

Control Plane Protection, configuration 299

Converged Enhanced Ethernet (see CEE) 130

COPP, configuration 299

COS queue information 100

cost

STP information 51, 53

cost (STP information) 55

CPU use

history 229

statistics 226, 229

D

daylight saving time 246

DCB Capability Exchange Protocol (see DCBX) 130

DCBX

Application Protocol information 135

configuration 464

control information 131

debugging 539

ETS information 132

feature information 132

information 130

PFC information 134

debugging 533

default gateway

information 60

interval, for health checks 372

IPv6 442

default password 10

delete

ACL statistics 230

all defined management networks 277

all IP statistics 172

all IPv4 statistics 170, 173

all IPv6 statistics 176

ARP statistics 171

DNS statistics 172

dump information 550

Hot Links statistics 163

ICMP statistics 172

IGMP statistics 172

LACP statistics 163

MLD statistics 190

OSPF statistics 172

RIP statistics 172

static route 373

statistics for specific ports 145

- statistics on a specific trunk group 162
 - TCP statistics 172
 - UDP statistics 172
 - VRRP statistics 172
- DHCP
 - and BOOTP commands 427
 - and managed address configuration flag 370
 - and Netboot configuration 520
 - and other stateful configuration flag 370
 - binding table information 90
 - packets logged 222
- DiffServ Code Point (see DSCP) 298
- direct (IP route type) 63
- directed broadcasts 377
- DISC (port state) 51
- disconnect idle timeout 12
- downloading software 522
- DSCP
 - configuration 298
 - disable for in-profile traffic 320
 - disable for out-profile traffic 320
 - re-mark for in-profile traffic 322
 - re-marking configuration 284, 298
 - set value of in-profile packets 320
 - set value of out-profile packets 320
- dump
 - configuration command 500
 - maintenance 533
- duplex mode
 - interface status 13
 - link status 112
- Dynamic Host Configuration Protocol (see DHCP) 427
- dynamic routes 541

E

- ECMP route information 80
- ECN (Explicit Congestion Notification) 300
- ECP
 - configuration 341
- Edge Virtual Bridging, configuration 485
- Enhanced Transmission Selection (see ETS) 137
- ENode 467
- Error Disable and Recovery
 - port 287
 - system 249
- EtherChannel, and port trunking 345
- ETS
 - configuration 462
 - information 130, 132, 137
 - Priority Group configuration 462
- EVB
 - configuration 485
 - configuration mode 5
 - information 121
- Explicit Congestion Notification (ECN) 300

F

- factory configuration block 525
- failover
 - auto monitor configuration 354
 - configuration 353
 - Layer 2 configuration 353
 - Layer 2 information 36, 41
 - manual monitor port configuration 355
 - trigger configuration 354
 - uplink, for vNIC group 475
- FCF port 467
- FCoE
 - configuration 466
 - FIPS port configuration 467
 - forwarding 467
 - information 139
 - Initialization Protocol (see FIP) 467
 - statistics 232
- FDB
 - configuration 338
 - configuring static entries 339
 - hot links update 357
 - information 37
 - learning 285
 - maintenance 533, 535
 - troubleshooting 533, 535
- Fiber Channel Initialization Protocol (see FIP) 139
- Fibre Channel over Ethernet (see FCoE) 139
- FIP
 - Snooping (see FIPS) 467
 - snooping information 139
- FIPS
 - list of ACLs 139
 - port configuration 467
- fixed (IP route tag) 63
- flag field 65
- flow control
 - configuring 288, 294
 - configuring for port link 287
 - configuring management port 293
 - information 13, 112
 - Ingress Back Pressure 156
 - pause packets 154, 155
 - priority (see PFC) 134
- Forwarding Database (see FDB) 37
- forwarding state
 - (FWD) 55
- forwarding state (FWD) 38, 51, 56
- FWD (port state) 38, 51
- fwd (STP bridge option) 337
- FwdDel (forward delay), bridge port 51, 53, 55

G

- getting help 567
- gtcfg (TFTP load command) 502

H

- hardware service and support 572
- health checks
 - default gateway interval, retries 372
 - retry, number of failed health checks 372
- hello (STP information) 50, 53, 55
- help
 - getting 567
 - online 7
- Hot Links configuration 357
- hot-standby failover 433
- http
 - controlling access 275
 - port 275
- HTTPS 281

I

- IBM support line 571
- ICMP statistics 184
- idle timeout, setting 12
- IEEE standards
 - 802.1d 330
 - 802.1p 297
 - 802.1X 48, 50
- IGMP
 - advanced parameters 415
 - configuration 406
 - filter definition commands 413
 - filtering configuration 412
 - filtering port configuration 414
 - group information 83
 - group maintenance 543
 - mrouter maintenance commands 544
 - multicast group information 81
 - multicast
 - group information 81
 - multicast router information 84
 - relay configuration 409
 - relay mrouter configuration 410
 - snooping configuration 407
 - static mrouter configuration 411
 - statistics 188
- IGMPv3
 - and stacking mode 518
 - configuration 408
 - information 83
 - snooping information 544
 - statistics 188
- IKEv2
 - configuration 418
 - configuration mode 5
 - debugging 538
 - identification configuration 419
 - information 60, 92
 - information commands 91
 - preshare key configuration 419
 - proposal configuration 418
- image
 - downloading 522
 - software, selecting 523
- indirect (IP route type) 63
- information
 - VMware 119
- Information Commands 13 to 141
- Interface change stats 200
- IP address
 - ARP information 64
 - configuring default gateway 372
- IP forwarding
 - configuration 377
 - directed broadcasts 377
 - information 60
- IP Information 60, 89
- IP interfaces 63
 - active 435
 - configuring address 368
 - configuring VLANs 368
 - information 60
 - IP route tag 63
 - priority increment value (ifs) for VRRP 437
- IP network filter configuration 378
- IP route
 - manipulation 541
 - tag parameters 63
- IP Static Route commands 373
- IP statistics 173
- IPMC group information 84
- IPsec
 - configuration 420
 - debugging 538
 - dynamic policy configuration 423
 - information 93
 - Layer 3 configuration 454
 - manual policy configuration 424
 - manual policy information 94
 - traffic selector configuration 422
 - transform set configuration 421
- IPv6
 - ACL configuration 307
 - default gateway configuration 442
 - interface information 88
 - Neighbor Discovery
 - cache configuration 443
 - cache information 79
 - cache information commands 79
 - cache manipulation 546
 - configuration commands 370
 - prefix configuration 444
 - prefix information 80
 - Path MTU
 - configuration 444
 - information 88
 - re-mark configuration 310
 - re-marking

- configuration 321
 - in-profile configuration 322
- routing information 78
- static route 443
- statistics 176
- IPv6 route 182
- ISCLI command modes 3

L

- LACP
 - add trunk to vNIC Group 475
 - admin key
 - add to Auto Monitor 354
 - add to Backup interface 360
 - add to Manual Monitor Control 356
 - add to Manual Monitor Port 355
 - add to Master interface 359
 - add to VM group 480
 - remove from Auto Monitor 354
 - remove from Manual Monitor Control 356
 - remove from Manual Monitor Port 355
 - remove from VM group 480
 - aggregator information 40
 - and trunk hash configuration 346
 - configuration 351
 - information 40
 - port configuration 352
 - port status information 40
 - remove trunk from vNIC group 475
 - show trunk groups 36
 - statistics 163, 164
 - virtual (see vLAG) 348
- Layer 2 commands 35
- Layer 3 commands 59
- LDAP server configuration 258
- Lightweight Directory Access Protocol (see LDAP) 258
- Link Aggregation Control Protocol (see LACP) 36
- Link Layer Discovery Protocol (see LLDP) 43
- link speed, configuring 287
- link status 13
 - command 112
 - duplex mode 13, 112
 - information 112
 - port speed 13, 112
- linkt (SNMP option) 264
- LLDP
 - and stacking mode 518
 - cache manipulation commands 542
 - configuration 341
 - disable 342
 - enable 342
 - information 43
 - packets received 217
 - PDU's logged 223
 - remote device information 44
 - statistics 163, 166
 - TLV configuration 343

- local (IP route type) 63
- log, syslog messaging options 251
- LRN (port state) 51, 55

M

- MAC address
 - ARP information 64
 - display 14
 - FDB information 37
 - FDB maintenance 535
 - multicast, configuring 340
 - switch management processor 25
- MAC address spoof prevention 481
- Maintenance commands 533
- Management Processor (see MP) 14
- manual style conventions xvi
- martian
 - IP route tag (filtered) 64
 - IP route type (filtered out) 63
- MaxAge (STP information) 51, 53, 55
- MD5
 - cryptographic authentication 389
 - key 392
 - key configuration, OSPF 396
- meter
 - ACL
 - configuring 318
 - current parameters 318
 - delete 318
 - log, configuring 318
 - port metering 314
 - configuring vNIC bandwidth 473
 - readiness 529
- Miscellaneous Debug commands 537
- MLD
 - configuration 404
 - configuration mode 5
 - global statistics 191
 - information 60, 85
 - mrouter information 86
 - statistics 190
- monitor port 323
- MP
 - display MAC address 14, 25
 - packet statistics 213
 - snap trace buffer 537
 - statistics 212
 - trace buffer 537
- Mrouter information 84
- MTU 444
- multicast
 - IP route type 63
 - router information 84
 - static MAC configuration 340
- Multicast Listener Discovery protocol (see MLD) 5
- multiple management VLANs 361
- mxage (STP bridge option) 336

N

- nbr change statistics 199
- Neighbor Discovery
 - cache configuration, IPv6 443
 - cache manipulation, IPv6 546
 - IPv6, configuration 370
 - prefix 444
- Neighbor Discovery prefix 444
- notice 247
- NTP synchronization 262

O

- OAM
 - information 46
 - statistics 144, 163, 167
- online help 7
- OpenFlow
 - configuration 487
 - configuration mode 5
 - information 103
 - flow allocation 104
 - flow configuration 105
 - flow tables 106
 - global configuration 104
 - static flows 492
 - actions 494
 - qualifiers 493
 - statistics 204
- Operations commands 503
- operations-level
 - 802.1X port commands 505
 - BGP commands 508
 - port commands 504
 - VRRP options 507
- OSPF
 - and stacking mode 518
 - area index 389
 - authentication key 392
 - configuration 387
 - host entry 395
 - interface 392
 - MD5 key 396
 - route redistribution 396
 - summary range 391
 - virtual link 394
 - cost of the selected path 392
 - cost value of the host 395
 - dead
 - declaring a silent router to be down 392
 - health parameter of a hello packet 394
 - export 396
 - fixed routes 397
 - general information 70
 - hello, authentication parameter of a hello packet 394
 - host routes 387
 - information
 - commands 68

- database 71
 - general 69
 - interface 70
 - interface loopback 70
 - route 72
- interface 387
- link state database 387, 447
- Not-So-Stubby Area 389, 448
- priority value of the switch interface 392
- range number 387
- SPF, shortest path first 389
- statistics
 - commands 193
 - delete 172
 - global 194
- stub area 389, 448
- transit area 389, 448
- transit delay 392
- type 389
- virtual link 387
- virtual neighbor, router ID 394

- ospf (IP route tag) 63
- OSPFv3
 - and stacking mode 518
 - configuration 446
 - area index 448
 - interface 452
 - virtual link 456
- dead
 - declaring a silent router to be down 453
 - health parameter of a hello packet 456
- hello, authentication parameter of a hello packet 456
- information
 - commands 73
 - database 75
 - dump of 74
 - interface 75
 - route 76
- statistics
 - commands 197
 - global 198
- type 448
- virtual neighbor, router ID 456

P

- parameters
 - tag 63
 - type 63
- passwords 10
 - administrator account 10
 - changing 278
 - default 10
 - user account 10
- Path MTU 444
- path-cost (STP port option) 337
- PFC configuration 463
- PIM mode 438

- ping 7
- poisoned reverse, as used with split horizon 384
- port
 - ACL configuration 290
 - configuration 284
 - disabling temporarily 288
 - Error Disable and Recovery 287
 - failover manual monitor configuration 355
 - FIPS configuration 467
 - HTTP 275
 - IGMP filtering configuration 414
 - information 114
 - LACP
 - configuration 352
 - status information 40
 - link configuration 287
 - link speed, configuring 287
 - management, configuring 293
 - membership of the VLAN 36, 58
 - mirroring, configuring 323
 - number 112
 - priority 51, 55
 - reference 38
 - speed 13, 112
 - state information 38
 - telnet 276
 - TFTP 276
 - trunking
 - configuration 345
 - description 345
 - VLAN ID 13, 114
- port ECN configuration 292
- port WRED configuration 292
- preemption
 - assuming VRRP master routing authority 432
 - hot links trigger, configuring 358
 - virtual router, configuring 431
 - VRRP, configuring 434
- Priority Flow Control 463
- Priority Groups
 - 802.1p mapping to 137
 - configuration 462
 - information 132
- Private VLAN 365
- Protected Mode 509
- Protocol-based VLAN (see PVLAN) 363
- ptcfg (TFTP save command) 501
- PTP
 - configuration 497
 - statistics 239
- PVID (port VLAN ID) 13, 114
- PVLAN
 - configuration 361, 363
 - current parameters 364

Q

QoS

- ACL parameters 290
- configuration 290, 297
- control plane protection 299
- DSCP configuration 298
- ECN information 100
- information 99
- transmit-queue information 99
- WRED information 100

R

- RADIUS server
 - 802.1X response timeout, setting 326
 - and 802.1X configuration 325
 - configuration commands 253
 - current parameters 254
 - packets logged 222
 - primary 253
 - shared secret 253
- receive flow control 288, 294
- reference ports 38
- re-mark
 - ACL
 - configuration 316, 319
 - parameters 102
 - DSCP
 - configuration 284
 - global configuration 298
 - in-profile
 - configuration 320
 - settings 316
 - IPv6 ACL 310
 - configuration 321
 - in-profile configuration 322
 - out-of-profile
 - configuration 320
 - settings 316
 - TOS precedence, configuring 316
 - user update priority 316
- Remote Monitoring (RMON) 468
- Rendezvous Point (RP) 439
- retries
 - health checks for default gateway 372
 - radius server 253
- RIP
 - and stacking mode 518
 - configuration 383, 384
 - BGP redistribution 402
 - route redistribution 386
 - configuration mode 4, 383
 - information 77
 - interface 77
 - routes 77
 - user configuration 59, 77
 - IPv4 route statistics 181
 - packets logged 223
 - poisoned reverse 384
 - split horizon 384

- statistics 171, 172, 203
- version 384
- rip (IP route tag) 63
- RMON
 - configuration 468
 - information 108
- route statistics
 - IPv4 181
 - IPv6 182
- router hops 400
- Routing Information Protocol (see RIP) 4
- RSTP information 52
- Rx/Tx statistics 194, 198

S

- save (global command) 245
- secret, RADIUS server 253
- Secure Shell 252
- service and support 572
- shortcuts (CLI) 9
- SLP
 - configuration 498
 - information 124
 - statistics 240
- snap trace buffer 537
- SNMP
 - configuration
 - commands 263
 - current 264
 - link traps 264
 - location 263
 - read community string 263
 - source interface for traps 264
 - system authentication trap 264
 - system contact 263
 - timeout 264
 - trap host server 264
 - version 266
 - write community string 264
 - options 263
 - statistics 234
- SNMPv3
 - configuration
 - access rights 265
 - commands 265
 - community table 265, 271
 - destination 266
 - display 266
 - group 265, 270
 - MIB views 265
 - Notify table 274
 - parameters 266
 - target address table 272
 - target parameters 273
 - user access 269
 - user security 267
 - USM 265, 267

- version 266
- view 268
- information 24
 - access 20
 - commands 17
 - community table 21
 - group 20
 - Notify table 23
 - target address table 21
 - target parameters table 23
 - USM user table 18
 - View Table 19
- software
 - image 522
 - image file and version 14, 25
 - service and support 571
 - upgrade recovery 529
- Spanning Tree protocol (see STP) 50
- SPAR. *See* Switch Partition.
- split horizon 384
- Stacking
 - boot options 517
 - configuration 295
- state (STP information) 51, 53, 55
- static (IP route tag) 63
- static multicast MAC 340
- static route
 - add 373
 - delete 373
 - IPv6 443
- statistics
 - 182
 - 802.1X 146
 - ACL 230
 - ARP 182
 - bridging 150
 - commands 143 to 242
 - CPU 226
 - DNS 183
 - ethernet 151
 - FCoE 232
 - hot links 165
 - ICMP 184
 - IGMP 188
 - interface 154
 - interface protocol 157
 - IPv4 173
 - IPv4 route 181
 - IPv6 176
 - LACP 164
 - Layer 2 163
 - Layer 3 170
 - link 157
 - LLDP 166
 - logged packet 221
 - management processor 212
 - MLD 190
 - NTP 238

- OAM 167
- OSPF 193
- OSPFv3 197
- port 144
- RIP 203
- RMON 158
- SNMP 234
- TCP 186, 225
- trunk group 162
- UDP 187, 226
- VMAP 231
- VRRP 201
- STG
 - information 35, 50
 - Topology Change Count 51
- STP
 - and trunk groups 56
 - bridge parameters 336
 - bridge priority 50, 55
 - configuration 330
 - information 50, 331
 - path-cost option 337
 - root bridge 50, 55, 336
 - RSTP/PVRST 335
 - switch reset effect 526
- support
 - line 571
 - Web site 571
- switch
 - name and location 14, 25
 - resetting 526
- Switch Partition (SPAR)
 - configuration 495
- Switch Partition (SPAR)
 - configuration 6
- system
 - date and time 14, 25
 - information 14, 25
- System Error Disable and Recovery 249

T

- tab completion (CLI) 9
- TACACS+ 255
- TCP statistics 186, 225
- technical assistance 567
- telephone assistance 571
- telephone numbers 573
- telnet
 - configuring switches using 500
 - controlling access 276
 - port 276
 - radius server 253, 258
- text conventions xvi
- TFTP 522
 - port 276
 - PUT and GET commands 501
 - server 501

- timeout
 - idle connection 12
 - radius server 253
- timers kickoff 197, 200
- TLV 343
- trace buffer 537
- traceroute 8
- transceiver status 116
- transmit flow control 288, 294
- Trunk group information 56
- trunk hash algorithm 346
- type of area
 - OSPF 389
 - OSPFv3 448
- type parameters 63
- typographic conventions, manual xvi

U

- UCB statistics 226
- UDLD
 - configuration 289
 - information 45
 - statistics 216, 221
- UDP statistics 187
- UFP. See Unified Fabric Port.
- UFP. See Universal Fabric Port.
- Unified Fabric Port (UFP)
 - configuration 476
- Universal Fabric Port (UFP)
 - configuration 6
- unknown (UNK) port state 38
- Unscheduled System Dump 551
- upgrade
 - recover from failure 529
 - switch software 522
- user access control configuration 278
- user account 10
- Uuencode Flash Dump 548

V

- Virtual Link Aggregation Control protocol (see vLAG) 348
- virtual router
 - description 430
 - increasing priority level of 432
 - priority increment values (vrs) for VRRP 437
 - tracking criteria 432
- virtual router group
 - configuration 433
 - priority tracking 435
- Virtual Router Redundancy Protocol (see VRRP) 5
- virtualization
 - configuration 472
 - information 118
- vLAG
 - configuration 348

- information 349
- VLAN
 - active port 435
 - ARP entry information 64
 - configuration 361
 - information 57
 - name 36
 - Number 57
 - port membership 36, 58
 - setting default number (PVID) 284
 - tagging 114
 - port configuration 285
 - port restrictions 362
 - port use of 13
 - Type 57

- VLAN Map (see VMAP) 313

- VM
 - bandwidth management 472
 - Distributed Virtual Switch 513
 - Edge Virtual Bridge configuration 485
 - group configuration 478
 - information 118
 - policy configuration 472
 - profile configuration 482
 - VMready configuration 484
 - VMware
 - configuration 483
 - dvSwitch operations 513, 514
 - information 119
 - operations 511

- VM Check
 - configuration 480, 481, 483
 - information 119

- VMAP
 - configuration 313
 - definition 313
 - information 57, 101
 - statistics 231

- VMware
 - configuration 483
 - distributed port group operations 514
 - dvSwitch administration 513
 - information 119
 - operations 511

- VNIC
 - configuration 473
 - group configuration 474
 - information 122

- VRRP
 - authentication parameters for IP interfaces 436
 - configuration 429
 - configuration mode 5
 - information 87
 - interface configuration 436
 - master advertisements 431
 - master advertisements, time interval 433
 - operations-level options 507
 - priority tracking options 399, 432

- statistics 201
- tracking configuration 437

- VSI
 - configuration mode 5

W

- watchdog timer 533

- Web site
 - ordering publications 569
 - support 571
 - telephone support numbers 572

- weight
 - COS queue 99, 297
 - COS scheduling 100
 - route map 380
 - setting virtual router priority values 437
 - VRRP priority 437

- Weighted Random Early Detection (WRED) 300
- WRED (Weighted Random Early Detection) 300



Part Number: 00AY515

Printed in USA

(IP) P/N: 00AY515