

BLADEOS™ 6.6

ISCLI—Industry Standard CLI

Command Reference

RackSwitch™ G8264

Part Number: BMD00255-B, April 2011

BLADE

NETWORK TECHNOLOGIES

AN IBM COMPANY

2051 Mission College Blvd.
Santa Clara, CA 95054
www.bladenetwork.net

Copyright © 2011 BLADE Network Technologies, an IBM company, 2051 Mission College Blvd., Santa Clara, California, 95054, USA. All rights reserved. Part Number: BMD00255-B.

This document is protected by copyright and distributed under licenses restricting its use, copying, distribution, and decompilation. No part of this document may be reproduced in any form by any means without prior written authorization of BLADE Network Technologies. Documentation is provided “as is” without warranty of any kind, either express or implied, including any kind of implied or express warranty of non-infringement or the implied warranties of merchantability or fitness for a particular purpose.

U.S. Government End Users: This document is provided with a “commercial item” as defined by FAR 2.101 (Oct. 1995) and contains “commercial technical data” and “commercial software documentation” as those terms are used in FAR 12.211-12.212 (Oct. 1995). Government End Users are authorized to use this documentation only in accordance with those rights and restrictions set forth herein, consistent with FAR 12.211- 12.212 (Oct. 1995), DFARS 227.7202 (JUN 1995) and DFARS 252.227-7015 (Nov. 1995).

BLADE Network Technologies reserves the right to change any products described herein at any time, and without notice. BLADE Network Technologies assumes no responsibility or liability arising from the use of products described herein, except as expressly agreed to in writing by BLADE Network Technologies. The use and purchase of this product does not convey a license under any patent rights, trademark rights, or any other intellectual property rights of BLADE Network Technologies.

BLADE Network Technologies, the BLADE logo, BLADEHarmony, BNT, NMotion, RackSwitch, Rackonomics, RackSwitch Solution Partner, ServerMobility, SmartConnect and VMready are trademarks of BLADE Network Technologies. All other names or marks are property of their respective owners.

Originated in the USA.

Contents

Preface ■ 15

- Who Should Use This Book ■ 15
- How This Book Is Organized ■ 15
- Typographic Conventions ■ 16
- How to Get Help ■ 19

Chapter 1: ISCLI Basics ■ 21

- Accessing the ISCLI ■ 21
- ISCLI Command Modes ■ 22
- Global Commands ■ 25
- Command Line Interface Shortcuts ■ 27
 - CLI List and Range Inputs ■ 27
 - Command Abbreviation ■ 27
 - Tab Completion ■ 28
- User Access Levels ■ 28
- Idle Timeout ■ 29

Chapter 2: Information Commands ■ 31

- System Information ■ 33
 - Error Disable and Recovery Information ■ 34
 - SNMPv3 System Information ■ 34
 - SNMPv3 USM User Table Information ■ 36
 - SNMPv3 View Table Information ■ 37
 - SNMPv3 Access Table Information ■ 38
 - SNMPv3 Group Table Information ■ 39
 - SNMPv3 Community Table Information ■ 39
 - SNMPv3 Target Address Table Information ■ 40
 - SNMPv3 Target Parameters Table Information ■ 41
 - SNMPv3 Notify Table Information ■ 42
 - SNMPv3 Dump Information ■ 43

- General System Information ■ 44
- Show Recent Syslog Messages ■ 45
- User Status ■ 46
- Layer 2 Information ■ 47
 - 802.1X Information ■ 50
 - FDB Information ■ 52
 - Show All FDB Information ■ 53
 - Clearing Entries from the Forwarding Database ■ 53
 - Link Aggregation Control Protocol Information ■ 54
 - Link Aggregation Control Protocol ■ 54
 - Layer 2 Failover Information ■ 55
 - Layer 2 Failover Information ■ 56
 - Hot Links Information ■ 57
 - LLDP Information ■ 58
 - LLDP Remote Device Information ■ 58
 - Unidirectional Link Detection Information ■ 59
 - UDLD Port Information ■ 60
 - OAM Discovery Information ■ 61
 - OAM Port Information ■ 61
 - vLAG Information ■ 62
 - vLAG Trunk Information ■ 62
 - Spanning Tree Information ■ 63
 - RSTP/MSTP/PVRST Information ■ 66
 - Common Internal Spanning Tree Information ■ 69
 - Trunk Group Information ■ 71
 - VLAN Information ■ 72
- Layer 3 Information ■ 74
 - IP Routing Information ■ 76
 - Show All IP Route Information ■ 77
 - ARP Information ■ 79
 - ARP Address List Information ■ 80
 - Show All ARP Entry Information ■ 80
 - BGP Information ■ 81
 - BGP Peer information ■ 81
 - BGP Summary information ■ 82
 - Dump BGP Information ■ 82
 - OSPF Information ■ 83
 - OSPF General Information ■ 85
 - OSPF Interface Information ■ 86
 - OSPF Database Information ■ 86

OSPF Information Route Codes	■	88
OSPFv3 Information	■	89
OSPFv3 Information Dump	■	91
OSPFv3 Interface Information	■	91
OSPFv3 Database Information	■	92
OSPFv3 Route Codes Information	■	93
Routing Information Protocol	■	94
RIP Routes Information	■	94
RIP Interface Information	■	95
IPv6 Routing Information	■	95
IPv6 Routing Table Information	■	96
IPv6 Neighbor Discovery Cache Information	■	97
IPv6 Neighbor Discovery Cache Information	■	97
IPv6 Neighbor Discovery Prefix Information	■	98
ECMP Static Route Information	■	98
IGMP Multicast Group Information	■	99
IGMP Querier Information	■	100
IGMP Group Information	■	101
IGMP Multicast Router Information	■	102
VRRP Information	■	102
Interface Information	■	103
IPv6 Interface Information	■	104
IPv6 Path MTU Information	■	105
IP Information	■	106
DHCP Snooping Binding Table Information	■	107
PIM Information	■	108
PIM Component Information	■	109
PIM Interface Information	■	110
PIM Neighbor Information	■	110
PIM Multicast Route Information Commands	■	111
PIM Multicast Route Information	■	112
Quality of Service Information	■	113
802.1p Information	■	114
Access Control List Information Commands	■	115
Access Control List Information	■	116
RMON Information Commands	■	117
RMON History Information	■	118
RMON Alarm Information	■	119
RMON Event Information	■	120
Link Status Information	■	122

- Port Information ■ 123
- Port Transceiver Status ■ 124
- Virtual Machines Information ■ 125
 - VM Information ■ 126
 - VMware Information ■ 127
 - VMware Host Information ■ 128
- vNIC Information ■ 128
 - Virtual NIC (vNIC) Information ■ 129
 - vNIC Group Information ■ 130
- Converged Enhanced Ethernet Information ■ 131
 - DCBX Information ■ 131
 - DCBX Control Information ■ 132
 - DCBX Feature Information ■ 133
 - DCBX ETS Information ■ 134
 - DCBX PFC Information ■ 135
 - DCBX Application Protocol Information ■ 136
 - ETS Information ■ 137
 - PFC Information ■ 139
- FCoE Information ■ 140
 - FIP Snooping Information ■ 140
- 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 ■ 152
 - Interface Statistics ■ 154
 - Interface Protocol Statistics ■ 157
 - Link Statistics ■ 157
 - RMON Statistics ■ 158
- Layer 2 Statistics ■ 161
 - FDB Statistics ■ 162
 - LACP Statistics ■ 163
 - Hotlinks Statistics ■ 164
 - LLDP Port Statistics ■ 165
 - OAM Statistics ■ 166
 - vLAG Statistics ■ 167
 - vLAG ISL Statistics ■ 167

vLAG Statistics	■	168
Layer 3 Statistics	■	170
IPv4 Statistics	■	174
IPv6 Statistics	■	176
Route Statistics	■	181
IPv6 Route Statistics	■	182
ARP statistics	■	183
DNS Statistics	■	184
ICMP Statistics	■	184
TCP Statistics	■	186
UDP Statistics	■	188
IGMP Statistics	■	189
OSPF Statistics	■	190
OSPF Global Statistics	■	191
OSPFv3 Statistics	■	195
OSPFv3 Global Statistics	■	196
VRRP Statistics	■	200
PIM Statistics	■	201
Routing Information Protocol Statistics	■	202
DHCP Statistics	■	203
DHCP Snooping Statistics	■	203
Management Processor Statistics	■	204
MP Packet Statistics	■	205
MP Packet Statistics	■	207
TCP Statistics	■	209
UDP Statistics	■	210
CPU Statistics	■	210
QoS Statistics	■	211
Access Control List Statistics	■	212
ACL Statistics	■	213
VMAP Statistics	■	213
Fiber Channel over Ethernet Statistics	■	214
SNMP Statistics	■	215
NTP Statistics	■	219
Statistics Dump	■	220
Chapter 4: Configuration Commands	■	221
Viewing and Saving Changes	■	222
System Configuration	■	223
System Error Disable and Recovery Configuration	■	225

- Link Flap Dampening Configuration ■ 226
- System Host Log Configuration ■ 227
- SSH Server Configuration ■ 228
- RADIUS Server Configuration ■ 229
- TACACS+ Server Configuration ■ 232
- LDAP Server Configuration ■ 236
- NTP Client Configuration ■ 238
- System SNMP Configuration ■ 239
- SNMPv3 Configuration ■ 242
 - User Security Model Configuration ■ 244
 - SNMPv3 View Configuration ■ 245
 - View-based Access Control Model Configuration ■ 246
 - SNMPv3 Group Configuration ■ 248
 - SNMPv3 Community Table Configuration ■ 249
 - SNMPv3 Target Address Table Configuration ■ 250
 - SNMPv3 Target Parameters Table Configuration ■ 251
 - SNMPv3 Notify Table Configuration ■ 253
- System Access Configuration ■ 254
 - Management Network Configuration ■ 256
 - NETCONF Configuration ■ 257
 - NETCONF over SSH Configuration ■ 258
- User Access Control Configuration ■ 258
 - System User ID Configuration ■ 259
 - Strong Password Configuration ■ 260
 - HTTPS Access Configuration ■ 261
- Custom Daylight Savings Time Configuration ■ 263
- sFlow Configuration ■ 264
 - sFlow Port Configuration ■ 265
- Server Port Configuration ■ 265
- Port Configuration ■ 266
 - Port Error Disable and Recovery Configuration ■ 269
 - Port Link Flap Dampening Configuration ■ 270
 - Port Link Configuration ■ 271
 - Temporarily Disabling a Port ■ 272
 - UniDirectional Link Detection Configuration ■ 272
 - Port OAM Configuration ■ 272
 - Port ACL Configuration ■ 273
 - Port Spanning Tree Configuration ■ 275
 - Port Spanning Tree Guard Configuration ■ 276
 - Port WRED Configuration ■ 277

- Port WRED Transmit Queue Configuration ■ 278
- Quality of Service Configuration ■ 279
 - 802.1p Configuration ■ 279
 - DSCP Configuration ■ 280
 - Control Plane Protection ■ 281
 - Weighted Random Early Detection Configuration ■ 283
 - WRED Transmit Queue Configuration ■ 284
- Access Control Configuration ■ 285
 - ACL IPv4 Configuration ■ 286
 - ACL Mirroring Configuration ■ 287
 - Ethernet Filtering Configuration ■ 287
 - IPv4 Filtering Configuration ■ 289
 - TCP/UDP Filtering Configuration ■ 291
 - ACL Metering Configuration ■ 292
 - ACL Re-Mark Configuration ■ 293
 - Packet Format Filtering Configuration ■ 295
 - ACL IPv6 Configuration ■ 296
 - IP version 6 Filtering Configuration ■ 297
 - IPv6 TCP/UDP Filtering Configuration ■ 298
 - IPv6 Re-Mark Configuration ■ 299
 - ACL Group Configuration ■ 300
 - Management ACL Configuration ■ 301
 - MACL IPv4 Filtering Configuration ■ 302
 - MACL TCP/UDP Filtering Configuration ■ 304
 - VMAP Configuration ■ 306
- Port Mirroring ■ 307
 - Port-Mirroring Configuration ■ 308
- Layer 2 Configuration ■ 309
 - 802.1X Configuration ■ 310
 - 802.1X Global Configuration ■ 311
 - 802.1X Guest VLAN Configuration ■ 313
 - 802.1X Port Configuration ■ 314
 - RSTP/MSTP/PVRST Configuration ■ 316
 - Common Internal Spanning Tree Configuration ■ 317
 - CIST Bridge Configuration ■ 318
 - CIST Port Configuration ■ 319
 - Spanning Tree Configuration ■ 321
 - Bridge Spanning Tree Configuration ■ 322
 - Spanning Tree Port Configuration ■ 324
 - Forwarding Database Configuration ■ 326

- Static FDB Configuration ■ 326
- Static Multicast MAC Configuration ■ 327
- LLDP Configuration ■ 328
 - LLDP Port Configuration ■ 330
 - LLDP Optional TLV configuration ■ 330
- Trunk Configuration ■ 332
- IP Trunk Hash Configuration ■ 334
 - Layer 2 Trunk Hash ■ 334
 - Layer 3 Trunk Hash ■ 336
- Virtual Link Aggregation Control Protocol Configuration ■ 337
 - vLAG ISL Configuration ■ 338
- Link Aggregation Control Protocol Configuration ■ 339
 - LACP Port Configuration ■ 340
- Layer 2 Failover Configuration ■ 341
 - Failover Trigger Configuration ■ 342
 - Failover Manual Monitor Port Configuration ■ 342
 - Failover Manual Monitor Control Configuration ■ 344
- Hot Links Configuration ■ 345
 - Hot Links Trigger Configuration ■ 346
 - Hot Links Master Configuration ■ 347
 - Hot Links Backup Configuration ■ 348
- VLAN Configuration ■ 349
- Protocol-Based VLAN Configuration ■ 351
- Private VLAN Configuration ■ 353
- Layer 3 Configuration ■ 355
 - IP Interface Configuration ■ 357
 - IPv6 Neighbor Discovery Configuration ■ 359
 - Default Gateway Configuration ■ 361
 - IPv4 Static Route Configuration ■ 363
 - IP Multicast Route Configuration ■ 365
 - ARP Configuration ■ 366
 - ARP Static Configuration ■ 367
 - IP Forwarding Configuration ■ 368
 - Network Filter Configuration ■ 369
 - Routing Map Configuration ■ 370
 - IP Access List Configuration ■ 372
 - Autonomous System Filter Path Configuration ■ 373
 - Routing Information Protocol Configuration ■ 374
 - Routing Information Protocol Interface Configuration ■ 375
 - RIP Route Redistribution Configuration ■ 377

- Open Shortest Path First Configuration ■ 378
 - Area Index Configuration ■ 380
 - OSPF Summary Range Configuration ■ 382
 - OSPF Interface Configuration ■ 383
 - OSPF Virtual Link Configuration ■ 386
 - OSPF Host Entry Configuration ■ 388
 - OSPF Route Redistribution Configuration. ■ 389
 - OSPF MD5 Key Configuration ■ 390
- Open Shortest Path First Version 3 Configuration ■ 390
 - OSPFv3 Area Index Configuration ■ 392
 - OSPFv3 Summary Range Configuration ■ 394
 - OSPFv3 AS-External Range Configuration ■ 395
 - OSPFv3 Interface Configuration ■ 397
 - OSPFv3 Virtual Link Configuration ■ 399
 - OSPFv3 Host Entry Configuration ■ 400
 - OSPFv3 Redist Entry Configuration ■ 401
 - OSPFv3 Redistribute Configuration ■ 402
- Border Gateway Protocol Configuration ■ 403
 - BGP Peer Configuration ■ 405
 - BGP Redistribution Configuration ■ 408
 - BGP Aggregation Configuration ■ 409
- IGMP Configuration ■ 410
 - IGMP Snooping Configuration ■ 411
 - IGMPv3 Configuration ■ 412
 - IGMP Relay Configuration ■ 413
 - IGMP Relay Multicast Router Configuration ■ 414
 - IGMP Static Multicast Router Configuration ■ 416
 - IGMP Filtering Configuration ■ 417
 - IGMP Advanced Configuration ■ 419
 - IGMP Querier Configuration ■ 421
- Domain Name System Configuration ■ 423
- Bootstrap Protocol Relay Configuration ■ 424
 - BOOTP Relay Broadcast Domain Configuration ■ 425
- VRRP Configuration ■ 427
- Virtual Router Configuration ■ 428
 - Virtual Router Priority Tracking Configuration ■ 431
- Virtual Router Group Configuration ■ 432
 - Virtual Router Group Priority Tracking Configuration ■ 434
- VRRP Interface Configuration ■ 435
- VRRP Tracking Configuration ■ 436

- Protocol Independent Multicast Configuration ■ 437
 - PIM Component Configuration ■ 438
 - PIM Interface Configuration ■ 439
- IPv6 Default Gateway Configuration ■ 442
- IPv6 Static Route Configuration ■ 443
- IPv6 Neighbor Discovery Cache Configuration ■ 444
- IPv6 Path MTU Configuration ■ 444
- IPv6 Neighbor Discovery Prefix Configuration ■ 445
- IPv6 Prefix Policy Table Configuration ■ 447
- IP Loopback Interface Configuration ■ 448
- DHCP Snooping ■ 449
- Converged Enhanced Ethernet Configuration ■ 451
 - ETS Global Configuration ■ 451
 - ETS Global Priority Group Configuration ■ 452
 - Priority Flow Control Configuration ■ 453
 - 802.1p PFC Configuration ■ 453
 - DCBX Port Configuration ■ 454
- Fiber Channel over Ethernet Configuration ■ 455
 - FIPS Port Configuration ■ 456
- Remote Monitoring Configuration ■ 457
 - RMON History Configuration ■ 458
 - RMON Event Configuration ■ 459
 - RMON Alarm Configuration ■ 460
- Virtualization Configuration ■ 462
 - VM Policy Bandwidth Management ■ 463
 - Virtual NIC Configuration ■ 464
 - vNIC Port Configuration ■ 465
 - Virtual NIC Group Configuration ■ 466
 - VM Group Configuration ■ 468
 - VM Profile Configuration ■ 470
 - VM Ware Configuration ■ 471
- Configuration Dump ■ 472
- Saving the Active Switch Configuration ■ 473
- Restoring the Active Switch Configuration ■ 473
- USB Copy ■ 474
 - Copy to USB ■ 474
 - Copy from USB ■ 474

Chapter 5: Operations Commands ■ 475

- Operations-Level Port Commands ■ 476

- Operations-Level FCoE Commands ■ 477
- Operations-Level VRRP Commands ■ 477
- Operations-Level BGP Commands ■ 478
- VMware Operations ■ 478

Chapter 6: Boot Options ■ 481

- Scheduled Reboot of the Switch ■ 482
- Netboot Configuration ■ 483
 - QSFP Port Configuration ■ 484
- USB Boot Configuration ■ 485
- Updating the Switch Software Image ■ 486
 - Loading New Software to Your Switch ■ 486
 - Selecting a Software Image to Run ■ 487
 - Uploading a Software Image from Your Switch ■ 488
- Selecting a Configuration Block ■ 489
- Resetting the Switch ■ 489
- Accessing the BLADEOS CLI ■ 490
- Using the Boot Management Menu ■ 491
 - Recovering from a Failed Upgrade ■ 491

Chapter 7: Maintenance Commands ■ 495

- Forwarding Database Maintenance ■ 497
- Debugging Commands ■ 499
- LLDP Cache Manipulation ■ 500
- ARP Cache Maintenance ■ 501
- IP Route Manipulation ■ 502
- IGMP Snooping Maintenance ■ 503
- IGMP Multicast Routers Maintenance ■ 504
- IPv6 Neighbor Discovery Cache Manipulation ■ 505
- IPv6 Route Maintenance ■ 506
- Uencode Flash Dump ■ 507
- TFTP or FTP System Dump Put ■ 507
- Clearing Dump Information ■ 508
- Unscheduled System Dumps ■ 508

Appendix A: BLADEOS System Log Messages ■ 509

- LOG_ALERT ■ 510
- LOG_CRIT ■ 513
- LOG_ERR ■ 514

LOG_INFO ■ 517
LOG_NOTICE ■ 521
LOG_WARNING ■ 531

Index ■ 535

Preface

The *BLADEOS 6.6 Command Reference* describes how to configure and use the BLADE OS 6.6 software with your RackSwitch G8264. 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 G8264. For details about the configuration and operation of the G8264, see the *BLADE OS 6.6 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.

“**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> <p>show sys-info</p>
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>
block body text	<p>Indicates objects such as window names, dialog box names, and icons, as well as user interface objects such as buttons and tabs.</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> <p>ping <IP address></p> <p>you enter</p> <p>ping 192.32.10.12</p>

Table 1 Typographic Conventions

Typeface or Symbol	Meaning
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 show portchannel { <1-64> hash information }</p> <p>you enter:</p> <p>show portchannel <1-64></p> <p>or</p> <p>show portchannel hash</p> <p>or</p> <p>show portchannel information</p>
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 show ip interface [<1-128>]</p> <p>you enter</p> <p>show ip interface</p> <p>or</p> <p>show ip interface <1-128></p>

Table 1 Typographic Conventions

Typeface or Symbol	Meaning
vertical line	<p data-bbox="582 222 1310 319">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 data-bbox="582 350 1310 413">Example: If the command syntax is show portchannel {<1-64> hash information}</p> <p data-bbox="582 444 1310 472">you must enter:</p> <p data-bbox="582 479 1310 506">show portchannel <1-64></p> <p data-bbox="582 534 1310 562">or</p> <p data-bbox="582 590 1310 618">show portchannel hash</p> <p data-bbox="582 645 1310 673">or</p> <p data-bbox="582 701 1310 729">show portchannel information</p>

How to Get Help

If you need help, service, or technical assistance, call BLADE Network Technologies Technical Support:

US toll free calls: 1-800-414-5268

International calls: 1-408-834-7871

You also can visit our web site at the following address:

<http://www.bladenetwork.net>

Click the **Support** tab.

The warranty card received with your product provides details for contacting a customer support representative. If you are unable to locate this information, please contact your reseller. Before you call, prepare the following information:

- Serial number of the switch unit
- Software release version number
- Brief description of the problem and the steps you have already taken
- Technical support dump information (`# show tech-support`)

CHAPTER 1

ISCLI Basics

Your RackSwitch G8264 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 G8264.

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 G8264, it boots into BLADEOS CLI. To access the ISCLI, enter the following command and reset the G8264:

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

To access the BLADEOS CLI, enter the following command from the ISCLI and reload the G8264:

```
Router(config)# boot cli-mode bladeos-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 BLADEOS 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 G8264. Several sub-modes can be accessed from the Global Configuration mode. For more details, see [Table 2](#).

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 2](#) lists the ISCLI command modes.

Table 2 ISCLI Command Modes

Command Mode/Prompt	Command used to enter or exit
User EXEC	Default mode, entered automatically on console
G8264>	Exit: exit or logout
Privileged EXEC	Enter Privileged EXEC mode, from User EXEC mode: enable
G8264#	Exit to User EXEC mode: disable Quit ISCLI: exit or logout
Global Configuration	Enter Global Configuration mode, from Privileged EXEC mode: configure terminal
G8264(config)#	Exit to Privileged EXEC: end or exit
Interface IP	Enter Interface IP Configuration mode, from Global Configuration mode: interface ip <interface number>
G8264(config-ip-if)#	Exit to Global Configuration mode: exit Exit to Privileged EXEC mode: end

Table 2 ISCLI Command Modes

Command Mode/Prompt	Command used to enter or exit
Interface port G8264(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
VLAN G8264(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 G8264(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 OSPFv3 G8264(config-router-ospf3)#	Enter OSPFv3 Configuration mode, from Global Configuration mode: ipv6 router ospf Exit to Global Configuration mode: exit Exit to Privileged EXEC mode: end
Router RIP G8264(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 G8264(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 2 ISCLI Command Modes

Command Mode/Prompt	Command used to enter or exit
Router VRRP G8264(config-vrrp)#	Enter VRRP Configuration mode, from Global Configuration mode: router vrrp Exit to Global Configuration mode: exit Exit to Privileged EXEC mode: end
PIM Component G8264(config-ip-pim-comp)#	Enter Protocol Independent Multicast (PIM) Component Configuration mode, from Global Configuration mode: ip pim component <1-2> 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 3 Description of Global Commands

Command	Action
<code>?</code>	Provides more information about a specific command or lists commands available at the current level.
<code>list</code>	Lists the commands available at the current level.
<code>exit</code>	Go up one level in the command mode structure. If already at the top level, exit from the command line interface and log out.
<code>copy running-config startup-config</code>	Write configuration changes to non-volatile flash memory.
<code>logout</code>	Exit from the command line interface and log out.
<code>ping</code>	<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] [-m -mgt -d -data]</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>By default, the -m or -mgt option for management port is used. To use data ports, specify the -d or -data option.</p>

Table 3 Description of Global Commands

Command	Action
traceroute	<p>Use this command to identify the route used for station-to-station connectivity across the network. The format is as follows:</p> <pre data-bbox="529 314 1250 378">traceroute <hostname> <IP address> [<max-hops (1-32)> [<msec-delay (1-4294967295)>]] [-m -mgt -d -data]</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. By default, the -m or -mgt option for management port is used. To use data ports, specify the -d or -data option.</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 data-bbox="529 777 1082 841">telnet { <hostname> <IP address> } [<port>] [-m -mgt -d -data]</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> <p>By default, the -m or -mgt option for management port is used. To use data ports, specify the -d or -data option.</p>
show history	This command displays the last ten issued commands.
show who	Displays a list of users who are currently logged in.

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:

# <code>vlan 1,3,4094</code>	<i>(access VLANs 1, 3, and 4094)</i>
# <code>vlan 1-20</code>	<i>(access VLANs 1 through 20)</i>
# <code>vlan 1-5,90-99,4090-4094</code>	<i>(access multiple ranges)</i>
# <code>vlan 1-5,19,20,4090-4094</code>	<i>(access a mix of lists and ranges)</i>

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:

# <code>interface port 1-4</code>	<i>(Access ports 1 though 4)</i>
-----------------------------------	----------------------------------

Note – Port ranges accept only port numbers, not port aliases.

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)# <code>spanning-tree stp 2 bridge hello 2</code>
or
Router(config)# <code>sp stp 2 br h 2</code>

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.

If multiple commands share the typed characters, when you press <Tab>, the ISCLI completes the common part of the shared syntax.

User Access Levels

To enable better switch management and user accountability, three levels or *classes* of user access have been implemented on the G8264. 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 G8264. 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 G8264. 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/reset of the switch. Administrators can access switch functions to configure and troubleshoot problems on the G8264. 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 4 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 RackSwitch G8264, 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:

```
system idle <1-60>
```

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 5 Information Commands

Command Syntax and Usage

show interface status *<port alias or number>*

Displays configuration information about the selected port(s), including:

- 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)

Command mode: All

For details, see [page 122](#).

Table 5 Information Commands (continued)

Command Syntax and Usage

show interface trunk *<port alias or number>*

Displays port status information, including:

- Port alias and number
- Whether the port uses VLAN Tagging or not
- Port VLAN ID (PVID)
- Port name
- VLAN membership
- Fast Forwarding status
- FDB Learning status
- Flood Blocking status

For details, see [page 123](#).

Command mode: All

show interface transceiver

Displays the status of the port transceiver module on each port. For details, see [page 124](#).

Command mode: All

show information-dump

Dumps all switch information available (10K or more, depending on your configuration).

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.

Command mode: All

System Information

The information provided by each command option is briefly described in [Table 6 on page 33](#), with pointers to where detailed information can be found.

Table 6 System Information Options

Command Syntax and Usage

show sys-info

Displays system information, including:

- 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

For details, see [page 44](#).

Command mode: All

show logging

Displays most recent syslog messages. For details, see [page 45](#).

Command mode: All

show access user

Displays configured user names and their status.

Command mode: All

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 Options

Command Syntax and Usage

show errdisable recovery

Displays a list ports with their Error Recovery status.

Command mode: All

show errdisable timers

Displays a list of active recovery timers, if applicable.

Command mode: All

show errdisable information

Displays all Error Disable and Recovery information.

Command mode: All

show errdisable link-flap information

Displays ports that have been disabled due to excessive link flaps.

Command mode: All

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 Information Options

Command Syntax and Usage

show snmp-server v3 user

Displays User Security Model (USM) table information. To view the table, see [page 36](#).

Command mode: All

show snmp-server v3 view

Displays information about view, subtrees, mask and type of view. To view a sample, see [page 37](#).

Command mode: All

show snmp-server v3 access

Displays View-based Access Control information. To view a sample, see [page 38](#).

Command mode: All

show snmp-server v3 group

Displays information about the group, including the security model, user name, and group name. To view a sample, see [page 39](#).

Command mode: All

show snmp-server v3 community

Displays information about the community table information. To view a sample, see [page 39](#).

Command mode: All

show snmp-server v3 target-address

Displays the Target Address table information. To view a sample, see [page 40](#).

Command mode: All

show snmp-server v3 target-parameters

Displays the Target parameters table information. To view a sample, see [page 41](#).

Command mode: All

Table 8 SNMPv3 Information Options (continued)**Command Syntax and Usage****show snmp-server v3 notify**

Displays the Notify table information. To view a sample, see [page 42](#).

Command mode: All

show snmp-server v3

Displays all the SNMPv3 information. To view a sample, see [page 43](#).

Command mode: All

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. BLADEOS 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	1.3		included
v1v2only	1.3		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 sub system 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.

Table 13 SNMPv3 Community Table Information Parameters (continued)

Field	Description
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 Model Level ReadV WriteV NotifyV
-----
v1v2grp snmpv1 noAuthNoPriv iso iso v1v2only
admingrp usm authPriv iso iso iso

vacmViewTreeFamily Table:
View Name Subtree Mask Type
-----
iso 1.3 included
v1v2only 1.3 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 13:41:04 Fri Jan 20, 2011
Time zone: America/US/Pacific
Daylight Savings Time Status: Disabled

Blade Network Technologies RackSwitch G8264

Switch has been up for 0 days, 17 hours, 10 minutes and 45 seconds.
Last boot: 20:41:01 Thu Jan 19, 2011 (power cycle)

MAC address: fc:cf:62:9d:2b:00   IP (If 1) address: 0.0.0.0
Management Port MAC Address: fc:cf:62:9d:2b:fe
Management Port IP Address (if 128): 203.203.21.2
Hardware Revision: 0
Hardware Part No: BAC-000*a*00
Switch Serial No: US7C45t78
Manufacturing date:

Software Version 6.6.0 (FLASH imagel), active configuration.

Temperature Mother      Top: 34 C
Temperature Mother     Bottom: 38 C
Temperature Daughter   Top: 35 C
Temperature Daughter  Bottom: 37 C

Warning at 70 C and Recover at 100 C

Fan 1 in Module 1: RPM=17647 PWM=255(100%) Front-To-Back
Fan 2 in Module 1: RPM= 9310 PWM=255(100%) Front-To-Back
Fan 3 in Module 2: RPM=17419 PWM=255(100%) Front-To-Back
Fan 4 in Module 2: RPM= 9326 PWM=255(100%) Front-To-Back
Fan 5 in Module 3: RPM=17197 PWM=255(100%) Front-To-Back
Fan 6 in Module 3: RPM= 9523 PWM=255(100%) Front-To-Back
Fan 7 in Module 4: RPM=17252 PWM=255(100%) Front-To-Back
Fan 8 in Module 4: RPM= 9490 PWM=255(100%) Front-To-Back

System Fan Airflow: Front-To-Back

Power Supply 1: Vin Fault
Power Supply 2: OK
```

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

Show Recent Syslog Messages

The following command displays system log messages:

show logging messages

Command mode: All

Date	Time	Criticality	level	Message
Jul 8	17:25:41	NOTICE		system: link up on port 1
Jul 8	17:25:41	NOTICE		system: link up on port 8
Jul 8	17:25:41	NOTICE		system: link up on port 7
Jul 8	17:25:41	NOTICE		system: link up on port 2
Jul 8	17:25:41	NOTICE		system: link up on port 1
Jul 8	17:25:41	NOTICE		system: link up on port 4
Jul 8	17:25:41	NOTICE		system: link up on port 3
Jul 8	17:25:41	NOTICE		system: link up on port 6
Jul 8	17:25:41	NOTICE		system: link up on port 5
Jul 8	17:25:41	NOTICE		system: link up on port 4
Jul 8	17:25:41	NOTICE		system: link up on port 1
Jul 8	17:25:41	NOTICE		system: link up on port 3
Jul 8	17:25:41	NOTICE		system: link up on port 2
Jul 8	17:25:41	NOTICE		system: link up on port 3
Jul 8	17:25:42	NOTICE		system: link up on port 2
Jul 8	17:25:42	NOTICE		system: link up on port 4
Jul 8	17:25:42	NOTICE		system: link up on port 3
Jul 8	17:25:42	NOTICE		system: link up on port 6
Jul 8	17:25:42	NOTICE		system: link up on port 5
Jul 8	17:25:42	NOTICE		system: link up on port 1
Jul 8	17:25:42	NOTICE		system: link up on port 6

Each syslog message has a criticality 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 that the administrator is being notified of, as shown below.

- 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

User Status

The following command displays user status information:

show access user

Command mode: All except User EXEC

```
Username:
  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.

Layer 2 Information

Table 17 Layer 2 Information Commands

Command Syntax and Usage

show dot1x information

Displays 802.1X Information. For details, see [page 50](#).

Command mode: All

show spanning-tree

Displays Spanning Tree information, including the status (on or off), Spanning Tree mode (RSTP, PVRST, or MSTP), and VLAN membership.

In addition to seeing if STG is enabled or disabled, you can view the following STG bridge information:

- Priority
- Hello interval
- Maximum age value
- Forwarding delay
- Aging time

You can also see the following port-specific STG information:

- Port alias and priority
- Cost
- State
- Port Fast Forwarding state

Command mode: All

show spanning-tree stp <1-128> information

Displays information about a specific Spanning Tree Group.

Command mode: All

For details, see [page 63](#).

Table 17 Layer 2 Information Commands (continued)

Command Syntax and Usage

show spanning-tree mstp cist information

Displays Common Internal Spanning Tree (CIST) information, including the MSTP digest and VLAN membership.

CIST bridge information includes:

- Priority
- Hello interval
- Maximum age value
- Forwarding delay
- Root bridge information (priority, MAC address, path cost, root port)

CIST port information includes:

- Port number and priority
- Cost
- State

For details, see [page 69](#).

Command mode: All

show portchannel information

Displays the state of each port in the various trunk groups. For details, see [page 71](#).

Command mode: All

show vlan

Displays VLAN configuration information for all configured VLANs, including:

- VLAN Number
- VLAN Name
- Status
- Port membership of the VLAN

For details, see [page 72](#).

Command mode: All

show failover trigger <trigger number>

Displays Layer 2 Failover information. For details, see [page 55](#).

Command mode: All

Table 17 Layer 2 Information Commands (continued)

Command Syntax and Usage

show hotlinks information

Displays Hot Links information. For details, see [page 57](#).

Command mode: All

show layer2 information

Dumps all Layer 2 switch information available (10K or more, depending on your configuration).

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.

Command mode: All

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   Backend
-----  -
*1        force-auth   unauthorized   initialize      initialize
  2        force-auth   unauthorized   initialize      initialize
*3        force-auth   unauthorized   initialize      initialize
*4        force-auth   unauthorized   initialize      initialize
*5        force-auth   unauthorized   initialize      initialize
*6        force-auth   unauthorized   initialize      initialize
*7        force-auth   unauthorized   initialize      initialize
*8        force-auth   unauthorized   initialize      initialize
*9        force-auth   unauthorized   initialize      initialize
*10       force-auth   unauthorized   initialize      initialize
*11       force-auth   unauthorized   initialize      initialize
*12       force-auth   unauthorized   initialize      initialize
*13       force-auth   unauthorized   initialize      initialize
*14       force-auth   unauthorized   initialize      initialize
*15       force-auth   unauthorized   initialize      initialize
*16       force-auth   unauthorized   initialize      initialize
*17       force-auth   unauthorized   initialize      initialize
*18       force-auth   unauthorized   initialize      initialize
*19       force-auth   unauthorized   initialize      initialize
*20       force-auth   unauthorized   initialize      initialize
...
-----
* - Port down or disabled

```

The following table describes the IEEE 802.1X parameters.

Table 18 802.1X 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"> <input type="checkbox"/> force-unauth <input type="checkbox"/> auto <input type="checkbox"/> force-auth
Auth Status	Displays the current authorization status of the port, either authorized or unauthorized.
Authenticator PAE State	Displays the Authenticator Port Access Entity State. The PAE state can be one of the following: <ul style="list-style-type: none"> <input type="checkbox"/> initialize <input type="checkbox"/> disconnected <input type="checkbox"/> connecting <input type="checkbox"/> authenticating <input type="checkbox"/> authenticated <input type="checkbox"/> aborting <input type="checkbox"/> held <input type="checkbox"/> forceAuth
Backend Auth State	Displays the Backend Authorization State. The Backend Authorization state can be one of the following: <ul style="list-style-type: none"> <input type="checkbox"/> initialize <input type="checkbox"/> request <input type="checkbox"/> response <input type="checkbox"/> success <input type="checkbox"/> fail <input type="checkbox"/> timeout <input type="checkbox"/> idle

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 128K MAC address entries on the MP per switch.

Table 19 FDB Information Options

Command Syntax and Usage

show mac-address-table address *<MAC address>*

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

You can also enter the MAC address using the format, *xxxxxxxxxxxxxx*. For example, 080020123456

Command mode: All

show mac-address-table interface port *<port alias or number>*

Displays all FDB entries for a particular port.

Command mode: All

show mac-address-table portchannel *<trunk group number>*

Displays all FDB entries for a particular trunk group (portchannel).

Command mode: All

show mac-address-table vlan *<VLAN number>*

Displays all FDB entries on a single VLAN.

Command mode: All

show mac-address-table state {*unknown*|*forward*|*trunk*}

Displays all FDB entries for a particular state.

Command mode: All

show mac-address-table multicast

Displays all Multicast MAC entries in the FDB.

Command mode: All

Table 19 FDB Information Options (continued)**Command Syntax and Usage****show mac-address-table static**

Displays all static MAC entries in the FDB.

Command mode: All

show mac-address-table configured static

Displays all configured static MAC entries in the FDB.

Command mode: All

show mac-address-table

Displays all entries in the Forwarding Database.

Command mode: All

For more information, see [page 53](#).

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	4		FWD	
00:09:6b:9b:01:5f	1	13		FWD	
00:09:6b:ca:26:ef	4095	1		FWD	
00:0f:06:ec:3b:00	4095	1		FWD	
00:11:43:c4:79:83	1	4		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 which reference the address as a destination will be listed under “Reference ports.”

Clearing Entries from the Forwarding Database

To clear the entire FDB, refer to “[Forwarding Database Maintenance](#)” on [page 497](#).

Link Aggregation Control Protocol Information

Use these commands to display LACP status information about each port on the G8264.

Table 20 LACP Information Options

Command Syntax and Usage

show lacp aggregator <aggregator ID>

Displays detailed information about the LACP aggregator.

Command mode: All

show interface port <port alias or number> **lacp information**

Displays LACP information about the selected port.

Command mode: All

show lacp information

Displays a summary of LACP information.

Command mode: All

For details, see [page 54](#).

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
1	active	30	30	yes	32768	17	19	up
2	active	30	30	yes	32768	17	19	up
3	off	3	3	no	32768	--	--	--
4	off	4	4	no	32768	--	--	--
...								

LACP dump includes the following information for each port in the G8264:

- **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 or down).

Layer 2 Failover Information

Table 21 Layer 2 Failover Information Options

Command Syntax and Usage

show failover trigger *<trigger number>*

Displays detailed information about the selected Layer 2 Failover trigger.

Command mode: All

show failover trigger

Displays a summary of Layer 2 Failover information. For details, see [page 56](#).

Command mode: All

Layer 2 Failover Information

The following command displays Layer 2 Failover information:

show failover trigger

Command mode: All

```

Trigger 1 Auto Monitor: Enabled
Trigger 1 limit: 0
Monitor State: Up
Member      Status
-----
trunk 1
  2          Operational
  3          Operational

Control State: Auto Disabled
Member      Status
-----
  1          Operational
  2          Operational
  3          Operational
  4          Operational
  ...

```

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 the above 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
bpdu disabled
sndfdb disabled

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

Active state: None

Master settings:
port 1
Backup settings:
port 2
```

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

LLDP Information

Table 22 LLDP Information Options

Command Syntax and Usage

show lldp port

Displays Link Layer Discovery Protocol (LLDP) port information.

Command mode: All

show lldp receive

Displays information about the LLDP receive state machine.

Command mode: All

show lldp transmit

Displays information about the LLDP transmit state machine.

Command mode: All

show lldp remote-device

Displays information received from LLDP -capable devices. To view a sample display, see [page 58](#).

show lldp information

Displays all LLDP information.

Command mode: All

LLDP Remote Device Information

The following command displays LLDP remote device information:

show lldp remote-device

Command mode: All

```
LLDP Remote Devices Information
```

LocalPort	Index	Remote Chassis ID	RemotePort	Remote System Name
-----	-----	-----	-----	-----
2	210	00 16 ca ff 7e 00	15	BNT Gb Ethernet Switch...
4	12	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.

```

Local Port Alias: 1
  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        : 23

  System Name             :
  System Description      :

  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

Table 23 UDLD Information Options

Command Syntax and Usage

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

Displays UDLD information about the selected port.

Command mode: All

show udld

Displays all UDLD information.

Command mode: All

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 1
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: 1
```

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 24 OAM Discovery Information Options

Command Syntax and Usage

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

Displays OAM information about the selected port.

Command mode: All

show oam

Displays all OAM information.

Command mode: All

OAM Port Information

The following command displays OAM information for the selected port:

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

Command mode: All

```
OAM information on port 1
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
```

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

vLAG Information

Table 25 vLAG Information Options

Command Syntax and Usage

show vlag adminkey <1-65535>

Displays vLAG LACP information.

show vlag portchannel <trunk group number>

Displays vLAG static trunk group information.

show vlag isl

Displays vLAG Inter-Switch Link (ISL) information.

Command mode: All

show vlag information

Displays all vLAG information.

vLAG Trunk Information

The following command displays vLAG information for the trunk group:

show vlag portchannel <trunk group number>

Command mode: All

```
Peer IP Address:192.1.1.199
ISL Information: VLAN 4094, Trunk 1, LACP Key 0
Health check Peer IP Address:0.0.0.0

vLAG 2 : active
trunk id 2 ports 10

vLAG 3 : active
trunk id 3 ports 3
```

Spanning Tree Information

The following command displays Spanning Tree information:

show spanning-tree stp <1-128> information

Command mode: All

```

-----
upfast disabled, update 40
Pvst+ compatibility mode enabled
-----
Spanning Tree Group 1: On (PVRST)
VLANs: 1

Current Root:          Path-Cost  Port Hello MaxAge FwdDel
8000 00:22:00:ee:cc:00    2000      1   2    20    15

Parameters:  Priority  Hello  MaxAge  FwdDel  Aging
              32769    2      20      15      300

Port  Prio  Cost      State  Role Designated Bridge      Des Port Type
-----
1     128    2000!    FWD    ROOT 8000-00:22:00:ee:cc:00    8001 P2P
2     128    2000!    DISC   ALTN 8000-00:22:00:ee:cc:00    8002 P2P
3     128    2000!    DISC   ALTN 8000-00:22:00:ee:cc:00    8003 P2P
10    128    2000!    DISC   DESG 8001-00:22:00:7d:5f:00    800a P2P
11    128    2000!    DISC   DESG 8001-00:22:00:7d:5f:00    800b P2P
! = Automatic path cost.

-----
Spanning Tree Group 128: Off (PVRST), FDB aging timer 300
VLANs: 4095

Port  Prio  Cost      State  Role Designated Bridge      Des Port Type
-----
MGT   0      0          FWD   *

* = STP turned off for this port.

```

The switch software uses the IEEE 802.1D Spanning Tree Protocol (STP). If 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) are turned on, see [“RSTP/MSTP/PVRST Information” on page 66](#).

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

Table 26 Spanning Tree 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.
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 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 27 Spanning Tree 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.
FastFwd	The Fast Forward field shows whether the port is in Fast Forwarding mode or not, which permits the port that participates in Spanning Tree to bypass the Listening and Learning states and enter directly into the Forwarding state.
State	The State field shows the current state of the port. The state field can be BLOCKING, LISTENING, LEARNING, FORWARDING, or DISABLED.
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

```

-----
upfast disabled, update 40
Pvst+ compatibility mode enabled
-----
Spanning Tree Group 1: On (RSTP)
VLANs: 1

Current Root:                Path-Cost  Port Hello MaxAge FwdDel
0000 00:16:60:ba:6c:01      2026        1   2    20    15

Parameters:  Priority  Hello  MaxAge  FwdDel  Aging
              32768    2      20     15     300

Port  Prio  Cost      State  Role Designated Bridge      Des Port Type
-----
1     128    2000!    FWD    ROOT fffe-00:13:0a:4f:7d:d0      8013 P2P
23    128    2000!    FWD    DESG 8000-00:13:0a:4f:7e:10      8017 P2P
24    128    2000!    FWD    DESG 8000-00:13:0a:4f:7e:10      8018 P2P
-----

Spanning Tree Group 128: Off (RSTP), FDB aging timer 300
VLANs: 4095

Port  Prio  Cost      State  Role Designated Bridge      Des Port Type
-----
MGT   0      0      FWD *

* = STP turned off for this port.
! = Automatic path cost.

```

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 28 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 29 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.

Table 29 RSTP/MSTP/PVRST Port Parameter Descriptions (continued)

Parameter	Description
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).
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 30 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 31 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.

Table 31 CIST Parameter Descriptions (continued)

Parameter	Description
State	The state field shows the current state of the port. The state field can be either 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), 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:
  1: STG 1 forwarding
  2: 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 32 VLAN Information Options

Command Syntax and Usage

show vlan <VLAN number>

Displays general VLAN information.

Command mode: All

show protocol-vlan <protocol number (1-8)>

Displays Protocol VLAN information.

Command mode: All

show private-vlan <VLAN number>

Displays Private VLAN information.

Command mode: All

show vlan information

Displays information about all VLANs, including:

- VLAN number and name
- Port membership
- VLAN status (enabled or disabled)
- Protocol VLAN status
- Private VLAN status
- Spanning Tree membership
- VMAP configuration

Command mode: All

The following command displays VLAN information:

show vlan

Command mode: All

VLAN	Name	Status	Ports	
1	Default VLAN	ena	1-20	
2	VLAN 2	dis	21-22	
4095	Mgmt VLAN	ena	MGT	
Private-VLAN	Type	Mapped-To	Status	Ports
100	primary	200 300	ena	2 3 10
200	community	100	ena	12
300	isolated	100	ena	14

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 Name
- Status
- Port membership of the VLAN
- Protocol VLAN information (if available)
- Private VLAN information (if available)

Layer 3 Information

Table 33 Layer 3 Information Commands

Command Syntax and Usage

show ip route

Displays all routes configured on the switch. For details, see [page 77](#).

Command mode: All

show arp

Displays Address Resolution Protocol (ARP) information. For details, see [page 79](#).

Command mode: All

show ip bgp information

Displays Border Gateway Protocol (BGP) information. For details, see [page 82](#).

Command mode: All

show ip ospf information

Displays the OSPF information. For details, see [page 83](#).

Command mode: All

show ipv6 ospf information

Displays OSPFv3 information. For more OSPFv3 information options, see [page 89](#).

Command mode: All

show interface ip rip

Displays RIP user's configuration. For details, see [page 94](#).

Command mode: All

Table 33 Layer 3 Information Commands (continued)

Command Syntax and Usage

show ip interface brief

Displays IP Information. For details, see [page 76](#).

IP information, includes:

- ❑ 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

Command mode: All

show ip igmp groups

Displays IGMP Information.

Command mode: All

show ip vrrp information

Displays VRRP information. For details, see [page 102](#).

Command mode: All

show ip pim component [*<1-2>*]

Displays Protocol Independent Multicast (PIM) component information. For more PIM information options, see [page 108](#).

Command mode: All

show layer3

Dumps all Layer 3 switch information available (10K or more, depending on your configuration).

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.

Command mode: All

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 34 Route Information Options

Command Syntax and Usage

show ip route address *<IP address>*

Displays a single route by destination IP address.

Command mode: All

show ip route gateway *<IP address>*

Displays routes to a single gateway.

Command mode: All

show ip route type {*indirect* | *direct* | *local* | *broadcast* | *martian* | *multicast*}

Displays routes of a single type. For a description of IP routing types, see [Table 35 on page 77](#).

Command mode: All

show ip route tag {*fixed* | *static* | *addr* | *rip* | *ospf* | *bgp* | *broadcast* | *martian* | *multicast*}

Displays routes of a single tag. For a description of IP routing tags, see [Table 36 on page 78](#).

Command mode: All

show ip route interface *<interface number>*

Displays routes on a single interface.

Command mode: All

show ip route ecmphash

Displays the current ECMP hashing mechanism.

Command mode: All

Table 34 Route Information Options (continued)**Command Syntax and Usage****show ip route static**

Displays static routes configured on the switch.

Command mode: All

show ip route

Displays all routes configured in the switch.

Command mode: All

For more information, see [page 77](#).

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
* 0.0.0.0	0.0.0.0	172.31.1.1	indirect	static		1
* 12.0.0.0	255.0.0.0	0.0.0.0	martian	martian		
* 12.31.0.0	255.255.0.0	172.31.36.139	direct	fixed		1
* 12.31.36.139	255.255.255.255	172.31.36.139	local	addr		1
* 12.31.255.255	255.255.255.255	172.31.255.255	broadcast	broadcast		1
* 224.0.0.0	224.0.0.0	0.0.0.0	martian	martian		
* 224.0.0.0	240.0.0.0	0.0.0.0	multicast	addr		
* 255.255.255.255	255.255.255.255	255.255.255.255	broadcast	broadcast		

The following table describes the Type parameters.

Table 35 IP Routing Type Parameters

Parameter	Description
indirect	The next hop to the host or subnet destination will be forwarded through a router at the Gateway 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.

Table 35 IP Routing Type Parameters (continued)

Parameter	Description
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 36 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 RackSwitch G8264.
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).
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 38 on page 80](#)), VLAN and port for the address, and port referencing information.

Table 37 ARP Information Options

Command Syntax and Usage

show arp find *<IP address>*

Displays a single ARP entry by IP address.

Command mode: All

show arp interface port *<port alias or number>*

Displays the ARP entries on a single port.

Command mode: All

show arp vlan *<VLAN number>*

Displays the ARP entries on a single VLAN.

Command mode: All

show arp

Displays all ARP entries. including:

- 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)

For more information, see [page 80](#).

Command mode: All

show arp reply

Displays the ARP address list: IP address, IP mask, MAC address, and VLAN flags.

Command mode: All

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
12.31.36.139	255.255.255.255	00:13:0a:4f:7e:30	1	
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	

Show All ARP Entry Information

The following command displays ARP information:

show arp

Command mode: All

IP address	Flags	MAC address	VLAN	Age	Port
10.100.130.1		00:0e:40:99:cc:5d	1	276	19
10.100.130.12	P	00:22:00:d5:a8:00	1		

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

The Flags field is interpreted as follows:

Table 38 ARP 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.

BGP Information

Table 39 BGP Peer Information Options

Command Syntax and Usage

show ip bgp neighbor information

Displays BGP peer information. See [page 81](#) for a sample output.

Command mode: All

show ip bgp neighbor summary

Displays peer summary information such as AS, message received, message sent, up/down, state. See [page 82](#) for a sample output.

Command mode: All

show ip bgp information

Displays the BGP routing table. See [page 82](#) for a sample output.

Command mode: All

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	

Dump BGP Information

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

```
show ip bgp information
```

Command mode: All

Status codes: * valid, > best, i - internal							
Origin codes: i - IGP, e - EGP, ? - incomplete							
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 rmap; or, a loop detected.

OSPF Information

Table 40 OSPF Information Options

Command Syntax and Usage

show ip ospf general-information

Displays general OSPF information.

Command mode: All

See [page 85](#) for a sample output.

show ip ospf area information

Displays area information for all areas.

Command mode: All

show ip ospf area <area index>

Displays area information for a particular area index.

Command mode: All

show interface ip {<interface number>} ospf

Displays interface information for a particular interface. If no parameter is supplied, it displays information for all the interfaces.

Command mode: All

See [page 86](#) for a sample output.

show ip ospf area-virtual-link information

Displays information about all the configured virtual links.

Command mode: All

show ip ospf neighbor

Displays the status of all the current neighbors.

Command mode: All

show ip ospf summary-range <area index>

Displays the list of summary ranges belonging to non-NSSA areas.

Command mode: All

Table 40 OSPF Information Options (continued)

Command Syntax and Usage

show ip ospf summary-range-nssa *<area index>*

Displays the list of summary ranges belonging to NSSA areas.

Command mode: All

show ip ospf routes

Displays OSPF routing table.

Command mode: All

See [page 88](#) for a sample output.

show ip ospf information

Displays the OSPF information.

Command mode: All

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 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,
      Poll interval 0, Transit delay 1
Neighbor count is 1   If Events 4, Authentication type none
```

OSPF Database Information

Table 41 OSPF Database Information Options

Command Syntax and Usage

```
show ip ospf database advertising-router <router ID>
```

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.

Command mode: All

```
show ip ospf database asbr-summary [advertising-router <router ID> |
link-state-id <A.B.C.D> | self]
```

Displays ASBR summary LSAs. The usage of this command is as follows:

- a. `asbr-summary advertising-router 20.1.1.1` displays ASBR summary LSAs having the advertising router 20.1.1.1.
- b. `asbr-summary link-state-id 10.1.1.1` displays ASBR summary LSAs having the link state ID 10.1.1.1.
- c. `asbr-summary self` displays the self advertised ASBR summary LSAs.
- d. `asbr-summary` with no parameters displays all the ASBR summary LSAs.

Command mode: All

Table 41 OSPF Database Information Options (continued)

Command Syntax and Usage

show ip ospf database database-summary

Displays the following information about the LS database in a table format:

- a. Number of LSAs of each type in each area.
- b. Total number of LSAs for each area.
- c. Total number of LSAs for each LSA type for all areas combined.
- d. Total number of LSAs for all LSA types for all areas combined.

No parameters are required.

Command mode: All

show ip ospf database external [advertising-router <router ID> | link-state-id <A.B.C.D> | self]

Displays the AS-external (type 5) LSAs with detailed information of each field of the LSAs.

Command mode: All

show ip ospf database network [advertising-router <router ID> | link-state-id <A.B.C.D> | self]

Displays the network (type 2) LSAs with detailed information of each field of the LSA.network LS database.

Command mode: All

show ip ospf database nssa

Displays the NSSA (type 7) LSAs with detailed information of each field of the LSAs.

Command mode: All

show ip ospf database router [advertising-router <router ID> | link-state-id <A.B.C.D> | self]

Displays the router (type 1) LSAs with detailed information of each field of the LSAs.

Command mode: All

show ip ospf database self

Displays all the self-advertised LSAs. No parameters are required.

Command mode: All

Table 41 OSPF Database Information Options (continued)**Command Syntax and Usage**

```
show ip ospf database summary [advertising-router
  <router ID> | link-state-id <A.B.C.D> | self]
```

Displays the network summary (type 3) LSAs with detailed information of each field of the LSAs.

Command mode: All

```
show ip ospf database
```

Displays all the LSAs.

Command mode: All

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 42 OSPFv3 Information Options

Command Syntax and Usage

show ipv6 ospf area *<area index (0-2)>*

Displays the area information

show ipv6 ospf areas

Displays the OSPFv3 Area Table.

Command mode: All

show ipv6 ospf interface *<interface number>*

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 91](#).

Command mode: All

show ipv6 ospf area-virtual-link

Displays information about all the configured virtual links.

Command mode: All

show ipv6 ospf neighbor *<nbr router-id (A.B.C.D)>*

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.

Command mode: All

show ipv6 ospf host

Displays OSPFv3 host configuration information.

Command mode: All

show ipv6 ospf request-list *<nbr router-id (A.B.C.D)>*

Displays the OSPFv3 request list. If no router ID is supplied, it displays the information about all the current neighbors.

Command mode: All

show ipv6 ospf retrans-list *<nbr router-id (A.B.C.D)>*

Displays the OSPFv3 retransmission list. If no router ID is supplied, it displays the information about all the current neighbors.

Command mode: All

Table 42 OSPFv3 Information Options

Command Syntax and Usage

show ipv6 ospf summary-prefix *<area index (0-2)>*

Displays the OSPFv3 external summary-address configuration information.

Command mode: All

show ipv6 ospf redistrib-config

Displays OSPFv3 redistribution information to be applied to routes learned from the route table.

Command mode: All

show ipv6 ospf area-range information

Displays OSPFv3 summary ranges.

Command mode: All

show ipv6 ospf routes

Displays OSPFv3 routing table. To view a sample display, see [page 93](#).

Command mode: All

show ipv6 ospf border-routers

Displays OSPFv3 routes to an ABR or ASBR.

Command mode: All

show ipv6 ospf information

Displays all OSPFv3 information. To view a sample display, see [page 91](#).

Command mode: All

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          Ext Lsdb Limit: none
  Trace Value: 0x00008000     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

```

          Ospf3 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 43 OSPFv3 Database Information Options

Command Syntax and Usage

show ipv6 ospf database as-external [detail|hex]

Displays AS-External LSAs database information. If no parameter is supplied, it displays condensed information.

Command mode: All

show ipv6 ospf database inter-prefix [detail|hex]

Displays Inter-Area Prefix LSAs database information. If no parameter is supplied, it displays condensed information.

Command mode: All

show ipv6 ospf database inter-router [detail|hex]

Displays Inter-Area router LSAs database information. If no parameter is supplied, it displays condensed information.

Command mode: All

show ipv6 ospf database intra-prefix [detail|hex]

Displays Intra-Area Prefix LSAs database information. If no parameter is supplied, it displays condensed information.

Command mode: All

show ipv6 ospf database link [detail|hex]

Displays Link LSAs database information. If no parameter is supplied, it displays condensed information.

Command mode: All

show ipv6 ospf database network [detail|hex]

Displays Network LSAs database information. If no parameter is supplied, it displays condensed information.

Command mode: All

show ipv6 ospf database router [detail|hex]

Displays the Router LSAs with detailed information of each field of the LSAs. If no parameter is supplied, it displays condensed information.

Command mode: All

Table 43 OSPFv3 Database Information Options**Command Syntax and Usage****show ipv6 ospf database nssa [detail|hex]**

Displays Type-7 (NSSA) LSA database information. If no parameter is supplied, it displays condensed information.

Command mode: All

show ipv6 ospf database [detail|hex]

Displays all the LSAs.

Command mode: All

OSPFv3 Route Codes Information

The following command displays OSPFv3 route information:

show ipv6 ospf database routes

Command mode: All

Dest/ Prefix-Length	NextHp/ 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 44 Routing Information Protocol Options

Command Syntax and Usage

show ip rip routes

Displays RIP routes.

Command mode: All

For more information, see [page 94](#).

show interface ip <interface number> rip

Displays RIP user's configuration.

Command mode: All

For more information, see [page 95](#).

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 interface ip <interface number> rip
```

Command mode: All

```
RIP USER CONFIGURATION :
  RIP on update 30
  RIP Interface 1 : 10.4.4.2,          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 45](#) describes the IPv6 Routing information options.

Table 45 IPv6 Routing Information Options

Command Syntax and Usage

```
show ipv6 route address <IPv6 address>
```

Displays a single route by destination IP address.

```
show ipv6 route gateway <default gateway address>
```

Displays routes to a single gateway.

```
show ipv6 route type {connected|static|ospf}
```

Displays routes of a single type. For a description of IP routing types, see [Table 35 on page 77](#).

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

Displays routes on a single interface.

```
show ipv6 route summary
```

Displays a summary of IPv6 routing information, including inactive routes.

```
show ipv6 route
```

Displays all IPv6 routing information. For more information, see [page 96](#).

IPv6 Routing Table Information

The following command displays IPv6 routing information:

show ipv6 route

Command mode: All

```
IPv6 Routing Table - 3 entries
Codes : C - Connected, S - Static
        O - OSPF
        M - 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]
```

Note that 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 46 IPv6 Neighbor Discovery Cache Information Options

Command Syntax and Usage

show ipv6 neighbors find <IPv6 address>

Displays a single IPv6 Neighbor Discovery cache entry by IP address.

Command mode: All

show ipv6 neighbors interface port <port alias or number>

Displays IPv6 Neighbor Discovery cache entries on a single port.

Command mode: All

show ipv6 neighbors vlan <VLAN number>

Displays IPv6 Neighbor Discovery cache entries on a single VLAN.

Command mode: All

show ipv6 neighbors static

Displays static IPv6 Neighbor Discovery cache entries.

Command mode: All

show ipv6 neighbors

Displays all IPv6 Neighbor Discovery cache entries.

Command mode: All

For more information, see [page 97](#).

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	1
fe80::250:bfff:feb7:76b0	0	00:50:bf:b7:76:b0	Stale	2	1	2

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 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                    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 health-check ping interval: 1
ECMP health-check retries number: 3
ECMP Hash Mechanism: dipsip
```

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

IGMP Multicast Group Information

Table 47 IGMP Multicast Group Information Options

Command Syntax and Usage

show ip igmp querier vlan *<VLAN number>*

Displays IGMP Querier information. For details, see [page 100](#).

Command mode: All

show ip igmp snoop

Displays IGMP Snooping information.

Command mode: All

show ip igmp mrouter information

Displays IGMP Multicast Router information.

Command mode: All

show ip igmp mrouter vlan *<VLAN number>*

Displays IGMP Multicast Router information for the specified VLAN.

Command mode: All

show ip igmp filtering

Displays current IGMP Filtering parameters.

Command mode: All

show ip igmp profile *<1-16>*

Displays information about the current IGMP filter.

Command mode: All

show ip igmp ipmcgrp

Displays IPMC group entries learned by the switch.

Command mode: All

show ip igmp groups address *<IP address>*

Displays a single IGMP multicast group by its IP address.

Command mode: All

Table 47 IGMP Multicast Group Information Options (continued)

Command Syntax and Usage

show ip igmp groups vlan <VLAN number>

Displays all IGMP multicast groups on a single VLAN.

Command mode: All

show ip igmp groups interface port <port alias or number>

Displays all IGMP multicast groups on a single port.

Command mode: All

show ip igmp groups portchannel <trunk number>

Displays all IGMP multicast groups on a single trunk group.

Command mode: All

show ip igmp groups detail <IP address>

Displays details about an IGMP multicast group, including source and timer information.

Command mode: All

show ip igmp groups

Displays information for all multicast groups.

Command mode: All

IGMP Querier Information

The following command displays IGMP Querier information:

show ip igmp querier <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
- 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	4	V3	INC	4:16	Yes
10.1.1.5	232.1.1.1	2	4	V3	INC	4:16	Yes
*	232.1.1.1	2	4	V3	INC	-	No
10.10.10.43	235.0.0.1	9	1	V3	INC	2:26	Yes
*	236.0.0.1	9	1	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	21	V3	4:09	128	2	125
10.1.1.5	2	23	V2	4:09	125	-	-
10.10.10.43	9	24	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)

VRRP Information

Virtual Router Redundancy Protocol (VRRP) support on RackSwitch G8264 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.
 - `rener` 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 127.31.35.5      255.255.0.0  172.31.255.255,  vlan 1,   up
 2: IP6 2002:0:0:0:0:0:5/64 ,          vlan 1,   up
    fe80::213:aff:fe4f:7c01
 3: IP6 3003:0:0:0:0:0:5/64 ,          vlan 2,   up
    fe80::213:aff:fe4f:7c02

127: IP6 10:90:90:0:0:0:0:97/64 ,          vlan 4095, DOWN
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: IPv6 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:
  1: 10.200.30.3      255.255.0.0      10.200.255.255,  vlan 1, up
  2: IP6 10:90:90:0:0:0:0:91/64      , vlan 4094, up
      fe80::222:ff:fe7d:717e

Default gateway information: metric strict
  1: 10.200.1.1,      vlan any,  up

Default IP6 gateway information:

Current BOOTP relay settings: OFF
Current primary BOOTP server: 0.0.0.0
Current secondary BOOTP server: 0.0.0.0

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

Current network filter settings:
  none

Current route map settings:

```

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.

PIM Information

Table 48 PIM Information Options

Command Syntax and Usage

show ip pim bsr [*<component ID>*]

Displays information about the PIM bootstrap router (BSR).

Command mode: All

show ip pim component [*<component ID (1-2)>*]

Displays PIM component information. For details, see [page 109](#).

Command mode: All

show ip pim interface [*<interface number>*] | **detail**

Displays PIM interface information. To view sample output, see [page 110](#).

Command mode: All

show ip pim neighbor [*<interface number>*]

Displays PIM neighbor information. To view sample output, see [page 110](#).

Command mode: All

show ip pim neighbor-filters

Displays information about PIM neighbor filters.

Command mode: All

show ip pim mroute [*<component ID>*] **count** | **flags** |
group *<multicast group address>* | **inteface** *<interface number>* |
source *<multicast source address>*

Displays information about PIM multicast routes. For more information about displaying PIM multicast route information, see [page 111](#).

Command mode: All

show ip pim rp-candidate [*<component ID>*]

Displays a list of the candidate Rendezvous Points configured.

Command mode: All

Table 48 PIM Information Options**Command Syntax and Usage**

```
show ip pim rp-set [<RP IP address>]
```

Displays a list of the Rendezvous Points learned.

Command mode: All

```
show ip pim rp-static [<component ID>]
```

Displays a list of the static Rendezvous Points configured.

Command mode: All

```
show ip pim elected-rp [group <multicast group address>]
```

Displays a list of the elected Rendezvous Points.

Command mode: All

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 49 PIM Multicast Route Information Options

Command Syntax and Usage

show ip pim mroute [*<component ID>*]

Displays PIM multicast routes for the selected component.

Command mode: All

show ip pim mroute flags [*s*] [*r*] [*w*]

Displays PIM multicast routes based on the selected entry flags. Enter flags in any combination:

- s**: Shortest Path Tree (SPT) bit
- r**: Rendezvous Point Tree (RPT) bit
- w**: Wildcard bit

Command mode: All

show ip pim mroute group *<multicast group IP address>*

Displays PIM multicast routes for the selected multicast group.

Command mode: All

show ip pim mroute interface *<interface number>*

Displays PIM multicast routes for the selected incoming IP interface.

Command mode: All

show ip pim mroute source *<multicast source IP address>*

Displays PIM multicast routes for the selected source IP address.

Command mode: All

Table 49 PIM Multicast Route Information Options (continued)**Command Syntax and Usage****show ip pim mroute count**

Displays a count of PIM multicast routes of each type.

Command mode: All

show ip pim mroute

Displays information about all PIM multicast routes.

Command mode: All

PIM Multicast Route Information

The following command displays PIM multicast route information:

show ip pim mroute

Command mode: All

```

IP Multicast Routing Table
-----
Route Flags S: SPT Bit W: Wild Card Bit R: RPT Bit
Timers: Uptime/Expires
Interface State: Interface, State/Mode

PIM Multicast Routing Table for Component 1
(*, 224.1.0.0), 00:04:35/--- , RP:12.0.0.1
Incoming Interface: vlan1, RPF nbr: NULL, Route Flags: WR
Outgoing InterfaceList:
vlan2, Forwarding/Sparse, 00:04:35/---
(12.0.0.30,224.1.0.0), 00:00:04/00:03:26
Incoming Interface : vlan1, RPF nbr : NULL, Route Flags : S
Outgoing InterfaceList
vlan2, Forwarding/Sparse, 00:00:04/---

```


Quality of Service Information

Table 50 QoS information Options

Command Syntax and Usage

show qos transmit-queue

Displays mapping of 802.1p value to Class of Service queue number, and COS queue weight value.

Command mode: All

show qos transmit-queue information

Displays all 802.1p information.

Command mode: All

For details, see [page 114](#).

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
-----  -
1         0        0      1
2         0        0      1
3         0        0      1
4         0        0      1
5         0        0      1
6         0        0      1
7         0        0      1
8         0        0      1
9         0        0      1
10        0        0      1
...

```

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

Table 51 802.1p 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 52 802.1p 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.

Access Control List Information Commands

Table 53 ACL Information Options

Command Syntax and Usage

show access-control list *<ACL number>*

Displays ACL list information. For details, see [page 116](#).

Command mode: All

show access-control list6 *<ACL number>*

Displays IPv6 ACL list information.

Command mode: All

show access-control group *<ACL group number>*

Displays ACL group information.

Command mode: All

show access-control vmap *<VMAP number>*

Displays VMAP information.

Command mode: All

Access Control List Information

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

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

Command mode: All

```
Current ACL List information:
-----
Filter 1 profile:
  Ethernet
    - SMAC      : 00:00:aa:aa:01:fe/ff:ff:ff:ff:ff:ff
    - DMAC      : 00:0d:60:9c:ec:d5/ff:ff:ff:ff:ff:ff
    - VID       : 10/0xfff
    - Ethertype : IP (0x0800)
    - Priority   : 3
  Meter
    - Set to disabled
    - Set committed rate : 64
    - Set max burst size : 32
  Re-Mark
    - Set use of TOS precedence to disabled
  Packet Format
    - Ethernet format : None
    - Tagging format  : Any
    - IP format       : None
  Actions          : Deny
  Statistics       : enabled

Mirror Target Configuration:
  Mirror target destination: port
  Egress port for mirror target: 4
```

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

Table 54 ACL List Parameter Descriptions

Parameter	Description
Filter x profile	Indicates the ACL number.
Ethernet	Displays the ACL Ethernet header parameters, if configured.
IPv4	Displays the ACL IPv4 header parameters, if configured.
TCP/UDP	Displays the ACL TCP/UDP header parameters, if configured.
Meter	Displays the ACL meter parameters.
Re-Mark	Displays the ACL re-mark parameters.

Table 54 ACL List Parameter Descriptions (continued)

Parameter	Description
Packet Format	Displays the ACL Packet Format parameters, if configured.
Actions	Displays the configured action for the ACL.
Statistics	Displays status of ACL statistics (enabled or disabled).
Mirror Target Configuration	Displays ACL port mirroring parameters.

RMON Information Commands

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

Table 55 RMON Information Options

Command Syntax and Usage

show rmon history

Displays RMON History information. For details, see [page 118](#).

Command mode: All

show rmon alarm

Displays RMON Alarm information. For details, see [page 119](#).

Command mode: All

show rmon event

Displays RMON Event information. For details, see [page 120](#).

Command mode: All

show rmon

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 56 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 57 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"> <input type="checkbox"/> <code>abs</code>—absolute value, the value of the selected variable is compared directly with the thresholds at the end of the sampling interval. <input type="checkbox"/> <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.
Type	Displays the type of alarm, as follows: <ul style="list-style-type: none"> <input type="checkbox"/> <code>falling</code>—alarm is triggered when a falling threshold is crossed. <input type="checkbox"/> <code>rising</code>—alarm is triggered when a rising threshold is crossed. <input type="checkbox"/> <code>either</code>—alarm is triggered when either a rising or falling threshold is crossed.

Table 57 RMON Alarm Parameter Descriptions (continued)

Parameter	Description
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.
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 58 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
----	----	-----	-----	--TX--	--RX--	-----
1	1	40000	full	no	no	down
2	2	10000	full	no	no	down
3	3	10000	full	no	no	down
4	4	10000	full	no	no	down
5	5	40000	full	no	no	down
6	6	10000	full	no	no	down
7	7	10000	full	no	no	down
8	8	10000	full	no	no	down
9	9	40000	full	no	no	down
10	10	10000	full	no	no	down
11	11	10000	full	no	no	down
12	12	10000	full	no	no	down
13	13	40000	full	no	no	down
14	14	10000	full	no	no	down
15	15	10000	full	no	no	down
16	16	10000	full	no	no	down
17	17	10000	full	no	no	disabled
18	18	1G/10G	full	no	no	down
19	19	1G/10G	full	no	no	down
20	20	1G/10G	full	no	no	down
21	21	1G/10G	full	no	no	down
22	22	1G/10G	full	no	no	down
...						
58	58	10000	full	no	no	disabled
59	59	10000	full	no	no	disabled
60	60	1G/10G	full	no	no	down
61	61	1G/10G	full	no	no	down
62	62	1G/10G	full	no	no	down
63	63	1G/10G	full	no	no	down
64	64	1G/10G	full	no	no	down
MGT	65	1000	full	yes	yes	up

Use this command to display link status information about each port on the G8264, 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)

Port Information

The following command displays port information:

show interface trunk <port alias or number>

Command mode: All

Alias	Port	Tag	RMON	Lrn	Fld	PVID	NAME	VLAN(s)
1	1	n	d	e	e	1		1
2	2	n	d	e	e	1		1
3	3	n	d	e	e	1		1
4	4	n	d	e	e	1		1
5	5	n	d	e	e	1		1
6	6	n	d	e	e	1		1
7	7	n	d	e	e	1		1
8	8	n	d	e	e	1		1
9	9	n	d	e	e	1		1
10	10	n	d	e	e	1		1
...								
58	58	n	d	e	e	1		1
59	59	n	d	e	e	1		1
60	60	n	d	e	e	1		1
61	61	n	d	e	e	1		1
62	62	n	d	e	e	1		1
63	63	n	d	e	e	1		1
64	64	n	d	e	e	1		1
MGT	65	n	d	e	e	4095		4095

* = PVID is tagged.

Port information includes:

- Port alias and number
- Whether the port uses VLAN tagging or not (y or n)
- Whether the port has FDB learning enabled (**Lrn**)
- Whether the port has Port Flood Blocking enabled (**Fld**)
- Port VLAN ID (**PVID**)
- Port name
- VLAN membership

Port Transceiver Status

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

show interface transceiver

Command mode: All

Name	TX	RXLos	TXFlt	Volts	DegsC	TXuW	RXuW	Media	Laser	Approval
1 Q10G 1.A	Ena	LINK	no	0.00	0.0	N/A	N/A	CX QSFP 0nm		Accepted
Amphenol			Part:582410002			Date:100524	S/N:APF10200020040			
2 Q10G 1.B	Ena	LINK	no	0.00	0.0	N/A	N/A	CX QSFP 0nm		Accepted
Amphenol			Part:582410002			Date:100524	S/N:APF10200020040			
3 Q10G 1.C	Ena	LINK	no	0.00	0.0	N/A	N/A	CX QSFP 0nm		Accepted
Amphenol			Part:582410002			Date:100524	S/N:APF10200020040			
4 Q10G 1.D	Ena	LINK	no	0.00	0.0	N/A	N/A	CX QSFP 0nm		Accepted
Amphenol			Part:582410002			Date:100524	S/N:APF10200020040			
5 QSFP+ 2	Ena	LINK	no	3.29	27.0	N/A	N/A	SR QSFP 0nm		Accepted
Blade-Network			Part:BN-CKM-QP-SR4			Date:101102	S/N:BNTS10440U			
9 QSFP+ 3	Ena	LINK	no	0.00	1.5	N/A	N/A	SR QSFP 0nm		Accepted
Amphenol			Part:594090007			Date:101013	S/N:APF10410070003			
13 Q10G 4.A	Ena	LINK	no	0.00	0.0	N/A	N/A	CX QSFP 0nm		Accepted
Amphenol			Part:582410003			Date:100524	S/N:APF10200030008			
14 Q10G 4.B	Ena	LINK	no	0.00	0.0	N/A	N/A	CX QSFP 0nm		Accepted
Amphenol			Part:582410003			Date:100524	S/N:APF10200030008			
15 Q10G 4.C	Ena	LINK	no	0.00	0.0	N/A	N/A	CX QSFP 0nm		Accepted
Amphenol			Part:582410003			Date:100524	S/N:APF10200030008			
16 Q10G 4.D	Ena	LINK	no	0.00	0.0	N/A	N/A	CX QSFP 0nm		Accepted
Amphenol			Part:582410003			Date:100524	S/N:APF10200030008			
17 SFP+ 1	N/A	LINK	-N/A-	---	---	---	---	3m DAC	-N/A-	Approved
BLADE NETWORKS			Part:BN-SP-CBL-3M			Date:100411	S/N:APF101400300EU			
18 SFP+ 2	< NO Device Installed >									
19 SFP+ 3	< NO Device Installed >									
20 SFP+ 4	< NO Device Installed >									
21 SFP+ 5	< NO Device Installed >									
22 SFP+ 6	N/A	LINK	-N/A-	---	---	---	---	3m DAC	-N/A-	Approved
BLADE NETWORKS			Part:BN-SP-CBL-3M			Date:100413	S/N:APF1014003001M			
23 SFP+ 7	N/A	LINK	-N/A-	---	---	---	---	3m DAC	-N/A-	Approved
BLADE NETWORKS			Part:BN-SP-CBL-3M			Date:100414	S/N:APF101500300HE			
24 SFP+ 8	N/A	LINK	-N/A-	---	---	---	---	3m DAC	-N/A-	Approved
BLADE NETWORKS			Part:BN-SP-CBL-3M			Date:090821	S/N:APF09340030101			
25 SFP+ 9	N/A	LINK	-N/A-	---	---	---	---	3m DAC	-N/A-	Approved
BLADE NETWORKS			Part:BN-SP-CBL-3M			Date:100413	S/N:APF1014003003N			
26 SFP+ 10	N/A	LINK	-N/A-	---	---	---	---	3m DAC	-N/A-	Approved
BLADE NETWORKS			Part:BN-SP-CBL-3M			Date:100503	S/N:APF101800303U1			
...										

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

- Name identifies the port number and media type
- TX enable/disable
- 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/Transceiver type (LX, LR, SX, SR)
- Laser wavelength, in nano-meters
- Approval status

Virtual Machines Information

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

Table 59 Virtual Machines Information Options

Command Syntax and Usage

show virt port *<port alias or number>*

Displays Virtual Machine information for the selected port.

Command mode: All

show virt vm

Displays all Virtual Machine information.

Command mode: All

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	3	
*127.31.46.10	00:50:56:4f:f2:85	2	4	
+127.31.46.51	00:50:56:72:ec:86	1	3	
+127.31.46.11	00:50:56:7c:1c:ca	3	4	
127.31.46.25	00:50:56:9c:00:c8	5	4	
127.31.46.15	00:50:56:9c:21:2f	0	4	
127.31.46.35	00:50:56:9c:29:29	6	3	

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
- Server port on which the VM was detected
- VM group that contains the VM, if applicable
- State of the Virtual Machine (~ indicates the VM is inactive/idle)

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 60 VMware Information Options

Command Syntax and Usage

show virt vmware hosts

Displays a list of VMware hosts.

Command mode: All

show virt vmware showhost *<host UUID>* | *<host IP address>* | *<host name>*

Displays detailed information about a specific VMware host.

Command mode: All

show virt vmware showvm *<VM UUID>* | *<VM IP address>* | *<VM name>*

Displays detailed information about a specific Virtual Machine (VM).

Command mode: All

show virt vmware vms

Displays a the names of all VMware VMs.

Command mode: All

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.

vNIC Information

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

Table 61 vNIC Information Options

Command Syntax and Usage

```
show vnic vnic
```

Displays information about each vNIC.

Command mode: All

Table 61 vNIC Information Options**Command Syntax and Usage****show vnic vnicgroup**

Displays information about each vNIC Group, including:

- ❑ 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)

Command mode: All

show vnic information-dump

Displays all vNIC information.

Command mode: All

Virtual NIC (vNIC) Information

The following command displays Virtual NIC (vNIC) information:

show vnic vnic

Command mode: All

vNIC	vNICGroup	Vlan	MaxBandwidth	MACAddress	Link
1.1	10	10	25	none	down
50.2	4	44	25	00 :00 :c9 :93 :d2 :07	up
53.1	#	*	10	none	disabled
53.4	4	44	25	00 :00 :c9 :93 :d5 :03	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          : 3001
Failover      : enabled

vNIC          Link
-----
1.1          up
7.1          up
8.1          down
9.1          up
10.1         up

Port          Link
-----
2            up

UplinkPort    Link
-----
10           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)

Converged Enhanced Ethernet Information

[Table 62](#) describes the Converged Enhanced Ethernet (CEE) information options.

Table 62 CEE Information Options

Command Syntax and Usage

show cee information

Displays all CEE information

Command mode: All

DCBX Information

[Table 63](#) describes the Data Center Bridging Capability Exchange (DCBX) protocol information options.

Table 63 DCBX Information Options

Command Syntax and Usage

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

Displays information about the DCBX Control state machine for the selected port.
For details, see [page 132](#).

Command mode: All

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

Displays information about the DCBX Feature state machine for the selected port.
For details, see [page 133](#).

Command mode: All

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

Displays information about the DCBX ETS state machine. For details, see [page 134](#).

Command mode: All

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

Displays information about the DCBX PFC state machine. For details, see [page 135](#).

Command mode: All

Table 63 DCBX Information Options**Command Syntax and Usage**

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

Displays information about the DCBX Application Protocol state machine on the selected port. For details, see [page 136](#).

Command mode: All

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

Displays all DCBX information.

Command mode: All

DCBX Control Information

The following command displays DCBX Control information:

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

Command mode: All

Alias	Port	OperStatus	OperVer	MaxVer	SeqNo	AckNo
1	1	enabled	0	0	0	0
2	2	enabled	0	0	4	2
3	3	enabled	0	0	0	0
4	4	enabled	0	0	1	1
...						
20	20	enabled	0	0	0	0
21	21	enabled	0	0	0	0
22	22	enabled	0	0	0	0
23	23	enabled	0	0	0	0
24	24	enabled	0	0	0	0

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
-----
  1  1   ETS   enabled No  Yes  0   0   No    0   No disabled No
  2  2   ETS   enabled No  Yes  0   0   Yes   4   No  enabled Yes
  3  3   ETS   enabled No  Yes  0   0   No    0   No disabled No
  4  4   ETS   enabled No  Yes  0   0   Yes   1   No  enabled Yes
  5  5   ETS   enabled No  Yes  0   0   Yes   1   No  enabled Yes
  6  6   ETS   disabled No  Yes  0   0   No    0   No disabled No
  7  7   ETS   disabled No  Yes  0   0   No    0   No disabled No
  8  8   ETS   disabled No  Yes  0   0   No    0   No disabled No
  9  9   ETS   disabled No  Yes  0   0   No    0   No disabled No
 10 10   ETS   enabled No  Yes  0   0   No    0   No disabled No
...

```

The following table describes the DCBX Feature information.

Table 64 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.

Table 64 DCBX Feature Information Fields

Parameter	Description
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
-----
  2  2    0      PGID0  PGID0  PGID0
  2  2    1      PGID0  PGID0  PGID0
  2  2    2      PGID0  PGID0  PGID0
  2  2    3      PGID1  PGID0  PGID0
  2  2    4      PGID2  PGID0  PGID0
  2  2    5      PGID2  PGID0  PGID0
  2  2    6      PGID2  PGID0  PGID0
  2  2    7      PGID2  PGID0  PGID0

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

```

The following table describes the DCBX ETS information.

Table 65 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

Table 65 DCBX Feature Information Fields

Parameter	Description
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
-----
  2  2  0      disabled   disabled   disabled
  2  2  1      disabled   disabled   disabled
  2  2  2      disabled   disabled   disabled
  2  2  3      enabled    disabled   disabled
  2  2  4      disabled   disabled   disabled
  2  2  5      disabled   disabled   disabled
  2  2  6      disabled   disabled   disabled
  2  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
-----
  2  2  0      enabled    enabled    enabled
  2  2  1      disabled   disabled   disabled
  2  2  2      disabled   disabled   disabled
  2  2  3      enabled    enabled    enabled
  2  2  4      disabled   disabled   disabled
  2  2  5      disabled   disabled   disabled
  2  2  6      disabled   disabled   disabled
  2  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
-----
  2  2  0      enabled    enabled    enabled
  2  2  1      disabled   disabled   disabled
  2  2  2      disabled   disabled   disabled
  2  2  3      enabled    enabled    enabled
  2  2  4      disabled   disabled   disabled
  2  2  5      disabled   disabled   disabled
  2  2  6      disabled   disabled   disabled
  2  2  7      disabled   disabled   disabled

```


The following table describes the DCBX Application Protocol information.

Table 66 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"> <input type="checkbox"/> 0 = Ethernet Type <input type="checkbox"/> 1 = TCP socket ID
Organizationally Unique ID	DCBX TLV identifier
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 67](#) describes the Enhanced Transmission Selection (ETS) information options

Table 67 ETS Information Options

Command Syntax and Usage

show cee global ets information

Displays global ETS information.

Command mode: All

The following command displays ETS information:

```
show cee global ets information
```

Command mode: All

```
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
```

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 68 describes the Priority Flow Control (PFC) information options.

Table 68 PFC Information Options

Command Syntax and Usage

show cee global pfc priority <0-7>

Displays PFC information.

Command mode: All

show cee global pfc information

Displays PFC information.

Command mode: All

The following command displays PFC information:

show cee global pfc information

Command mode: All

```
Global PFC Information:
```

```
PFC - ON
```

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 69 describes the Fiber Channel over Ethernet (FCoE) information options.

Table 69 FCoE Information Options

Command Syntax and Usage

show fcoe information

Displays all current FCoE information.

Command mode: All

FIP Snooping Information

Table 70 describes the Fiber Channel Initialization Protocol (FIP) Snooping information options

Table 70 FIP Snooping Information Options

Command Syntax and Usage

show fcoe fips port <port alias or number> information

Displays FIP Snooping (FIPS) information for the selected port, including a list of current FIPS ACLs.

Command mode: All

show fcoe fips fcf

Displays FCF information for all ports.

Command mode: All

show fcoe fips fcoe

Displays FCoE connections established on the switch.

Command mode: All

show fcoe fips information

Displays FIP Snooping information for all ports.

Command mode: All

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:

- Fiber 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 71 Statistics Commands

Command Syntax and Usage

show layer3 counters

Command mode: All

Displays Layer 3 statistics.

show snmp-server counters

Command mode: All

Displays SNMP statistics. See [page 215](#) for sample output.

show ntp counters

Displays Network Time Protocol (NTP) Statistics.

Command mode: All

See [page 219](#) for a sample output and a description of NTP Statistics.

show counters

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 220](#).

Port Statistics

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

Table 72 Port Statistics Commands

Command Syntax and Usage

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

Displays IEEE 802.1X statistics for the port. See [page 146](#) for sample output.

Command mode: All

show interface port *<port alias or number>* **bitrate-usage**

Displays the traffic rate in kilobits per second.

Command mode: All

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

Displays bridging (“dot1”) statistics for the port.

Command mode: All

See [page 150](#) for sample output.

show interface port *<port alias or number>* **bridging-rate**

Displays per-second bridging (“dot1”) statistics for the port.

Command mode: All

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

Displays Ethernet (“dot3”) statistics for the port.

Command mode: All

See [page 152](#) for sample output.

show interface port *<port alias or number>* **ethernet-rate**

Displays per-second Ethernet (“dot3”) statistics for the port.

Command mode: All

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

Displays interface statistics for the port. See [page 154](#) for sample output.

Command mode: All

Table 72 Port Statistics Commands

Command Syntax and Usage

show interface port *<port alias or number>* **interface-rate**

Displays per-second interface statistics for the port.

Command mode: All

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

Displays IP statistics for the port. See [page 157](#) for sample output.

Command mode: All

show interface port *<port alias or number>* **ip-rate**

Displays per-second IP statistics for the port.

Command mode: All

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

Displays link statistics for the port. See [page 157](#) for sample output.

Command mode: All

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

Displays Remote Monitoring (RMON) statistics for the port. See [page 158](#) for sample output.

Command mode: All

show interface port *<port alias or number>* **oam-counters**

Displays Operation, Administrative, and Maintenance (OAM) protocol statistics for the port.

Command mode: All

clear interface port *<port alias or number>* **counters**

Clears all statistics for the port.

Command mode: Privileged EXEC

clear counters

Clears statistics for all ports.

Command mode: Privileged EXEC

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 73 802.1X 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 74 802.1X 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.
authEapLogoffsWhile Connecting	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.
authSuccessesWhile Authenticating	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.

Table 74 802.1X Authenticator Diagnostics of a Port

Statistics	Description
authTimeoutsWhile Authenticating	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.
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.

Table 74 802.1X Authenticator Diagnostics of a Port

Statistics	Description
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.
backendNonNakResponses FromSupplicant	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.

Use the following command to display the Active Multipath Protocol (AMP) statistics of the selected port:

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

Command mode: All

```
AMP statistics for port 1:
Keep-alive packets sent:           0
Keep-alive packets rcvd:          0
Fdb-Flush packets sent:           0
Fdb-Flush packets rcvd:           0
Dropped packets                   :
```

Table 75 AMP Statistics of a Port

Statistics	Description
Keep-alive packets sent	Number of keep-alive packets sent.
Keep-alive packets rcvd	Number of keep-alive packets received.
Fdb-Flush packets sent	Number of FDB-flush packets sent.

Table 75 AMP Statistics of a Port

Statistics	Description
Fdb-Flush packets rcvd	Number of FDB-flush packets received.
Dropped packets	Number of invalid AMP packets dropped.

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 1:
dot1PortInFrames:          63242584
dot1PortOutFrames:        63277826
dot1PortInDiscards:       0
dot1TpLearnedEntryDiscards: 0
dot1StpPortForwardTransitions: 0
```

Table 76 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.

Table 76 Bridging Statistics of a Port

Statistics	Description
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 1:
dot3StatsAlignmentErrors:                0
dot3StatsFCSErrors:                      0
dot3StatsSingleCollisionFrames:          0
dot3StatsMultipleCollisionFrames:        0
dot3StatsLateCollisions:                 0
dot3StatsExcessiveCollisions:            0
dot3StatsInternalMacTransmitErrors:      NA
dot3StatsFrameTooLongs:                  0
dot3StatsInternalMacReceiveErrors:       0
```

Table 77 Ethernet Statistics of a Port

Statistics	Description
dot3StatsAlignmentErrors	<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 77 Ethernet Statistics of a Port

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 77 Ethernet Statistics of a Port

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>
dot3StatsInternalMacReceiveErrors	<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 1:
                ifHCIn Counters          ifHCOut Counters
Octets:                51697080313          51721056808
UcastPkts:              65356399           65385714
BroadcastPkts:          0                   6516
MulticastPkts:          0                   0
FlowCtrlPkts:           0                   0
Discards:               0                   0
Errors:                 0                   21187

```

Table 78 Interface Statistics of a 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.
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> .

Table 78 Interface Statistics of a Port

Statistics	Description
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 pause 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.

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 1:
ipInReceives   :      0
ipInHeaderError:      0
ipInDiscards   :      0
```

Table 79 Interface Protocol Statistics of a Port

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 1:
linkStateChange:      1
```

Table 80 Link Statistics of a Port

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 81 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.

Table 81 RMON Statistics of a Port

Statistics	Description
etherStatsCRCAAlignErrors	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).
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).

Table 81 RMON Statistics of a Port

Statistics	Description
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).

Layer 2 Statistics

Table 82 Layer 2 Statistics Commands

Command Syntax and Usage

show mac-address-table counters

Displays FDB statistics.

Command mode: All

See [page 162](#) for sample output.

clear mac-address-table counters

Clears FDB statistics.

Command mode: Privileged EXEC

show interface port <port alias or number> lacp counters

Displays Link Aggregation Control Protocol (LACP) statistics.

Command mode: All

See [page 163](#) for sample output.

clear interface port <port alias or number> lacp counters

Clears Link Aggregation Control Protocol (LACP) statistics.

Command mode: Privileged EXEC

show hotlinks counters

Displays Hot Links statistics.

Command mode: All

See [page 164](#) for sample output.

clear hotlinks

Clears all Hot Links statistics.

Command mode: Privileged EXEC

Table 82 Layer 2 Statistics Commands**Command Syntax and Usage**

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

Displays LLDP statistics.

Command mode: All

See [page 165](#) for sample output.

```
show oam counters
```

Displays OAM statistics.

Command mode: All

See [page 166](#) for sample output.

FDB Statistics

Use the following command to display statistics regarding the use of the forwarding database, including the number of new entries, finds, and unsuccessful searches:

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

Command mode: All

FDB statistics:			
current:	83	hiwat:	855

FDB statistics are described in the following table:

Table 83 Forwarding Database Statistics

Statistic	Description
current	Current number of entries in the Forwarding Database.
hiwat	Highest number of entries recorded at any given time in the Forwarding Database.

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 1:
-----
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 84 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 85 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 1 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 86 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 1
-----
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 87 vLAG Statistics Options

Command Syntax and Usage

show vlag isl-counters

Displays vLAG ISL statistics for the selected port. See [page 167](#) for sample output.

clear vlag counters

Clears all vLAG statistics.

show vlag statistics

Displays all vLAG statistics. See [page 168](#) for sample output.

vLAG ISL Statistics

Use the following command to display vLAG statistics:

show vlag isl-counters

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 Key Enable    0      Peer Key Disable 0
FDB Static Add:    0      FDB Static Del:  0
FDB Dynamic Add:  0      FDB Dynamic Del: 0
FDB Inactive Add: 0      FDB Inactive Del:0
STP State:         0      STP BPDU Forward:0
Health Check:     0      IGMP Hello:      0
Other:            0      Unknown:         0

State Machine:

vLAG PDU received:
Role Election:      0      System Info      0
Peer Key Enable    0      Peer Key Disable 0
FDB Static Add:    0      FDB Static Del:  0
FDB Dynamic Add:  0      FDB Dynamic Del: 0
FDB Inactive Add: 0      FDB Inactive Del:0
STP State:         0      STP BPDU Forward:0
Health Check:     0      IGMP Hello:      0
Other:            0      Unknown:         0

```

The following table describes the vLAG statistics:

Table 88 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 Key Enable	Total number of vLAG PDUs sent for enabling peer key.
Peer Key Disable	Total number of vLAG PDUs sent for disabling peer key.
FDB Static Add	Total number of vLAG PDUs sent for addition of FDB static entry.
FDB Static Del	Total number of vLAG PDUs sent for deletion of FDB static entry.
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.

Table 88 VLAG Statistics

Statistic	Description
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.
STP State	Total number of vLAG PDUs sent for synchronizing STP state.
STP BPDU Forward	Total number of vLAG PDUs sent for STP BPDU forward.
Health Check	Total number of vLAG PDUs sent for health checks.
IGMP Hello	Total number of vLAG PDUs sent for IGMP hello.
Other	Total number of vLAG PDUs sent for other reasons.
Unknown	Total number of vLAG PDUs sent for unknown operations.

Layer 3 Statistics

Table 89 Layer 3 Statistics Commands

Command Syntax and Usage

show ip gea

show ip gea bucket *<IP address>*

show ip gea ecmp *<IP address>*

Displays Gigabit Ethernet Aggregators (GEA) statistics. GEA statistics are used by service and support personnel.

Command mode: All

show ip counters

Displays IP statistics. See [page 174](#) for sample output.

Command mode: All

clear ip counters

Clears IPv4 statistics. Use this command with caution as it deletes all the IPv4 statistics.

Command mode: Privileged EXEC

show ip route counters

Displays route statistics. See [page 181](#) for sample output.

Command mode: All

show ip arp counters

Displays Address Resolution Protocol (ARP) statistics. See [page 183](#) for sample output.

Command mode: All

show ip dns counters

Displays Domain Name System (DNS) statistics. See [page 184](#) for sample output.

Command mode: All

show ip icmp counters

Displays ICMP statistics. See [page 184](#) for sample output.

Command mode: All

Table 89 Layer 3 Statistics Commands

Command Syntax and Usage

show ip tcp counters

Displays TCP statistics. See [page 186](#) for sample output.

Command mode: All

show ip udp counters

Displays UDP statistics. See [page 188](#) for sample output.

Command mode: All

show ip ospf counters

Displays OSPF statistics. See [page 191](#) for sample output.

Command mode: All

show ipv6 ospf counters

Displays OSPFv3 statistics. See [page 195](#) for sample output.

Command mode: All

show ip igmp counters

Displays IGMP statistics. See [page 189](#) 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 ip vrrp counters

When virtual routers are configured, you can display the protocol statistics for VRRP. See [page 200](#) for sample output.

Command mode: All

Table 89 Layer 3 Statistics Commands

Command Syntax and Usage

show ip pim counters

Displays PIM statistics for all configured PIM interfaces. See [page 201](#) 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 202](#) for sample output.

Command mode: All

clear ip arp counters

Clears Address Resolution Protocol (ARP) statistics.

Command mode: Privileged EXEC

clear ip dns counters

Clears Domain Name System (DNS) statistics.

Command mode: Privileged EXEC

clear ip icmp counters

Clears Internet Control Message Protocol (ICMP) statistics.

Command mode: Privileged EXEC

clear ip tcp counters

Clears Transmission Control Protocol (TCP) statistics.

Command mode: Privileged EXEC

clear ip udp counters

Clears User Datagram Protocol (UDP) statistics.

Command mode: Privileged EXEC

Table 89 Layer 3 Statistics Commands

Command Syntax and Usage

clear ip igmp [*<VLAN number>*] **counters**

Clears IGMP statistics.

Command mode: Privileged EXEC

clear ip vrrp **counters**

Clears VRRP statistics.

Command mode: Privileged EXEC

clear ip pim **counters**

Clears PIM statistics for all interfaces.

Command mode: Privileged EXEC

clear ip pim interface *<interface number>* **counters**

Clears PIM statistics on the selected interface.

Command mode: Privileged EXEC

clear ip **counters**

Clears IP statistics. Use this command with caution as it will delete all the IP statistics.

Command mode: Privileged EXEC

clear ip rip **counters**

Clears Routing Information Protocol (RIP) statistics.

Command mode: Privileged EXEC

clear ip ospf **counters**

Clears Open Shortest Path First (OSPF) statistics.

Command mode: Privileged EXEC

Table 89 Layer 3 Statistics Commands**Command Syntax and Usage****clear ipv6 ospf counters**

Clears Open Shortest Path First version 3 (OSPFv3) statistics.

Command mode: Privileged EXEC

show layer3 counters

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

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:	0	ipInHdrErrors:	0
ipInAddrErrors:	0		
ipInUnknownProtos:	0	ipInDiscards:	0
ipInDelivers:	0	ipOutRequests:	1274
ipOutDiscards:	0		
ipDefaultTTL:	255		

Table 90 IPv4 Statistics

Statistics	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.

Table 90 IPv4 Statistics

Statistics	Description
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.
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.
ipDefaultTTL	The default value inserted into the Time-To-Live (TTL) 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.

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   ICMPEchoReq   10  ICMPEchoReps
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   PktTooBigMsg   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 91 describes the IPv6 statistics.

Table 91 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).

Table 91 IPv6 Statistics

Statistic	Description
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.
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 92 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.

Table 92 ICMP Statistics

Statistic	Description
TimeExcds	Number of ICMP Time Exceeded messages sent.
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 93](#) describes the UDP statistics.

Table 93 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).

Route Statistics

The following command displays IPv4 route statistics:

show ip route counters

Command mode: All

```

Route statistics:
-----
ipRoutesCur:           16  ipRoutesHighWater:      16
staticRoutesCur:       0
ripRoutesCur:          0
ospfRoutesCur:         1
bgpRoutesCur:          0
ipRoutesMax:            6144

ECMP statistics:
-----
Maximum number of ECMP routes           :      6272
Maximum number of static ECMP routes    :      128
Maximum number of dynamic ECMP routes   :      6144
Number of routes with ECMP paths        :          1

```

Table 94 Route Statistics

Statistics	Description
ipRoutesCur	Total number of outstanding routes in the route table.
ipRoutesHighWater	Highest number of routes ever recorded in the route table.
staticRoutesCur	Total number of static routes in the route table.
ripRoutesCur	Total number of Routing Information Protocol (RIP) routes in the route table.
ospfRoutesCur	Total number of OSPF routes in the route table.
bgpRoutesCur	Total number of Border Gateway Protocol routes in the route table.
ipRoutesMax	Maximum number of routes that are supported.

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
Number of routes with ECMP paths   :          0
```

Table 95 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.
Number of routes with ECMP paths	Current number of routes that contain ECMP paths.

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:         2048
```

Table 96 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:
dnsOutRequests:      0
dnsBadRequests:     0
```

Table 97 DNS Statistics

Statistics	Description
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 98 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 icmpInErrors.
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.
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 icmpOutErrors.
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.

Table 98 ICMP Statistics

Statistic	Description
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:         512
tcpActiveOpens:     252214  tcpPassiveOpens:    7
tcpAttemptFails:    528     tcpEstabResets:     4
tcpInSegs:          756401  tcpOutSegs:         756655
tcpRetransSegs:     0       tcpInErrs:          0
tcpCurBuff:         0       tcpCurConn:        3
tcpOutRsts:         417
```

Table 99 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.
tcpEstabResets	The number of times TCP connections have made a direct transition to the <code>CLOSED</code> state from either the <code>ESTABLISHED</code> state or the <code>CLOSE-WAIT</code> 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.

Table 99 TCP Statistics

Statistic	Description
tcpInErrs	The total number of segments received in error (for example, bad TCP checksums).
tcpCurBuff	The total number of outstanding memory allocations from heap by TCP protocol stack.
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 100 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 the use of the IGMP Multicast Groups:

show ip igmp counters

Command mode: All

IGMP Snoop vlan 2 statistics:			

rxIgmpValidPkts:	0	rxIgmpInvalidPkts:	0
rxIgmpGenQueries:	0	rxIgmpGrpSpecificQueries:	0
rxIgmpGroupSrcSpecificQueries:	0	rxIgmpDiscardPkts:	0
rxIgmpLeaves:	0	rxIgmpReports:	0
txIgmpReports:	0	txIgmpGrpSpecificQueries:	0
rxIgmpLeaves:	0	rxIgmpV3CurrentStateRecords:	0
rxIgmpV3SourceListChangeRecords:	0	rxIgmpV3FilterChangeRecords:	0
txIgmpGenQueries:	18		

Table 101 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
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.

Table 101 IGMP Statistics

Statistic	Description
rxIcmpV3FilterChangeRecords	Total number of Filter Change records received.
txIcmpGenQueries	Total number of General Membership Query packets transmitted

OSPF Statistics

Table 102 OSPF Statistics Commands

Command Syntax and Usage

show ip ospf counters

Displays OSPF statistics. See [page 191](#) for sample output.

Command mode: All

show ip ospf area counters

Displays OSPF area statistics.

Command mode: All

show ip ospf interface [*<interface number>*] counters

Displays OSPF interface statistics.

Command mode: All

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           hello          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 103 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.
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 ls Requests	The sum total of all Link State Request packets received on all OSPF areas and interfaces.
Tx ls Requests	The sum total of all Link State Request packets transmitted on all OSPF areas and interfaces.
Rx ls Acks	The sum total of all Link State Acknowledgement packets received on all OSPF areas and interfaces.
Tx ls Acks	The sum total of all Link State Acknowledgement packets transmitted on all OSPF areas and interfaces.
Rx ls Updates	The sum total of all Link State Update packets received on all OSPF areas and interfaces.
Tx ls Updates	The sum total of all Link State Update packets transmitted on all OSPF areas and interfaces.

Table 103 OSPF General Statistics

Statistic	Description
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 should 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.
bad sequence	<p>The sum total number of Database Description packets which have been received that either:</p> <ol style="list-style-type: none"> a. Has an unexpected DD sequence number b. Unexpectedly has the init bit set c. Has an options field differing from the last Options field received in a Database Description packet. <p>Any of these conditions indicate that some error has occurred during adjacency establishment for all OSPF areas and interfaces.</p>
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.

Table 103 OSPF General Statistics

Statistic	Description
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:	
hello	The sum total number of Hello packets sent on all interfaces and 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 103 OSPF General Statistics

Statistic	Description
Timers Kickoff:	
hello	The sum total number of times the Hello timer has been fired (which triggers the send of a Hello packet) across all OPSF areas and interfaces.
retransmit	The sum total number of times the Retransmit timer has been fired across all OPSF 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 Ack timer has been fired across all OSPF areas and interfaces.
dbage	The total number of times the data base age (Dbage) 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 104 OSPFv3 Statistics Commands

Command Syntax and Usage

show ipv6 ospf counters

Displays OSPFv3 statistics.

Command mode: All

See [page 191](#) for sample output.

show ipv6 ospf area counters

Displays OSPFv3 area statistics.

Command mode: All

show ipv6 ospf interface [*<interface number>*] counters

Displays OSPFv3 interface statistics.

Command mode: All

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

Errors
  rx on pasv intf      0
  rx but ospf off      0
  rx on intf not up    0
  rx version mismatch  0
  rx rtr id is zero    0
  rx with our rtr id   0
  instance id mismatch 0
  area mismatch        0
  dest addr mismatch   0
  bad checksum         0
  no associated nbr     0
  bad packet type      0
  hello mismatch       0
  options mismatch     0
  dead mismatch        0
  bad nbma/ptomp nbr   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

```

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

Table 105 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.
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.

Table 105 OSPFv3 General Statistics

Statistics	Description
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 (that is, 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
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.

Table 105 OSPFv3 General Statistics

Statistics	Description
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 send 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 G8264 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 106 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
CandRPAAdv 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 107 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
CandRPAAdv 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

Table 107 PIM Statistics

Statistics	Description
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 reponse 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
```

DHCP Statistics

Table 108 DHCP Statistics Options

Command Syntax and Usage

show ip dhcp snooping counters

Displays DHCP Snooping statistics.

Command mode: All

clear ip dhcp snooping counters

Clears DHCP Snooping statistics.

Command mode: Privileged EXEC

DHCP Snooping Statistics

The following command displays DHCP Snooping statistics:

show ip dhcp snooping counters

Command mode: All

DHCP Snooping statistics:	
Received Request packets	2
Received Reply packets	2
Received Invalid packets	0
Dropped packets out of rate	0
Dropped packets other reason	0

DHCP Snooping Statistics count all DHCP packets processed by DHCP snooping.

Management Processor Statistics

Table 109 Management Processor Statistics Commands

Command Syntax and Usage

show mp packet counters

Displays packet statistics, to check for leads and load. To view a sample output and a description of the stats, see [page 207](#).

Command mode: All

show mp tcp-block

Displays all TCP control blocks that are in use. To view a sample output and a description of the stats, see [page 209](#).

Command mode: All

show mp udp-block

Displays all UDP control blocks that are in use. To view a sample output, see [page 210](#).

Command mode: All

show processes cpu

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 210](#).

Command mode: All

MP Packet Statistics

Table 110 Packet Statistics Commands

Command Syntax and Usage

show mp packet counters

Displays packet statistics, to check for leads and load. To view a sample output and a description of the stats, see [page 207](#).

Command mode: All

show mp packet logs

Displays a log of all packets received by the CPU.

Command mode: All

show mp packet last *<number of logs>*

Displays a list of the most recent packets received by the CPU.

Command mode: All

show mp packet arp

Displays a list of Address Resolution Protocol packets logged.

Command mode: All

show mp packet rarp

Displays a list of reverse ARP packets logged.

Command mode: All

show mp packet bpdu

Displays a list of spanning-tree Bridge Protocol Data Units logged.

Command mode: All

show mp packet cisco

Displays a list of UniDirectional Link Detection (UDLD) packets and Cisco Discovery Protocol (CDP) packets logged.

Command mode: All

show mp packet fcoe

Displays a list of Fiber Channel over Ethernet packets logged.

Command mode: All

Table 110 Packet Statistics Commands

Command Syntax and Usage

show mp packet ipv4

Displays a list of IPv4 packets logged.

Command mode: All

show mp packet ipv6

Displays a list of IPv6 packets logged.

Command mode: All

show mp packet lldp

Displays a list of Link Layer Discovery Protocol PDUs logged.

Command mode: All

show mp packet other

Displays a list of packets that are not selectable.

Command mode: All

show mp packet raw

Displays a list of raw packet buffers and headers.

Command mode: All

show mp packet dump

Displays all packet statistics and logs.

Command mode: All

MP Packet Statistics

The following command displays MP packet statistics:

show mp packet

Command mode: All

```
CPU packet statistics at 16:57:24 Sat Apr 5, 2011
```

```
Packets received by CPU:
```

```
-----
Total packets:          7642 (7642 since bootup)
BPDUs:                  5599
Cisco packets:          0
ARP packets:            1732
IPv4 packets:           113
IPv6 packets:           0
LLDP PDUs:              198
Other:                  0
```

```
Packet Buffer Statistics:
```

```
-----
allocs:                  14311
frees:                   14311
failures:                 0
dropped:                  0
```

```
small packet buffers:
```

```
-----
current:                 0
max:                     2048
threshold:               512
hi-watermark:            1
hi-water time:          14:59:46 Sat Apr 5, 2011
```

```
medium packet buffers:
```

```
-----
current:                 0
max:                     2048
threshold:               512
hi-watermark:            1
hi-water time:          14:59:49 Sat Apr 5, 2011
```

```
jumbo packet buffers:
```

```
-----
current:                 0
max:                     4
hi-watermark:            0
```

Table 111 Packet Statistics

Statistics	Description
Packets received by CPU	
Total packets	Total number of packets received
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.
IPv6 packets	Total number of IPv6 packets received.
LLDP PDUs	Total number of Link Layer Discovery Protocol data units received.
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.
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.
medium packet buffers	

Table 111 Packet Statistics

Statistics	Description
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 medium 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.

TCP Statistics

The following command displays TCP statistics:

```
show mp tcp-block
```

Command mode: All

```
All TCP allocated control blocks:
10ad41e8: 0.0.0.0          0 <=> 0.0.0.0          80 listen
10ad5790: 47.81.27.5          1171 <=> 47.80.23.243     23 established
```

Table 112 MP Specified TCP Statistics

Statistics	Description
10ad41e8/10ad5790	Memory
0.0.0.0/47.81.27.5	Destination IP address
0/1171	Destination port
0.0.0.0/47.80.23.243	Source IP

Table 112 MP Specified TCP Statistics

Statistics	Description
80/23	Source port
listen/established	State

UDP Statistics

The following command displays UDP statistics:

```
show mp udp-block
```

Command mode: All

```
All UDP allocated control blocks:
 161: listen
```

CPU Statistics

The following command displays the CPU utilization statistics:

```
show processes cpu
```

Command mode: All .

```
CPU utilization:
cpuUtil1Second:      53%
cpuUtil4Seconds:     54%
cpuUtil64Seconds:    54%
```

Table 113 CPU Statistics

Statistics	Description
cpuUtil1Second	The utilization of MP CPU over 1 second. It shows the percentage.
cpuUtil4Seconds	The utilization of MP CPU over 4 seconds. It shows the percentage.
cpuUtil64Seconds	The utilization of MP CPU over 64 seconds. It shows the percentage.

QoS Statistics

Table 114 QoS Statistics Commands

Command Syntax and Usage

show qos protocol-packet-control protocol-counters *<packet type>*

Displays the total packet count of the selected packet type received by hardware.

Command mode: All

show qos protocol-packet-control queue-counters

Displays the total number of packets received by each queue.

Command mode: All

clear qos protocol-packet-control protocol-counters *<packet type>*

Clears packet queue statistics for the selected packet type.

Command mode: All

clear qos protocol-packet-control queue-counters *<queue number>*

Clears packet queue statistics for the selected queue.

Command mode: All

clear qos protocol-packet-control all

Clears all packet queue statistics.

Command mode: All

Access Control List Statistics

Table 115 ACL Statistics Commands

Command Syntax and Usage

show access-control list *<ACL number>* **counters**

Displays the Access Control List statistics for a specific ACL.

Command mode: All

show access-control list6 *<ACL number>* **counters**

Displays the IPv6 ACL statistics for a specific ACL.

Command mode: All

show access-control macl *<MACL number>* **counters**

Displays the ACL statistics for a specific management ACL (MACL).

Command mode: All

show access-control counters

Displays all ACL statistics.

Command mode: All

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

Displays VLAN Map statistics for the selected VMAP. For a sample display, see [page 213](#).

Command mode: All

clear access-control list {*<ACL number>*|**all**} **counters**

Clears ACL statistics.

Command mode: Privileged EXEC

clear access-control list6 {*<ACL number>*|**all**} **counters**

Clears IPv6 ACL statistics.

Command mode: Privileged EXEC

clear access-control macl {*<ACL number>*|**all**} **counters**

Clears Management ACL (MACL) statistics.

Command mode: Privileged EXEC

Table 115 ACL Statistics Commands**Command Syntax and Usage**

```
clear access-control vmap {<VMAP number>} counters
```

Clears VLAN Map statistics.

Command mode: Privileged EXEC

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

Displays ACL meter statistics.

Command mode: All

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

Clears ACL meter statistics.

Command mode: Privileged EXEC

ACL Statistics

This option 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
------------------	-------

Fiber Channel over Ethernet Statistics

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

show fcoe counters

Command mode: All

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

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

Table 116 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 FCoE statistics:

clear fcoe counters

Command mode: Privileged EXEC

SNMP Statistics

The following command displays SNMP statistics:

show snmp-server counters

Command mode: All

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	snmpInReadOnly:	0
snmpInGenErrs:	0	snmpInTotalReqVars:	798464
snmpInTotalSetVars:	2731	snmpInGetRequests:	17593
snmpInGetNexts:	131389	snmpInSetRequests:	615
snmpInGetResponses:	0	snmpInTraps:	0
snmpOutTooBig:	0	snmpOutNoSuchNames:	1
snmpOutBadValues:	0	snmpOutReadOnly:	0
snmpOutGenErrs:	1	snmpOutGetRequests:	0
snmpOutGetNexts:	0	snmpOutSetRequests:	0
snmpOutGetResponses:	150093	snmpOutTraps:	4
snmpSilentDrops:	0	snmpProxyDrops:	0

Table 117 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 117 SNMP Statistics

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 117 SNMP Statistics

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 117 SNMP Statistics

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 GetRequest-PDUs, GetNextRequest-PDUs, GetBulkRequest-PDUs, SetRequest-PDUs, and InformRequest-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 GetRequest-PDUs, GetNextRequest-PDUs, GetBulkRequest-PDUs, SetRequest-PDUs, and InformRequest-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

BLADEOS 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 Jan 13, 2011
Current system time: 18:55:49 Tue Jan 13, 2011
```

Table 118 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.
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

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 119 General Configuration Commands

Command Syntax and Usage

show running-config

Dumps current configuration to a script file. For details, see [page 472](#).

Command mode: All

copy running-config backup-config

Copy the current (running) configuration from switch memory to the backup-config partition. For details, see [page 473](#).

Command mode: Privileged EXEC

copy running-config startup-config

Copy the current (running) configuration from switch memory to the startup-config partition.

Command mode: Privileged EXEC

write memory

Copy the current (running) configuration from switch memory to the active-config partition.

Command mode: Privileged EXEC

Table 119 General Configuration Commands

Command Syntax and Usage

copy running-config {ftp|tftp}

Backs up current configuration to a file on the selected FTP/TFTP server.

Command mode: Privileged EXEC

copy {ftp|tftp} running-config

Restores current configuration from a FTP/TFTP server. For details, see [page 473](#).

Command mode: Privileged EXEC

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.

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 G8264 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 489](#).

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 120 System Configuration Options

Command Syntax and Usage

system date <yyyy> <mm> <dd>

Prompts the user for the system date. The date retains its value when the switch is reset.

Command mode: Global configuration

system time <hh>:<mm>:<ss>

Configures the system time using a 24-hour clock format. The time retains its value when the switch is reset.

Command mode: Global configuration

system timezone

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 Savings Time, etc.

Command mode: Global configuration

[no] **system daylight**

Disables or enables daylight savings 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.

Command mode: Global configuration

system idle <1-60>

Sets the idle timeout for CLI sessions, from 1 to 60 minutes. The default is 10 minutes.

Command mode: Global configuration

system notice <maximum 1024 character multi-line login notice> <'.' to end>

Displays login notice immediately before the “Enter password:” prompt. This notice can contain up to 1024 characters and new lines.

Command mode: Global configuration

Table 120 System Configuration Options

Command Syntax and Usage

[no] banner <1-80 characters>

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 `show sys-info` command.

Command mode: Global configuration

[no] hostname <character string>

Enables or disables displaying of the host name (system administrator's name) in the Command Line Interface (CLI).

Command mode: Global configuration

[no] system bootp

Enables or disables the use of BOOTP. If you enable BOOTP, the switch will query its BOOTP server for all of the switch IP parameters. The default setting is enabled.

Command mode: Global configuration

[no] system dhcp

Enables or disables Dynamic Host Control Protocol for setting the IP address on interface 1. When enabled, the IP address obtained from the DHCP server overrides the static IP address. The default setting is enabled.

Command mode: Global configuration

[no] system reset-control

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.

Command mode: Global configuration

[no] system packet-logging

Enables or disables logging of packets that come to the CPU. The default setting is enabled.

Command mode: Global configuration

system usb-eject

Allows you to safely remove a USB drive from the USB port, without corrupting files on the drive.

Command mode: Global configuration

Table 120 System Configuration Options

Command Syntax and Usage

[no] system service-led

Enables (on) or disables (off) the Service Required LED on the front panel of the switch unit.

Command mode: Global configuration

show system

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 121 Error Disable Configuration Options

Command Syntax and Usage

errdisable timeout <30 - 86400>

Configures the error-recovery timeout, in seconds. After the timer expires, the switch attempts to re-enable the port. The default value is 300.

Note: When you change the timeout value, all current error-recovery timers are reset.

Command mode: Global configuration

errdisable recovery

Globally enables automatic error-recovery for error-disabled ports. The default setting is disabled.

Note: Each port must have error-recovery enabled to participate in automatic error recovery.

Command mode: Global configuration

Table 121 Error Disable Configuration Options

Command Syntax and Usage

no errdisable recovery

Globally disables error-recovery for error-disabled ports.

Command mode: Global configuration

show errdisable

Displays the current system Error Disable configuration.

Command mode: All

Link Flap Dampening Configuration

The Link Flap Dampening feature allows the switch to automatically disable a port if too many link flaps (link up/link down) are detected on the port during a specified time interval. 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.

Table 122 Link Flap Dampening Configuration Options

Command Syntax and Usage

errdisable link-flap max-flaps <1-100>

Configures the maximum number of link flaps allowed in the configured time period. The default value is 5.

errdisable link-flap time <5-500>

Configures the time period, in seconds. The default value is 30 seconds.

errdisable link-flap enable

Enables Link Flap Dampening.

no errdisable link-flap enable

Disables Link Flap Dampening.

show errdisable link-flap

Displays the current Link Flap Dampening parameters.

System Host Log Configuration

Table 123 Host Log Configuration Options

Command Syntax and Usage

[no] logging host <1-2> **address** <IP address>

Sets the IP 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 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 `console` ensures the switch is not affected by syslog messages. It is enabled by default.

Command mode: Global configuration

[no] logging log [<feature>]

Displays a list of features for which syslog messages can be generated. You can choose to enable/disable specific features (such as `vllans`, `stg`, or `ssh`), or enable/disable syslog on all available features.

Command mode: Global configuration

show logging

Displays the current syslog settings.

Command mode: All

SSH Server Configuration

For the RackSwitch G8264, these commands enable Secure Shell access from any SSH client.

Table 124 SSH Server Configuration Options

Command Syntax and Usage

ssh interval <0-24>

Set the interval, in hours, for auto-generation of the RSA server key.

Command mode: Global configuration

ssh scp-password

Set the administration password for SCP access.

Command mode: Global configuration

ssh generate-host-key

Generate the RSA host key.

Command mode: Global configuration

ssh generate-server-key

Generate the RSA server key.

Command mode: Global configuration

ssh port <TCP port number>

Sets the SSH server port number.

Command mode: Global configuration

[no] **ssh version1 enable**

Enables or disables support for SSH version 1.

Command mode: Global configuration

ssh scp-enable

Enables the SCP apply and save.

Command mode: Global configuration

no ssh scp-enable

Disables the SCP apply and save.

Command mode: Global configuration

Table 124 SSH Server Configuration Options

Command Syntax and Usage

ssh enable

Enables the SSH server.

Command mode: Global configuration

no ssh enable

Disables the SSH server.

Command mode: Global configuration

show ssh

Displays the current SSH server configuration.

Command mode: All

RADIUS Server Configuration

Table 125 RADIUS Server Configuration Options

Command Syntax and Usage

[no] radius-server primary-host <IP address>

Sets the primary RADIUS server address.

Command mode: Global configuration

[no] radius-server secondary-host <IP address>

Sets the secondary RADIUS server address.

Command mode: Global configuration

radius-server primary-host <IP address> key <1-32 characters>

This is the primary shared secret between the switch and the RADIUS server(s).

Command mode: Global configuration

radius-server secondary-host <IP address> key <1-32 characters>

This is the secondary shared secret between the switch and the RADIUS server(s).

Command mode: Global configuration

Table 125 RADIUS Server Configuration Options

Command Syntax and Usage

[default] radius-server port <UDP port number>

Enter the number of the UDP port to be configured, between 1500 - 3000. The default is 1645.

Command mode: Global configuration

radius-server retransmit <1-3>

Sets the number of failed authentication requests before switching to a different RADIUS server. The default is 3 requests.

Command mode: Global configuration

radius-server timeout <1-10>

Sets the amount of time, in seconds, before a RADIUS server authentication attempt is considered to have failed. The default is 3 seconds.

Command mode: Global configuration

[no] radius-server backdoor

Enables or disables the RADIUS backdoor for Telnet/SSH/HTTP/HTTPS.
The default value is `disabled`.

To obtain the RADIUS backdoor password for your switch, contact your Service and Support line.

Command mode: Global configuration

[no] radius-server secure-backdoor

Enables or disables the RADIUS back door using secure password for telnet/SSH/HTTP/HTTPS. This command does not apply when backdoor (`telnet`) is enabled.

Command mode: Global configuration

radius-server enable

Enables the RADIUS server.

Command mode: Global configuration

Table 125 RADIUS Server Configuration Options

Command Syntax and Usage

no radius-server enable

Disables the RADIUS server.

Command mode: Global configuration

show radius-server

Displays the current RADIUS server parameters.

Command mode: All

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 126 TACACS+ Server Configuration Options

Command Syntax and Usage

[no] tacacs-server primary-host <IP address>

Defines the primary TACACS+ server address.

Command mode: Global configuration

[no] tacacs-server secondary-host <IP address>

Defines the secondary TACACS+ server address.

Command mode: Global configuration

[no] tacacs-server 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-server 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

Table 126 TACACS+ Server Configuration Options

Command Syntax and Usage

[no] tacacs-server primary-host [data-port | mgt-port]

Defines the primary interface port to use to send TACACS+ server requests.

Select the port to use for data transfer.

Command mode: Global configuration

[no] tacacs-server secondary-host [data-port | mgt-port]

Defines the secondary interface port to use to send TACACS+ server requests.

Select the port to use for data transfer.

Command mode: Global configuration

[no] tacacs-server chpassp <1-32 characters>

Defines the password for the primary TACACS+ server.

Command mode: Global configuration

[no] tacacs-server chpasss <1-32 characters>

Defines the password for the secondary TACACS+ server.

Command mode: Global configuration

[default] tacacs-server 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-server 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

tacacs-server attempts <1-10>

Sets the number of failed login attempts before disconnecting the user. The default is 2 attempts.

Command mode: Global configuration

Table 126 TACACS+ Server Configuration Options

Command Syntax and Usage

tacacs-server timeout <4-15>

Sets the amount of time, in seconds, before a TACACS+ server authentication attempt is considered to have failed. The default is 5 seconds.

Command mode: Global configuration

[no] tacacs-server user-mapping {<0-15> user|oper|admin}

Maps a TACACS+ authorization level to a switch user level. Enter a TACACS+ authorization level (0-15), followed by the corresponding switch user level.

Command mode: Global configuration

[no] tacacs-server backdoor

Enables or disables the TACACS+ back door for Telnet, SSH/SCP, or HTTP/HTTPS.

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.

The default setting is `disabled`.

To obtain the TACACS+ backdoor password for your G8264, contact your Service and Support line.

Command mode: Global configuration

[no] tacacs-server secure-backdoor

Enables or disables TACACS+ secure back door access through Telnet, SSH/SCP, or HTTP/HTTPS only when the TACACS+ servers are not responding.

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.

The default is `disabled`.

Command mode: Global configuration

[no] tacacs-server privilege-mapping

Enables or disables TACACS+ privilege-level mapping.

The default value is `disabled`.

Command mode: Global configuration

Table 126 TACACS+ Server Configuration Options

Command Syntax and Usage

[no] tacacs-server command-authorization

Enables or disables TACACS+ command authorization.

Command mode: Global configuration

[no] tacacs-server command-logging

Enables or disables TACACS+ command logging.

Command mode: Global configuration

[no] tacacs-server directed-request

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.

This command allows the following options:

- Restricted: Only the username is sent to the specified TACACS+ server.
- No-truncate: The entire login string is sent to the TACACS+ server.

Command mode: Global configuration

[no] tacacs-server accounting-enable

Enables or disables TACACS+ accounting.

Command mode: Global configuration

[no] tacacs-server enable

Enables or disables the TACACS+ server. By default, the server is disabled.

Command mode: Global configuration

show tacacs-server

Displays current TACACS+ configuration parameters.

Command mode: All

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 127 LDAP Server Configuration Options

Command Syntax and Usage

[no] ldap-server primary-host <IP address> [**data-port** | **mgt-port**]

Sets the primary LDAP server address.

Command mode: Global configuration

[no] ldap-server secondary-host <IP address> [**data-port** | **mgt-port**]

Sets the secondary LDAP server address.

Command mode: Global configuration

[default] ldap-server port <UDP port number>

Enter the number of the UDP port to be configured, between 1 - 65000. The default is 389.

Command mode: Global configuration

ldap-server retransmit <1-3>

Sets the number of failed authentication requests before switching to a different LDAP server. The default is 3 requests.

Command mode: Global configuration

ldap-server timeout <4-15>

Sets the amount of time, in seconds, before a LDAP server authentication attempt is considered to have failed. The default is 5 seconds.

Command mode: Global configuration

ldap-server domain [<1-128 characters> | **none**]

Sets the domain name for the LDAP server. Enter the full path for your organization. For example:

```
ou=people,dc=mydomain,dc=com
```

Command mode: Global configuration

Table 127 LDAP Server Configuration Options

Command Syntax and Usage

[no] ldap-server backdoor

Enables or disables the LDAP back door for Telnet, SSH/SCP, or HTTP/HTTPS. The default setting is disabled.

To obtain the LDAP back door password for your G8264, contact your Service and Support line.

Command mode: Global configuration

ldap-server enable

Enables the LDAP server.

Command mode: Global configuration

no ldap-server enable

Disables the LDAP server.

Command mode: Global configuration

show ldap-server

Displays the current LDAP server parameters.

Command mode: All

NTP Client Configuration

These commands allow you to synchronize the switch clock to a Network Time Protocol (NTP) server. By default, this option is disabled.

Table 128 NTP Client Configuration Options

Command Syntax and Usage

[no] ntp primary-server {<host name> | <IP address>}

Prompts for the hostname or IP addresses of the primary NTP server to which you want to synchronize the switch clock.

Command mode: Global configuration

[no] ntp secondary-server {<host name> | <IP address>}

Prompts for the hostname or IP addresses of the secondary NTP server to which you want to synchronize the switch clock.

Command mode: Global configuration

ntp interval <5-44640>

Specifies the interval, that is, how often, in minutes, to re-synchronize the switch clock with the NTP server.

Command mode: Global configuration

ntp enable

Enables the NTP synchronization service.

Command mode: Global configuration

no ntp enable

Disables the NTP synchronization service.

Command mode: Global configuration

show ntp

Displays the current NTP service settings.

Command mode: All

System SNMP Configuration

BLADEOS 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 129 System SNMP Options

Command Syntax and Usage

snmp-server name *<1-64 characters>*

Configures the name for the system. The name can have a maximum of 64 characters.

Command mode: Global configuration

snmp-server location *<1-64 characters>*

Configures the name of the system location. The location can have a maximum of 64 characters.

Command mode: Global configuration

snmp-server contact *<1-64 characters>*

Configures the name of the system contact. The contact can have a maximum of 64 characters.

Command mode: Global configuration

Table 129 System SNMP Options

Command Syntax and Usage

snmp-server read-community <1-32 characters>

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 *public*.

Command mode: Global configuration

snmp-server write-community <1-32 characters>

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 *private*.

Command mode: Global configuration

snmp-server trap-src-if <interface number>

Configures the source interface for SNMP traps. The default value is interface 1.

To send traps through the management port A, specify interface 127.

To send traps through management port B, specify interface 128.

Command mode: Global configuration

snmp-server host <trap host IP address> <trap host community string>

Adds a trap host server.

Command mode: Global configuration

no snmp-server host <trap host IP address>

Removes the trap host server.

Command mode: Global configuration

snmp-server timeout <1-30>

Sets the timeout value for the SNMP state machine, in minutes.

Command mode: Global configuration

[no] snmp-server authentication-trap

Enables or disables the use of the system authentication trap facility. The default setting is disabled.

Command mode: Global configuration

Table 129 System SNMP Options

Command Syntax and Usage

[no] snmp-server link-trap

Enables or disables the sending of SNMP link up and link down traps. The default setting is enabled.

Command mode: Global configuration

show snmp-server

Displays the current SNMP configuration.

Command mode: All

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 130 SNMPv3 Configuration Options

Command Syntax and Usage

snmp-server user <I-16>

This command allows you to create a user security model (USM) entry for an authorized user. You can also configure this entry through SNMP.

Command mode: Global configuration

To view command options, see [page 244](#).

snmp-server view <I-128>

This command allows you to create different MIB views.

Command mode: Global configuration

To view command options, see [page 245](#).

snmp-server access <I-32>

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.

Command mode: Global configuration

To view command options, see [page 246](#).

Table 130 SNMPv3 Configuration Options

snmp-server group <1-16>

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.

Command mode: Global configuration

To view command options, see [page 248](#).

snmp-server community <1-16>

The community table contains objects for mapping community strings and version-independent SNMP message parameters.

Command mode: Global configuration

To view command options, see [page 249](#).

snmp-server target-address <1-16>

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.

Command mode: Global configuration

To view command options, see [page 250](#).

snmp-server target-parameters <1-16>

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.

Command mode: Global configuration

To view command options, see [page 251](#).

snmp-server notify <1-16>

A notification application typically monitors a system for particular events or conditions, and generates Notification-Class messages based on these events or conditions.

Command mode: Global configuration

To view command options, see [page 253](#).

Table 130 SNMPv3 Configuration Options

```
snmp-server version {v1v2v3|v3only}
```

This command allows you to enable or disable the access to SNMP versions 1, 2 or 3. This command is enabled by default.

Command mode: Global configuration

```
show snmp-server v3
```

Displays the current SNMPv3 configuration.

Command mode: All

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 131 User Security Model Configuration Options

Command Syntax and Usage

```
snmp-server user <1-16> name <1-32 characters>
```

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.

Command mode: Global configuration

```
snmp-server user <1-16> authentication-protocol {md5|sha|none}  
authentication-password <password value>
```

This command allows you to configure the authentication protocol and password.

The authentication protocol can be HMAC-MD5-96 or HMAC-SHA-96, or none. The default algorithm is none.

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.

Command mode: Global configuration

Table 131 User Security Model Configuration Options

Command Syntax and Usage

snmp-server user <1-16> **privacy-protocol** {des|none}
privacy-password <password value>

This command allows you to configure the type of privacy protocol and the privacy password.

The privacy protocol protects messages from disclosure. The options are `des` (CBC-DES Symmetric Encryption Protocol) or `none`. If you specify `des` as the privacy protocol, then make sure that you have selected one of the authentication protocols (MD5 or HMAC-SHA-96). If you select `none` as the authentication protocol, you will get an error message.

You can create or change the privacy password.

Command mode: Global configuration

no snmp-server user <1-16>

Deletes the USM user entries.

Command mode: Global configuration

show snmp-server v3 user <1-16>

Displays the USM user entries.

Command mode: All

SNMPv3 View Configuration

Note that the first five default `vacmViewTreeFamily` entries cannot be removed, and their names cannot be changed.

Table 132 SNMPv3 View Configuration Options

Command Syntax and Usage

snmp-server view <1-128> **name** <1-32 characters>

This command defines the name for a family of view subtrees.

Command mode: Global configuration

snmp-server view <1-128> **tree** <1-64 characters>

This command defines MIB tree, which when combined with the corresponding mask defines a family of view subtrees.

Command mode: Global configuration

Table 132 SNMPv3 View Configuration Options**Command Syntax and Usage**

```
[no] snmp-server view <1-128> mask <1-32 characters>
```

This command defines the bit mask, which in combination with the corresponding tree defines a family of view subtrees.

Command mode: Global configuration

```
snmp-server view <1-128> type {included|excluded}
```

This command indicates whether the corresponding instances of `vacmViewTreeFamilySubtree` and `vacmViewTreeFamilyMask` define a family of view subtrees, which is included in or excluded from the MIB view.

Command mode: Global configuration

```
no snmp-server view <1-128>
```

Deletes the `vacmViewTreeFamily` group entry.

Command mode: Global configuration

```
show snmp-server v3 view <1-128>
```

Displays the current `vacmViewTreeFamily` 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 133 View-based Access Control Model Options**Command Syntax and Usage**

```
snmp-server access <1-32> name <1-32 characters>
```

Defines the name of the group.

Command mode: Global configuration

```
snmp-server access <1-32> security {usm|snmpv1|snmpv2}
```

Allows you to select the security model to be used.

Command mode: Global configuration

Table 133 View-based Access Control Model Options**Command Syntax and Usage**

```
snmp-server access <1-32> level {noAuthNoPriv|authNoPriv|authPriv}
```

Defines the minimum level of security required to gain access rights. The level `noAuthNoPriv` means that the SNMP message will be sent without authentication and without using a privacy protocol. The level `authNoPriv` means that the SNMP message will be sent with authentication but without using a privacy protocol. The `authPriv` means that the SNMP message will be sent both with authentication and using a privacy protocol.

Command mode: Global configuration

```
snmp-server access <1-32> read-view <1-32 characters>
```

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.

Command mode: Global configuration

```
snmp-server access <1-32> write-view <1-32 characters>
```

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.

Command mode: Global configuration

```
snmp-server access <1-32> notify-view <1-32 characters>
```

Defines a notify view name that allows you notify access to the MIB view.

Command mode: Global configuration

```
no snmp-server access <1-32>
```

Deletes the View-based Access Control entry.

Command mode: Global configuration

```
show snmp-server v3 access <1-32>
```

Displays the View-based Access Control configuration.

Command mode: All

SNMPv3 Group Configuration

Table 134 SNMPv3 Group Configuration Options

Command Syntax and Usage

snmp-server group <1-16> **security** {**usm** | **snmpv1** | **snmpv2**}

Defines the security model.

Command mode: Global configuration

snmp-server group <1-16> **user-name** <1-32 characters>

Sets the user name as defined in the following command on [page 244](#):

`snmp-server user <1-16> name <1-32 characters>`

Command mode: Global configuration

snmp-server group <1-16> **group-name** <1-32 characters>

The name for the access group as defined in the following command:

`snmp-server access <1-32> name <1-32 characters>` on [page 244](#).

Command mode: Global configuration

no snmp-server group <1-16>

Deletes the `vacmSecurityToGroup` entry.

Command mode: Global configuration

show snmp-server v3 group <1-16>

Displays the current `vacmSecurityToGroup` configuration.

Command mode: All

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 135 SNMPv3 Community Table Configuration Options

Command Syntax and Usage

snmp-server community <1-16> **index** <1-32 characters>

Allows you to configure the unique index value of a row in this table.

Command string: Global configuration

snmp-server community <1-16> **name** <1-32 characters>

Defines the user name as defined in the following command on [page 244](#):

`snmp-server user <1-16> name <1-32 characters>`

Command string: Global configuration

snmp-server community <1-16> **user-name** <1-32 characters>

Defines a readable string that represents the corresponding value of an SNMP community name in a security model.

Command mode: Global configuration

snmp-server community <1-16> **tag** <1-255 characters>

Allows you to configure a tag. This tag specifies a set of transport endpoints to which a command responder application sends an SNMP trap.

Command mode: Global configuration

no snmp-server community <1-16>

Deletes the community table entry.

Command mode: Global configuration

show snmp-server v3 community <1-16>

Displays the community table configuration.

Command mode: All

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 136 Target Address Table Configuration Options

Command Syntax and Usage

snmp-server target-address <1-16> **address** <IP address>
name <1-32 characters>

Allows you to configure the locally arbitrary, but unique identifier, target address name associated with this entry.

Command mode: Global configuration

snmp-server target-address <1-16> **name** <1-32 characters>
address <transport IP address>

Configures a transport IPv4 or IPv6 address that can be used in the generation of SNMP traps. IPv6 addresses are not displayed in the configuration, but they do receive traps.

Command mode: Global configuration

snmp-server target-address <1-16> **port** <port alias or number>

Allows you to configure a transport address port that can be used in the generation of SNMP traps.

Command mode: Global configuration

snmp-server target-address <1-16> **taglist** <1-255 characters>

Allows you to configure a list of tags that are used to select target addresses for a particular operation.

Command mode: Global configuration

snmp-server target-address <1-16> **parameters-name** <1-32 characters>

Defines the name as defined in the following command on [page 251](#):

snmp-server target-parameters <1-16> **name** <1-32 characters>

Command mode: Global configuration

Table 136 Target Address Table Configuration Options

Command Syntax and Usage

no snmp-server target-address <1-16>

Deletes the Target Address Table entry.

Command mode: Global configuration

show snmp-server v3 target-address <1-16>

Displays the current Target Address Table configuration.

Command mode: All

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 137 Target Parameters Table Configuration Options

Command Syntax and Usage

snmp-server target-parameters <1-16> **name** <1-32 characters>

Allows you to configure the locally arbitrary, but unique, identifier that is associated with this entry.

Command mode: Global configuration

snmp-server target-parameters <1-16> **message**
{snmpv1 | snmpv2c | snmpv3}

Allows you to configure the message processing model that is used to generate SNMP messages.

Command mode: Global configuration

snmp-server target-parameters <1-16> **security** {usm | snmpv1 | snmpv2}

Allows you to select the security model to be used when generating the SNMP messages.

Command mode: Global configuration

Table 137 Target Parameters Table Configuration Options

Command Syntax and Usage

snmp-server target-parameters <1-16> **user-name** <1-32 characters>

Defines the name that identifies the user in the USM table ([page 244](#)) on whose behalf the SNMP messages are generated using this entry.

Command mode: Global configuration

snmp-server target-parameters <1-16> **level**
{noAuthNoPriv|authNoPriv|authPriv}

Allows you to select the level of security to be used when generating the SNMP messages using this entry. The level noAuthNoPriv means that the SNMP message will be sent without authentication and without using a privacy protocol. The level authNoPriv means that the SNMP message will be sent with authentication but without using a privacy protocol. The authPriv means that the SNMP message will be sent both with authentication and using a privacy protocol.

Command mode: Global configuration

no snmp-server target-parameters <1-16>

Deletes the targetParamsTable entry.

Command mode: Global configuration

show snmp-server v3 target-parameters <1-16>

Displays the current targetParamsTable configuration.

Command mode: All

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 138 Notify Table Options

Command Syntax and Usage

snmp-server notify *<1-16>* **name** *<1-32 characters>*

Defines a locally arbitrary, but unique, identifier associated with this SNMP notify entry.

Command mode: Global configuration

snmp-server notify *<1-16>* **tag** *<1-255 characters>*

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 `snmpTargetAddrTable`, that matches the value of this tag, is selected.

Command mode: Global configuration

no snmp-server notify *<1-16>*

Deletes the notify table entry.

Command mode: Global configuration

show snmp-server v3 notify *<1-16>*

Displays the current notify table configuration.

Command mode: All

System Access Configuration

Table 139 System Access Configuration Options

Command Syntax and Usage

access user user-password

Sets the user (`user`) password. The user has no direct responsibility for switch management. The user view switch status information and statistics, but cannot make any configuration changes.

This command will prompt for required information: current admin password, new password (up to 128 characters) and confirmation of the new password.

Note: To disable the user account, set the password to null (no password).

Command Mode: Global configuration

access user operator-password

Sets the operator (`oper`) password. The operator manages all functions of the switch. The operator can view all switch information and statistics and can reset ports.

This command will prompt for required information: current admin password, new password (up to 128 characters) and confirmation of the new password.

Note: To disable the operator account, set the password to null (no password). The default setting is disabled (no password).

Command Mode: Global configuration

access user administrator-password

Sets the administrator (`admin`) password. The administrator has complete access to all menus, information, and configuration commands on the G8264, including the ability to change both the user and administrator passwords.

This command will prompt for required information: current admin password, new password (up to 128 characters) and confirmation of the new password.

Access includes “oper” functions.

Note: You cannot disable the administrator password.

Command Mode: Global configuration

Table 139 System Access Configuration Options

Command Syntax and Usage

[no] access http enable

Enables or disables HTTP (Web) access to the Browser-Based Interface. It is enabled by default.

Command mode: Global configuration

[default] access http port [*<port alias or number>*]

Sets the switch port used for serving switch Web content. The default is HTTP port 80.

Command mode: Global configuration

[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

Table 139 System Access Configuration Options

Command Syntax and Usage

[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 140 Management Network Configuration Options

Command Syntax and Usage

access management-network *<mgmt network IPv4 or IPv6 address>*
<mgmt network mask or prefix length>

Adds a defined network through which switch access is allowed through Telnet, SNMP, RIP, or the BLADEOS 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.

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.

Command mode: Global configuration

no access management-network *<mgmt network IPv4 or IPv6 address>*
<mgmt network mask or prefix length>

Removes a defined network, which consists of a management network address and a management network mask address.

Command mode: Global configuration

Table 140 Management Network Configuration Options

Command Syntax and Usage

show access management-network

Displays the current management network configuration.

Command mode: All except User EXEC

clear access management-network

Removes all defined management networks.

Command mode: Global configuration

NETCONF Configuration

This menu allows you to configure support for Network Configuration Protocol (NETCONF), which provides mechanisms to install, manipulate, and delete the configuration of network devices. NETCONF is described in RFC 4741.

Table 141 NETCONF Configuration Options

Command Syntax and Usage

[no] access netconf enable

Enables or disables NETCONF access to the switch.

Command mode: Global configuration

access netconf timeout <30-3600>

Configures the timeout value for NETCONF sessions, in seconds. The default value is 300 seconds.

Command mode: Global configuration

show access

Displays the current configuration.

Command mode: All

NETCONF over SSH Configuration

This menu allows you to enable NETCONF access over Secure Shell (SSH). NETCONF over SSH is described in RFC 4742.

Table 142 NETCONF over SSH Configuration Options

Command Syntax and Usage

[no] access netconf ssh enable

Enables or disables NETCONF access over SSH.

Command mode: Global configuration

access netconf ssh port *<TCP port number>*

Configures the TCP port used for NETCONF. The default port number is 830.

Command mode: Global configuration

User Access Control Configuration

The following table describes user-access control commands.

Passwords can be a maximum of 128 characters.

Table 143 User Access Control Configuration Options

Command Syntax and Usage

access user eject *<user name>*

Ejects the specified user from the G8264.

Command mode: Global configuration

access user user-password

Sets the user (*user*) password. This command will prompt for required information: current admin password, new password (up to 128 characters) and confirmation of the new password.

Command mode: Global configuration

access user operator-password

Sets the operator (*oper*) password. This command will prompt for required information: current admin password, new password (up to 128 characters) and confirmation of the new password.

Command mode: Global configuration

Table 143 User Access Control Configuration Options

Command Syntax and Usage

access user administrator-password

Sets the administrator (`admin`) password. This command will prompt for required information: current admin password, new password (up to 128 characters) and confirmation of the new password.

Access includes “oper” functions.

Command mode: Global configuration

show access user

Displays the current user status.

Command mode: All except User EXEC

System User ID Configuration**Table 144** User ID Configuration Options

Command Syntax and Usage

access user <1-10> level {user | operator | administrator}

Sets the Class-of-Service to define the user’s authority level. BLADEOS defines these levels as: User, Operator, and Administrator, with User being the most restricted level.

Command mode: Global configuration

access user <1-10> name <1-8 characters>

Defines the user name of maximum eight characters.

Command mode: Global configuration

access user <1-10> password

Sets the user (`user`) password. This command will prompt for required information: current admin password, new password (up to 128 characters) and confirmation of the new password.

Command mode: Global configuration

access user <1-10> enable

Enables the user ID.

Command mode: Global configuration

Table 144 User ID Configuration Options

Command Syntax and Usage

no access user <1-10> enable

Disables the user ID.

Command mode: Global configuration

no access user <1-10>

Deletes the user ID.

Command mode: Global configuration

show access user

Displays the current user ID configuration.

Command mode: All except User EXEC

Strong Password Configuration**Table 145** Strong Password Configuration Options

Command Syntax and Usage

access user strong-password enable

Enables Strong Password requirement.

Command mode: Global configuration

no access user strong-password enable

Disables Strong Password requirement.

Command mode: Global configuration

access user strong-password expiry <1-365>

Configures the number of days allowed before the password must be changed. The default value is 60 days.

Command mode: Global configuration

access user strong-password warning <1-365>

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

Table 145 Strong Password Configuration Options

Command Syntax and Usage

access user strong-password faillog <1-255>

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

show access user strong-password

Displays the current Strong Password configuration.

Command mode: All except User EXEC

HTTPS Access Configuration

Table 146 HTTPS Access Configuration Options

Command Syntax and Usage

[no] access https enable

Enables or disables BBI access (Web access) using HTTPS.

Command mode: Global configuration

[default] access https port [<TCP port number>]

Defines the HTTPS Web server port number. The default port is 443.

Command mode: Global configuration

Table 146 HTTPS Access Configuration Options

Command Syntax and Usage

access https generate-certificate

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:

- Country Name (2 letter code): CA
- State or Province Name (full name): Ontario
- Locality Name (for example, city): Ottawa
- Organization Name (for example, company): Blade
- Organizational Unit Name (for example, section): Operations
- Common Name (for example, user's name): Mr Smith
- Email (for example, email address): info@bladenetwork.net

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.

Command mode: Global configuration

access https save-certificate

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.

Command mode: Global configuration

show access

Displays the current SSL Web Access configuration.

Command mode: All except User EXEC

Custom Daylight Savings Time Configuration

Use these commands to configure custom Daylight Savings 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 147 Custom DST Options

Command Syntax and Usage

system custom-dst start-rule <WDDMMhh>

Configures the start date for custom DST, as follows:

WDDMMhh

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)

Note: Week 5 is always considered to be the last week of the month.

Command mode: Global configuration

system custom-dst end-rule <WDDMMhh>

Configures the end date for custom DST, as follows:

WDDMMhh

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)

Note: Week 5 is always considered to be the last week of the month.

Command mode: Global configuration

system custom-dst enable

Enables the Custom Daylight Savings Time settings.

Command mode: Global configuration

Table 147 Custom DST Options

Command Syntax and Usage

no system custom-dst enable

Disables the Custom Daylight Savings Time settings.

Command mode: Global configuration

show custom-dst

Displays the current Custom DST configuration.

Command mode: All except User EXEC

sFlow Configuration

BLADEOS 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 148 sFlow Configuration Options

Command Syntax and Usage

sflow enable

Enables the sFlow agent.

Command mode: Global configuration

no sflow enable

Disables the sFlow agent.

Command mode: Global configuration

sflow server <IP address> [data-port | mgt-port]

Defines the sFlow server address and interface port.

Command mode: Global configuration

sflow port <1-65535>

Configures the UDP port for the sFlow server. The default value is 6343.

Command mode: Global configuration

show sflow

Displays sFlow configuration parameters.

Command mode: All

sFlow Port Configuration

Use the following commands to configure the sFlow port on the switch.

Table 149 sFlow Port Configuration Options

Command Syntax and Usage

[no] sflow polling <5-60>

Configures the sFlow polling interval, in seconds. The default setting is disabled.

Command mode: Interface port

[no] sflow sampling <256-65536>

Configures the sFlow sampling rate, in packets per sample. The default setting is disabled.

Command mode: Interface port

Server Port Configuration

Use these commands to define a list of server ports. Ports that are not configured as server ports are considered to be uplink ports. VMready learns Virtual Machine information only from server ports.

Table 150 Server Port Configuration Options

Command Syntax and Usage

system server-ports port <port alias or number>

Adds one or more port physical ports to the list of server ports.

no system server-ports port <port alias or number>

Removes one of more ports from the list of server ports.

show system server-ports

Displays the current server port configuration.

Port Configuration

Use the Port Configuration commands to configure settings for interface ports.

Table 151 Port Configuration Options

Command Syntax and Usage

interface port <port alias or number>

Enter Interface port mode.

Command mode: Global configuration

interface portchannel <trunk number> | **lACP** <1-65535>

Enter Interface portchannel mode. These commands allow you to configure port parameters for all port members in the selected trunk group (portchannel).

Command mode: Global configuration

dot1p <0-7>

Configures the port's 802.1p priority level.

Command mode: Interface port/Interface portchannel

pvid <VLAN number>

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.

Command mode: Interface port/Interface portchannel

name <1-64 characters>

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.

Command mode: Interface port/Interface portchannel

[no] bpdu-guard

Enables or disables BPDU guard, to avoid Spanning-Tree loops on ports with Port Fast Forwarding enabled, or ports configured as edge ports.

Command mode: Interface port/Interface portchannel

[no] dscp-marking

Enables or disables DSCP re-marking on a port.

Command mode: Interface port/Interface portchannel

Table 151 Port Configuration Options

Command Syntax and Usage

[no] tagging

Disables or enables VLAN tagging for this port. The default setting is disabled.

Command mode: Interface port/Interface portchannel

[no] tag-pvid

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.

Command mode: Interface port/Interface portchannel

[no] flood-blocking

Enables or disables port Flood Blocking. When enabled, unicast and multicast packets with unknown destination MAC addresses are blocked from the port.

Command mode: Interface port/Interface portchannel

[no] mac-address-table mac-notification

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.

Command mode: Interface port/Interface portchannel

[no] learning

Enables or disables FDB learning on the port.

Command mode: Interface port/Interface portchannel

[no] broadcast-threshold <0-2097151>

Limits the number of broadcast packets per second to the specified value. If disabled, the port forwards all broadcast packets.

Command mode: Interface port/Interface portchannel

[no] multicast-threshold <0-2097151>

Limits the number of multicast packets per second to the specified value. If disabled, the port forwards all multicast packets.

Command mode: Interface port/Interface portchannel

Table 151 Port Configuration Options

Command Syntax and Usage

[no] dest-lookup-threshold <0-2097151>

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/Interface portchannel

[no] ip dhcp snooping trust

Configures this port as a trusted port for DHCP packets from the server.

Command mode: Interface port

ip dhcp snooping limit rate <1-2048>

Configures the maximum number of DHCP packets allowed per second.

Command mode: Interface port

no shutdown

Enables the port.

Command mode: Interface port/Interface portchannel

shutdown

Disables the port. (To temporarily disable a port without changing its configuration attributes, refer to [“Temporarily Disabling a Port” on page 272.](#))

Command mode: Interface port/Interface portchannel

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 152 Port Error Disable Options

Command Syntax and Usage

errdisable recovery

Enables automatic error-recovery for the port. The default setting is enabled.

Note: Error-recovery must be enabled globally before port-level commands become active.

Command mode: Interface port

no errdisable recovery

Enables automatic error-recovery for the port.

Command mode: Interface port

show interface port <port alias or number> errdisable

Displays current port Error Disable parameters.

Command mode: All

Port Link Flap Dampening Configuration

Table 153 Port Link Flap Dampening Configuration Options

Command Syntax and Usage

errdisable link-flap enable

Enables Link Flap Dampening on the port. For more information, see [“Link Flap Dampening Configuration”](#) on page 226.

Command mode: Interface port

no errdisable link-flap enable

Disables Link Flap Dampening on the port.

Command mode: Interface port

show interface port errdisable <port alias or number> link-flap

Displays the current Link Flap Dampening parameters for the port.

Command mode: All

Port Link Configuration

Use these commands to set flow control for the port link.

Table 154 Port Link Configuration Options

Command Syntax and Usage

duplex {full|half|any}

Sets the operating mode. The choices include:

- “Any,” for auto negotiation (default)
- Half-duplex
- Full-duplex

Note: Data ports are fixed at full duplex.

Command mode: Interface port/Interface portchannel

[no] flowcontrol {receive|send|both}

Sets the flow control. The choices include:

- Receive flow control
- Transmit flow control
- Both receive and transmit flow control
- No flow control (default)

Command mode: Interface port/Interface portchannel

[no] auto

Turns auto-negotiation on or off.

Note: Data ports are fixed at 10000 Mbps, and cannot be set to auto-negotiate, unless a 1 Gb SFP transceiver is used.

Command mode: Interface port/Interface portchannel

show interface port <port alias or number>

Displays current port parameters.

Command mode: All

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 RackSwitch G8264 is reset. See the “[Operations Commands](#)” on page 475 for other operations-level commands.

UniDirectional Link Detection Configuration

UDLD commands are described in the following table.

Table 155 Port UDLD Configuration Options

Command Syntax and Usage

[no] udld

Enables or disables UDLD on the port.

Command mode: Interface port

[no] udld aggressive

Configures the UDLD mode for the selected port, as follows:

- 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.

Command mode: Interface port

show udld

Displays current port UDLD parameters.

Command mode: All

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 156 Port OAM Configuration Options

Command Syntax and Usage

oam {**active**|**passive**}

Configures the OAM discovery mode, as follows:

- Active: This port link initiates OAM discovery.
- Passive: This port allows its peer link to initiate OAM discovery.

If OAM determines that the port is in an anomalous condition, the port is disabled.

Command mode: Interface port/

no oam {**active**|**passive**}

Disables OAM discovery on the port.

Command mode: Interface port

show oam

Displays current port OAM parameters.

Command mode: All

Port ACL Configuration

Table 157 ACL/QoS Configuration Options

Command Syntax and Usage

access-control list <ACL number>

Adds the specified ACL to the port. You can add multiple ACLs to a port, but the total number of precedence levels allowed is two.

Command mode: Interface port/Interface portchannel

no access-control list <ACL number>

Removes the specified ACL list from the port.

Command mode: Interface port/Interface portchannel

access-control list6 <ACL number>

Adds the specified IPv6 ACL to the port. You can add multiple ACLs to a port, but the total number of precedence levels allowed is two.

Command mode: Interface port/Interface portchannel

Table 157 ACL/QoS Configuration Options

Command Syntax and Usage

no access-control list6 *<ACL number>*

Removes the specified IPv6 ACL list from the port.

Command mode: Interface port/Interface portchannel

access-control group *<ACL group number>*

Adds the specified ACL group to the port. You can add multiple ACL groups to a port, but the total number of precedence levels allowed is two.

Command mode: Interface port/Interface portchannel

no access-control group *<ACL group number>*

Removes the specified ACL group from the port.

Command mode: Interface port/Interface portchannel

show interface port *<port alias or number>* **access-control**

Displays current ACL QoS parameters.

Command mode: All

Port Spanning Tree Configuration

Table 158 Port STP Options

Command Syntax and Usage

[no] spanning-tree edge

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).

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.

Command mode: Interface port/Interface portchannel

[no] spanning-tree link-type p2p|shared

Defines the type of link connected to the port, as follows:

- 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).

The default link type is `auto`.

Command mode: Interface port/Interface portchannel

[no] spanning-tree pvst-protection

Enables or disables PVST Protection on the selected port. If the port receives any PVST+/PVRST+ BPDUs, it is error disabled. The default setting for this feature is disabled (no protection).

Command mode: Interface port/Interface portchannel

show interface port {<port alias or number>}

Displays current port configuration parameters.

Command mode: All

Port Spanning Tree Guard Configuration

Table 159 Port STP Guard Options

Command Syntax and Usage

spanning-tree guard loop

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.

Command mode: Interface port/Interface portchannel

spanning-tree guard root

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).

Command mode: Interface port/Interface portchannel

spanning-tree guard none

Disables STP loop guard and root guard.

Command mode: Interface port/Interface portchannel

no spanning-tree guard

Sets the Spanning Tree guard parameters to their default values.

Command mode: Interface port/Interface portchannel

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 283](#).

Table 160 Port WRED Options

Command Syntax and Usage

[no] random-detect ecn enable

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.

Note: ECN functions only on TCP traffic.

Command mode: Interface port

random-detect enable

Turns on Random Detection and avoidance.

Command mode: Interface port

no random-detect enable

Turns off Random Detection and avoidance.

Command mode: Interface port

show interface port <port alias or number> random-detect

Displays current Random Detection and avoidance parameters.

Command mode: All

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 161 Port WRED Transmit Queue Options

Command Syntax and Usage

[no] random-detect transmit-queue <0-7>

tcp <min. threshold (1-100)> <max. threshold (1-100)> <drop rate (1-100)>

Configures the WRED thresholds for TCP traffic. Use the **no** form to clear the WRED threshold value.

Command mode: Interface port

[no] random-detect transmit-queue <0-7>

non-tcp <min. threshold (1-100)> <max. threshold (1-100)> <drop rate (1-100)>

Configures the WRED thresholds for non-TCP traffic. Use the **no** form to clear the WRED threshold value.

Command mode: Interface port

random-detect transmit-queue <0-7> enable

Sets the WRED transmit queue configuration to **on**.

Command mode: Interface port

no random-detect transmit-queue <0-7> enable

Sets the WRED transmit queue configuration to **off**.

Command mode: Interface port

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 G8264 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 162 802.1p Configuration Options

Command Syntax and Usage

qos transmit-queue mapping <priority (0-7)> <COSq number>

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.

Command mode: Global configuration

qos transmit-queue weight-cos <COSq number> <weight (0-15)>

Configures the weight of the selected Class of Service queue (COSq). Enter the queue number (0-1), followed by the scheduling weight (0-15).

Command mode: Global configuration

show qos transmit-queue

Displays the current 802.1p parameters.

Command mode: All

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 163 DSCP Configuration Options

Command Syntax and Usage

qos dscp dscp-mapping *<DSCP (0-63)>* *<new DSCP (0-63)>*

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.

Command mode: Global configuration

qos dscp dot1p-mapping *<DSCP (0-63)>* *<priority (0-7)>*

Maps the DiffServ Code point value to an 802.1p priority value. Enter the DSCP value, followed by the corresponding 802.1p value.

Command mode: Global configuration

qos dscp re-marking

Turns on DSCP re-marking globally.

Command mode: Global configuration

no qos dscp re-marking

Turns off DSCP re-marking globally.

Command mode: Global configuration

show qos dscp

Displays the current DSCP parameters.

Command mode: All

Control Plane Protection

These commands allow you to limit the number of selected protocol packets received by the control plane (CP) of the switch. These limits help protect the CP from receiving too many protocol packets in a given time period.

Table 164 Control Plane Protection Options

Command Syntax and Usage

qos protocol-packet-control packet-queue-map *<packet queue number (0-40)>*
<packet type>

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:

- 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)
- rip** (RIP packets)
- system** (system protocols, such as tftp, ftp, telnet, ssh)
- udld** (UDLD packets)
- vlag** (VLAG packets)
- vrrp** (VRRP packets)

Command mode: Global configuration

Table 164 Control Plane Protection Options

Command Syntax and Usage

qos protocol-packet-control rate-limit-packet-queue *<packet queue number (0-40)>* *<1-10000>*

Configures the number of packets per second allowed for each packet queue.

Command mode: Global configuration

no qos protocol-packet-control packet-queue-map *<packet type>*

Clears the selected packet type from its associated packet queue.

Command mode: Global configuration

no qos protocol-packet-control rate-limit-packet-queue *<packet queue number (0-40)>*

Clears the packet rate configured for the selected packet queue.

Command mode: Global configuration

show qos protocol-packet-control information protocol

Displays of mapping of protocol packet types to each packet queue number. The status indicates whether the protocol is running or not running.

Command mode: All

show qos protocol-packet-control information queue

Displays the packet rate configured for each packet queue.

Command mode: All

Weighted Random Early Detection Configuration

Weighted Random Early Detection (WRED) provides congestion avoidance by pre-emptively dropping packets before a queue becomes full. G8264 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 277](#).

Table 165 WRED Configuration Options

Command Syntax and Usage

qos random-detect ecn

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.

Note: ECN functions only on TCP traffic.

Command mode: Global configuration

qos random-detect enable

Turns on Random Detection and avoidance.

Command mode: Global configuration

no qos random-detect enable

Turns off Random Detection and avoidance.

Command mode: Global configuration

show qos random-detect

Displays current Random Detection and avoidance parameters.

Command mode: All

WRED Transmit Queue Configuration

Table 166 WRED Transmit Queue Options

Command Syntax and Usage

[no] qos random detect transmit-queue <0-7>
tcp <min. threshold (1-100)> <max. threshold (1-100)> <drop rate (1-100)>

Configures the WRED thresholds for TCP traffic. Use the **no** form to clear the WRED threshold value.

Command mode: Global configuration

[no] qos random detect transmit-queue <0-7>
non-tcp <min. threshold (1-100)> <max. threshold (1-100)> <drop rate (1-100)>

Configures the WRED thresholds for non-TCP traffic. Use the **no** form to clear the WRED threshold value.

Command mode: Global configuration

qos random detect transmit-queue <0-7> **enable**

Sets the WRED transmit queue configuration to **on**.

Command mode: Global configuration

no qos random detect transmit-queue <0-7> **enable**

Sets the WRED transmit queue configuration to **off**.

Command mode: Global configuration

Access Control Configuration

Use these commands to create Access Control Lists. 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 273.

Table 167 General ACL Configuration Options

Command Syntax and Usage

[no] access-control list <1-256>

Configures an Access Control List. To view command options, see [page 286](#).

Command mode: Global configuration

[no] access-control list6 <1-128>

Configures an Access Control List. To view command options, see [page 296](#).

Command mode: Global configuration

[no] access-control macl <1-256>

Configures an Access Control List. To view command options, see [page 286](#).

Command mode: Global configuration

[no] access-control group <1-256>

Configures an ACL Group. To view command options, see [page 300](#).

Command mode: Global configuration

[no] access-control vmap <1-256>

Configures an ACL VLAN map. To view command options, see [page 306](#).

Command mode: Global configuration

show access-control

Displays the current ACL parameters.

Command mode: All

ACL IPv4 Configuration

These commands allow you to define filtering criteria for each Access Control List (ACL).

Table 168 ACL Configuration Options

Command Syntax and Usage

access-control list <1-256> **action** {**permit**|**deny**|**set-priority** <0-7>}

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).

Command mode: Global configuration

[**no**] **access-control list** <1-256> **egress-port port** <port alias or number>

Configures the ACL to function on egress packets.

Command mode: Global configuration

[**no**] **access-control list** <1-256> **statistics**

Enables or disables the statistics collection for the Access Control List.

Command mode: All except User EXEC

default access-control list <1-256>

Resets the ACL parameters to their default values.

Command mode: Global configuration

show access-control list <1-256>

Displays the current ACL parameters.

Command mode: All

ACL Mirroring Configuration

These commands allow you to define port mirroring for an ACL. Packets that match the ACL are mirrored to the destination interface.

Table 169 ACL Port Mirroring Options

Command Syntax and Usage

[no] access-control list <1-256> mirror port <port alias or number> | none

Configures the destination to which packets that match this ACL are mirrored.

Command mode: Global configuration

show access-control list <1-256> mirror

Displays the current port mirroring parameters for the ACL.

Command mode: All

Ethernet Filtering Configuration

These commands allow you to define Ethernet matching criteria for an ACL.

Table 170 Ethernet Filtering Configuration Options

Command Syntax and Usage

**[no] access-control list <1-256> ethernet
source-mac-address <MAC address> <MAC mask>**

Defines the source MAC address for this ACL.

Command mode: Global configuration

**[no] access-control list <1-256> ethernet
destination-mac-address <MAC address> <MAC mask>**

Defines the destination MAC address for this ACL.

Command mode: Global configuration

[no] access-control list <1-256> ethernet vlan <VLAN ID> <VLAN mask>

Defines a VLAN number and mask for this ACL.

Command mode: Global configuration

Table 170 Ethernet Filtering Configuration Options

Command Syntax and Usage

```
[no] access-control list <1-256> ethernet ethernet-type  
  {arp|ip|ipv6|mpls|rarp|any|<other (0x600-0xFFFF)>}
```

Defines the Ethernet type for this ACL.

Command mode: Global configuration

```
[no] access-control list <1-256> ethernet priority <0-7>
```

Defines the Ethernet priority value for the ACL.

Command mode: Global configuration

```
default access-control list <1-256> ethernet
```

Resets Ethernet parameters for the ACL to their default values.

Command mode: Global configuration

```
no access-control list <1-256> ethernet
```

Removes Ethernet parameters for the ACL.

Command mode: Global configuration

```
show access-control list <1-256> ethernet
```

Displays the current Ethernet parameters for the ACL.

Command mode: All

IPv4 Filtering Configuration

These commands allow you to define IPv4 matching criteria for an ACL.

Table 171 IP version 4 Filtering Configuration Options

Command Syntax and Usage

[no] access-control list <1-256> ipv4 source-ip-address
 <IP address> <IP mask>

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.

Command mode: Global configuration

[no] access-control list <1-256> ipv4 destination-ip-address
 <IP address> <IP mask>

Defines a destination IP address for the ACL. If defined, traffic with this destination IP address will match this ACL.

Command mode: Global configuration

[no] access-control list <1-256> ipv4 protocol <0-255>

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.

Number	Name
1	icmp
2	igmp
6	tcp
17	udp
89	ospf
112	vrrp

Command mode: Global configuration

[no] access-control list <1-256> ipv4 type-of-service <0-255>

Defines a Type of Service (ToS) value for the ACL. For more information on ToS, refer to RFC 1340 and 1349.

Command mode: Global configuration

Table 171 IP version 4 Filtering Configuration Options

Command Syntax and Usage

default access-control list <1-256> **ipv4**

Resets the IPv4 parameters for the ACL to their default values.

Command mode: Global configuration

show access-control list <1-256> **ipv4**

Displays the current IPv4 parameters.

Command mode: All

TCP/UDP Filtering Configuration

These commands allow you to define TCP/UDP matching criteria for an ACL.

Table 172 TCP/UDP Filtering Configuration Options

Command Syntax and Usage

[no] access-control list <1-256> tcp-udp source-port <1-65535>
<mask (0xFFFF)>

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:

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

Command mode: Global configuration

[no] access-control list <1-256> tcp-udp destination-port
<1-65535> <mask (0xFFFF)>

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 `sport` above.

Command mode: Global configuration

[no] access-control list <1-256> tcp-udp
flags <value (0x0-0x3f)> <mask (0x0-0x3f)>

Defines a TCP/UDP flag for the ACL.

Command mode: Global configuration

Table 172 TCP/UDP Filtering Configuration Options**Command Syntax and Usage****default access-control list** <1-256> **tcp-udp**

Resets the TCP/UDP parameters for the ACL to their default values.

Command mode: Global configuration**show access-control list** <1-256> **tcp-udp**

Displays the current TCP/UDP Filtering parameters.

Command mode: All**ACL Metering Configuration**

These commands define the Access Control profile for the selected ACL.

Table 173 ACL Metering Configuration Options**Command Syntax and Usage****access-control list** <1-256> **meter committed-rate** <64-10000000>

Configures the committed rate, in kilobits per second. The committed rate must be a multiple of 64.

Command mode: Global configuration**access-control list** <1-256> **meter maximum-burst-size** <32-4096>

Configures the maximum burst size, in kilobits. Enter one of the following values for mbsize: 32, 64, 128, 256, 512, 1024, 2048, 4096

Command mode: Global configuration**[no] access-control list** <1-256> **meter enable**

Enables or disables ACL Metering.

Command mode: Global configuration**access-control list** <1-256> **meter action** {drop|pass}

Configures the ACL Meter to either drop or pass out-of-profile traffic.

Command mode: Global configuration**default access-control list** <1-256> **meter**

Sets the ACL meter configuration to its default values.

Command mode: Global configuration

Table 173 ACL Metering Configuration Options

Command Syntax and Usage

no access-control list <1-256> **meter**

Deletes the selected ACL meter.

Command mode: Global configuration

show access-control list <1-256> **meter**

Displays current ACL Metering parameters.

Command mode: All

ACL 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.

*Re-Marking In-Profile Configuration***Table 174** ACL Re-Marking In-Profile Options

Command Syntax and Usage

[no] access-control list <1-256> **re-mark in-profile dot1p** <0-7>

Remarks the 802.1p value. The value is the priority bits information in the packet structure.

Command mode: Global configuration

[no] no access-control list <1-256> **re-mark in-profile dscp** <0-63>

Remarks the DSCP value for in-profile traffic.

Command mode: Global configuration

[no] no access-control list <1-256> **re-mark in-profile use-tos-precedence**

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

Table 174 ACL Re-Marking In-Profile Options

Command Syntax and Usage

default access-control list <1-256> re-mark

Sets the ACL re-mark parameters to their default values.

Command mode: Global configuration

show access-control list <1-256> re-mark

Displays current re-mark parameters.

Command mode: All

*Re-Marking Out-of-Profile Configuration***Table 175** ACL Re-Marking Out-of-Profile Options

Command Syntax and Usage

access-control list <1-256> re-mark out-profile dscp <1-63>

Re-marks the DSCP value on out-of-profile packets for the ACL.

Command mode: Global configuration

no access-control list <1-256> re-mark out-profile

Disables re-marking on out-of-profile traffic.

Command mode: Global configuration

show access-control list <1-256> re-mark

Displays current re-mark parameters.

Command mode: All

Packet Format Filtering Configuration

These commands allow you to define Packet Format matching criteria for an ACL.

Table 176 Packet Format Filtering Configuration Options

Command Syntax and Usage

[no] access-control list <1-256> packet-format ethernet {ethertype2|snap|llc}

Defines the Ethernet format for the ACL.

Command mode: Global configuration

[no] access-control list <1-256> packet-format tagging {any|none|tagged}

Defines the tagging format for the ACL.

Command mode: Global configuration

[no] access-control list <1-256> packet-format ip {ipv4|ipv6}

Defines the IP format for the ACL.

Command mode: Global configuration

default access-control list <1-256> packet-format

Resets Packet Format parameters for the ACL to their default values.

Command mode: Global configuration

show access-control list <1-256> packet-format

Displays the current Packet Format parameters for the ACL.

Command mode: All

ACL IPv6 Configuration

These commands allow you to define filtering criteria for each IPv6 Access Control List (ACL).

Table 177 IPv6 ACL Options

Command Syntax and Usage

[no] access-control list6 <1-128> egress-port port <port alias or number>

Configures the ACL to function on egress packets.

Command mode: Global configuration

**access-control list6 <1-128> action {permit|deny|
set-priority <0-7>}**

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).

Command mode: Global configuration

[no] access-control list6 <1-128> statistics

Enables or disables the statistics collection for the Access Control List.

Command mode: Global configuration

default access-control list6 <1-128>

Resets the ACL parameters to their default values.

Command mode: Global configuration

show access-control list <1-128>

Displays the current ACL parameters.

Command mode: All

IP version 6 Filtering Configuration

These commands allow you to define IPv6 matching criteria for an ACL.

Table 178 IP version 6 Filtering Options

Command Syntax and Usage

[no] access-control list6 <1-128> **ipv6 source-address** <IPv6 address>
<prefix length (1-128)>

Defines a source IPv6 address for the ACL. If defined, traffic with this source address will match this ACL.

Command mode: Global configuration

[no] access-control list6 <1-128> **ipv6 destination-address**
<IPv6 address> <prefix length (1-128)>

Defines a destination IPv6 address for the ACL. If defined, traffic with this destination address will match this ACL.

Command mode: Global configuration

[no] access-control list6 <1-128> **ipv6 next-header** <0-255>

Defines the next header value for the ACL. If defined, traffic with this next header value will match this ACL.

[no] access-control list6 <1-128> **ipv6 flow-label** <0-0xFFFF>

Defines the flow label for the ACL. If defined, traffic with this flow label will match this ACL.

[no] access-control list6 <1-128> **ipv6 traffic-class** <0-255>

Defines the traffic class for the ACL. If defined, traffic with this traffic class will match this ACL.

default access-control list6 <1-128> **ipv6**

Resets the IPv6 parameters for the ACL to their default values.

Command mode: Global configuration

show access-control list6 <1-128> **ipv6**

Displays the current IPv6 parameters.

Command mode: All

IPv6 TCP/UDP Filtering Configuration

These commands allows you to define TCP/UDP matching criteria for an ACL.

Table 179 IPv6 ACL TCP/UDP Filtering Options

Command Syntax and Usage

[no] access-control list6 <1-128> tcp-udp source-port <1-65535>
<mask (0xFFFF)>

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:

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

Command mode: Global configuration

[no] access-control list6 <1-128> tcp-udp destination-port
<1-65535> <mask (0xFFFF)>

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 `source-port` above.

Command mode: Global configuration

[no] access-control list6 <1-128> tcp-udp
flags <value (0x0-0x3f)> <mask (0x0-0x3f)>

Defines a TCP/UDP flag for the ACL.

Command mode: Global configuration

Table 179 IPv6 ACL TCP/UDP Filtering Options

Command Syntax and Usage

default access-control list6 <1-128> **tcp-udp**

Resets the TCP/UDP parameters for the ACL to their default values.

Command mode: Global configuration

show access-control list6 <1-128> **tcp-udp**

Displays the current TCP/UDP Filtering parameters.

Command mode: All

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 180 IPv6 Re-Marking In-Profile Options

Command Syntax and Usage

[no] access-control list6 <1-128> **re-mark dot1p** <0-7>

Re-marks the 802.1p value. The value is the priority bits information in the packet structure.

Command mode: Global configuration

[no] no access-control list6 <1-128> **re-mark in-profile dscp** <0-63>

Re-marks the DSCP value for in-profile traffic.

Command mode: Global configuration

[no] no access-control list6 <1-128> **re-mark use-tos-precedence**

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

Table 180 IPv6 Re-Marking In-Profile Options

Command Syntax and Usage

default access-control list6 <1-128> **re-mark**

Sets the ACL re-mark parameters to their default values.

Command mode: Global configuration

show access-control list6 <1-128> **re-mark**

Displays current re-mark parameters.

Command mode: All

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 181 ACL Group Configuration Commands

Command Syntax and Usage

access-control group <1-256> **list** <1-256>

Adds the selected IPv4 ACL to the ACL group.

Command mode: Global configuration

no access-control group <1-256> **list** <1-256>

Removes the selected IPv4 ACL from the ACL group.

Command mode: Global configuration

access-control group <1-256> **list6** <1-128>

Adds the selected IPv6 ACL to the ACL group.

Command mode: Global configuration

no access-control group <1-256> **list6** <1-128>

Removes the selected IPv6 ACL from the ACL group.

Command mode: Global configuration

show access-control group <1-256>

Displays the current ACL group parameters.

Command mode: All

Management ACL Configuration

These commands allow you to define filtering criteria for each management ACL (MACL).

Table 182 MACL Configuration Options

Command Syntax and Usage

access-control macl <1-256> **action** {**permit**|**deny**|**set-priority** <0-7>}

Configures a filter action for packets that match the MACL definitions. You can choose to permit (pass) or deny (drop) packets, or set the 802.1p priority level (0-7).

Command mode: Global configuration

[**no**] **access-control macl** <1-256> **statistics**

Enables or disables the statistics collection for the MACL.

Command mode: All except User EXEC

[**no**] **access-control macl** <1-256> **enable**

Enables or disables the management ACL.

Command mode: Global configuration

show access-control macl <1-256>

Displays the current MACL parameters.

Command mode: All

MACL IPv4 Filtering Configuration

These commands allow you to define IPv4 matching criteria for an MACL.

Table 183 IP version 4 Filtering Configuration Options

Command Syntax and Usage

[no] access-control macl <1-256> ipv4 source-ip-address
 <IP address> <IP mask>

Defines a source IP address for the MACL. If defined, traffic with this source IP address will match this MACL. Specify an IP address in dotted decimal notation.

Command mode: Global configuration

[no] access-control macl <1-256> ipv4 destination-ip-address
 <IP address> <IP mask>

Defines a destination IP address for the MACL. If defined, traffic with this destination IP address will match this MACL.

Command mode: Global configuration

[no] access-control macl <1-256> ipv4 protocol <0-255>

Defines an IP protocol for the MACL. If defined, traffic from the specified protocol matches this filter. Specify the protocol number. Listed below are some of the well-known protocols.

Number	Name
1	icmp
2	igmp
6	tcp
17	udp
89	ospf
112	vrrp

Command mode: Global configuration

[no] access-control macl <1-256> ipv4 type-of-service <0-255>

Defines a Type of Service (ToS) value for the MACL. For more information on ToS, refer to RFC 1340 and 1349.

Command mode: Global configuration

Table 183 IP version 4 Filtering Configuration Options

Command Syntax and Usage

default access-control mac1 <1-256> ipv4

Resets the IPv4 parameters for the MACL to their default values.

Command mode: Global configuration

show access-control mac1 <1-256> ipv4

Displays the current IPv4 parameters.

Command mode: All

MACL TCP/UDP Filtering Configuration

These commands allow you to define TCP/UDP matching criteria for an MACL.

Table 184 TCP/UDP Filtering Configuration Options

Command Syntax and Usage

[no] access-control mac1 <1-256> tcp-udp source-port <1-65535>
<mask (0xFFFF)>

Defines a source port for the MACL. If defined, traffic with the specified TCP or UDP source port will match this MACL. Specify the port number. Listed below are some of the well-known ports:

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

Command mode: Global configuration

[no] access-control mac1 <1-256> tcp-udp destination-port
<1-65535> <mask (0xFFFF)>

Defines a destination port for the MACL. If defined, traffic with the specified TCP or UDP destination port will match this MACL. Specify the port number, just as with `sport` above.

Command mode: Global configuration

[no] access-control mac1 <1-256> tcp-udp
flags <value (0x0-0x3f)> <mask (0x0-0x3f)>

Defines a TCP/UDP flag for the MACL.

Command mode: Global configuration

Table 184 TCP/UDP Filtering Configuration Options

Command Syntax and Usage

default access-control mac1 <1-256> tcp-udp

Resets the TCP/UDP parameters for the MACL to their default values.

Command mode: Global configuration

show access-control mac1 <1-256> tcp-udp

Displays the current TCP/UDP Filtering parameters.

Command mode: All

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 [“ACL IPv4 Configuration” on page 286](#).

For more information about assigning VLAN Maps to a VLAN, see [“VLAN Configuration” on page 349](#).

For more information about assigning VLAN Maps to a VM group, see [“VM Group Configuration” on page 468](#).

Table 185 lists the general VMAP configuration commands.

Table 185 VMAP Configuration Options

Command Syntax and Usage

access-control vmap <1-256> **action** {**permit**|**deny**|**set-priority** <0-7>}

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).

Command mode: Global configuration

[no] **access-control vmap** <1-256> **statistics**

Enables or disables the statistics collection for the VMAP.

Command mode: All except User EXEC

default access-control vmap <1-256>

Resets the VMAP parameters to their default values.

Command mode: Global configuration

show access-control vmap <1-256>

Displays the current VMAP parameters.

Command mode: All except User EXEC

Port Mirroring

Port mirroring is disabled by default. For more information about port mirroring on the G8264, see “Appendix A: Troubleshooting” in the *BLADEOS 6.6 Application Guide*.

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 186 Port Mirroring Configuration Options

Command Syntax and Usage

[no] port-mirroring enable

Enables or disables port mirroring.

Command mode: Global configuration

show port-mirroring

Displays current settings of the mirrored and monitoring ports.

Command mode: All except User EXEC

Port-Mirroring Configuration

Table 187 Port-Based Port-Mirroring Configuration Options

Command Syntax and Usage

port-mirroring monitor-port *<port alias or number>* **mirroring-port**
<port alias or number> { **in** | **out** | **both** }

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:

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.

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.

Command mode: Global configuration

no port-mirroring monitor-port *<port alias or number>* **mirroring-port**
<port alias or number>

Removes the mirrored port.

Command mode: Global configuration

show port-mirroring

Displays the current settings of the monitoring port.

Command mode: All except User EXEC

Layer 2 Configuration

The following table describes basic Layer 2 Configuration commands. The following sections provide more detailed information and commands.

Table 188 Layer 2 Configuration Commands

Command Syntax and Usage

vlan <VLAN number>

Enter VLAN configuration mode. To view command options, see [page 349](#).

Command mode: Global configuration

spanning-tree mode disable

When enabled, globally turns Spanning Tree `off` (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.

To enable Spanning-Tree, select another Spanning-Tree mode.

Command mode: Global configuration

[no] spanning-tree pvst-compatibility

Enables or disables VLAN tagging of Spanning Tree BPDUs. The default setting is enabled.

Command mode: Global configuration

[no] spanning-tree loopguard

Globally enables or disables Spanning Tree loop guard. For information about setting loop guard on an individual port, see [page 276](#).

Command mode: Global configuration

show layer2

Displays current Layer 2 parameters.

Command mode: All

802.1X Configuration

These commands allow you to configure the G8264 as an IEEE 802.1X Authenticator, to provide port-based network access control.

Table 189 802.1x Configuration Options

Command Syntax and Usage

dot1x enable

Globally enables 802.1X.

Command mode: Global configuration

no dot1x enable

Globally disables 802.1X.

Command mode: Global configuration

show dot1x

Displays current 802.1X parameters.

Command mode: All

The following sections describe the 802.1x configuration options.

- [“802.1X Global Configuration” on page 311](#)
- [“802.1X Guest VLAN Configuration” on page 313](#)
- [“802.1X Port Configuration” on page 314](#)

802.1X Global Configuration

The global 802.1X commands allow you to configure parameters that affect all ports in the switch.

Table 190 802.1X Global Configuration Options

Command Syntax and Usage

dot1x mode [**force-unauthorized** | **auto** | **force-authorized**]

Sets the type of access control for all ports:

- ❑ **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.

The default value is `force-authorized`.

Command mode: Global configuration

dot1x quiet-time <0-65535>

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.

Command mode: Global configuration

dot1x transmit-interval <1-65535>

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.

Command mode: Global configuration

dot1x supplicant-timeout <1-65535>

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.

Command mode: Global configuration

Table 190 802.1X Global Configuration Options

Command Syntax and Usage

dot1x server-timeout <1-65535>

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.

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).

Command mode: Global configuration

dot1x max-request <1-10>

Sets the maximum number of times the authenticator retransmits an EAP-Request packet to the supplicant (client). The default value is 2.

Command mode: Global configuration

dot1x re-authentication-interval <1-604800>

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.

Command mode: Global configuration

dot1x re-authenticate

Sets the re-authentication status to on. The default value is off.

Command mode: Global configuration

[no] dot1x re-authenticate

Sets the re-authentication status to off. The default value is off.

Command mode: Global configuration

[no] dot1x vlan-assign

Sets the dynamic VLAN assignment status to on or off. The default value is off.

Command mode: Global configuration

Table 190 802.1X Global Configuration Options

Command Syntax and Usage

default dot1x

Resets the global 802.1X parameters to their default values.

Command mode: Global configuration

show dot1x

Displays current global 802.1X parameters.

Command mode: All

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 191 802.1X Guest VLAN Configuration Options

Command Syntax and Usage

[no] dot1x guest-vlan vlan <VLAN number>

Configures the Guest VLAN number.

Command mode: Global configuration

dot1x guest-vlan enable

Enables the 802.1X Guest VLAN.

Command mode: Global configuration

no dot1x guest-vlan enable

Disables the 802.1X Guest VLAN.

Command mode: Global configuration

show dot1x

Displays current 802.1X parameters.

Command mode: All

802.1X Port Configuration

The 802.1X port commands allows you to configure parameters that affect the selected port in the switch. These settings override the global 802.1X parameters.

Table 192 802.1X Port Options

Command Syntax and Usage

dot1x mode force-unauthorized | auto | force-authorized

Sets the type of access control for the port:

- ❑ **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.

The default value is `force-authorized`.

Command mode: Interface port

dot1x quiet-time *<0-65535>*

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.

Command mode: Interface port

dot1x transmit-interval *<1-65535>*

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.

Command mode: Interface port

dot1x supplicant-timeout *<1-65535>*

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.

Command mode: Interface port

Table 192 802.1X Port Options

Command Syntax and Usage

dot1x server-timeout <1-65535>

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.

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.

Command mode: Interface port

dot1x max-request <1-10>

Sets the maximum number of times the authenticator retransmits an EAP-Request packet to the supplicant (client). The default value is 2.

Command mode: Interface port

dot1x re-authentication-interval <1-604800>

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.

Command mode: Interface port

dot1x re-authenticate

Sets the re-authentication status to `on`. The default value is `off`.

Command mode: Interface port

[no] dot1x re-authenticate

Sets the re-authentication status `off`. The default value is `off`.

Command mode: Interface port

[no] dot1x vlan-assign

Sets the dynamic VLAN assignment status to `on` or `off`. The default value is `off`.

Command mode: Interface port

default dot1x

Resets the 802.1X port parameters to their default values.

Command mode: Interface port

Table 192 802.1X Port Options

Command Syntax and Usage

dot1x apply-global

Applies current global 802.1X configuration parameters to the port.

Command mode: Interface port

show interface port <port alias or number> dot1x

Displays current 802.1X port parameters.

Command mode: All

RSTP/MSTP/PVRST Configuration

BLADEOS 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. MRST is turned on by default and the default STP mode is RSTP.

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 193 Multiple Spanning Tree Configuration Options

Command Syntax and Usage

spanning-tree mstp name <1-32 characters>

Configures a name for the MSTP region. All devices within an MSTP region must have the same region name.

Command mode: Global configuration

spanning-tree mstp version <0-65535>

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.

Command mode: Global configuration

Table 193 Multiple Spanning Tree Configuration Options

Command Syntax and Usage

spanning-tree mstp maximum-hop <4-60>

Configures the maximum number of bridge hops a packet may traverse before it is dropped. The default value is 20.

Command mode: Global configuration

spanning-tree mode [**disable**|**mst**|**pvrst**|**rstp**]

Selects and enables Multiple Spanning Tree mode (**mst**), Per VLAN Rapid Spanning Tree mode (**pvrst**), or Rapid Spanning Tree mode (**rstp**).

The default mode is RSTP.

When you select **spanning-tree disable**, the switch globally turns Spanning Tree off. All ports are placed into forwarding state. Any BPDU's received are flooded. BPDU Guard is not affected by this command.

Command mode: Global configuration

show spanning-tree mstp mrst

Displays the current RSTP/MSTP/PVRST+ configuration.

Command mode: All

Common Internal Spanning Tree Configuration

[Table 194](#) 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 194 CIST Configuration Options

Command Syntax and Usage

default spanning-tree mstp cist

Resets all CIST parameters to their default values.

Command mode: Global configuration

show spanning-tree mstp cist

Displays the current CIST configuration.

Command mode: All

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 195 CIST Bridge Configuration Options

Command Syntax and Usage

spanning-tree mstp cist-bridge priority <0-65535>

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.

The range is 0 to 65535, in steps of 4096 (0, 4096, 8192...), and the default value is 61440.

Command mode: Global configuration

spanning-tree mstp cist-bridge maximum-age <6-40>

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.

Command mode: Global configuration

spanning-tree mstp cist-bridge forward-delay <4-30>

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.

Command mode: Global configuration

show spanning-tree mstp cist

Displays the current CIST bridge configuration.

Command mode: All Except User EXEC

CIST Port Configuration

CIST port parameters are used to modify MSTP 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 196 CIST Port Configuration Options

Command Syntax and Usage

spanning-tree mstp cist interface-priority <0-240>

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.

The range is 0 to 240, in steps of 16 (0, 16, 32...), and the default is 128.

Command mode: Interface port

spanning-tree mstp cist path-cost <0-200000000>

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:

- 1Gbps = 20000
- 10Gbps = 2000

The default value of 0 (zero) indicates that the default path cost will be computed for an auto negotiated link speed.

Command mode: Interface port

spanning-tree mstp cist hello <1-10>

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.

Command mode: Interface port

[no] spanning-tree mstp cist pvst-protection

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.

Command mode: Interface port

Table 196 CIST Port Configuration Options

Command Syntax and Usage

spanning-tree mstp cist enable

Enables MRST on the port.

Command mode: Interface port

no spanning-tree mstp cist enable

Disables MRST on the port.

Command mode: Interface port

show interface port <port alias or number> spanning-tree mstp cist

Displays the current CIST port configuration.

Command mode: All

Spanning Tree Configuration

BLADEOS supports the IEEE 802.1D Spanning Tree Protocol (STP). 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 197 Spanning Tree Configuration Options

Command Syntax and Usage

spanning-tree stp <STG number> **vlan** <VLAN number>

Associates a VLAN with a Spanning Tree Group and requires a VLAN ID as a parameter.

Command mode: Global configuration

no spanning-tree stp <STG number> **vlan** <VLAN number>

Breaks the association between a VLAN and a Spanning Tree Group and requires a VLAN ID as a parameter.

Command mode: Global configuration

no spanning-tree stp <STG number> **vlan all**

Removes all VLANs from a Spanning Tree Group.

Command mode: Global configuration

spanning-tree stp <STG number> **enable**

Globally enables Spanning Tree Protocol. STG is turned on by default.

Command mode: Global configuration

no spanning-tree stp <STG number> **enable**

Globally disables Spanning Tree Protocol.

Command mode: Global configuration

default spanning-tree <STG number>

Restores a Spanning Tree instance to its default configuration.

Command mode: Global configuration

show spanning-tree stp <STG number>

Displays current Spanning Tree Protocol parameters.

Command mode: All

Bridge Spanning Tree 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 198 Bridge Spanning Tree Configuration Options

Command Syntax and Usage

spanning-tree stp <STG number> **bridge priority** <0-65535>

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 default value is 32768.

Command mode: Global configuration

spanning-tree stp <STG number> **bridge hello-time** <1-10>

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.

This command does not apply to MSTP.

Command mode: Global configuration

spanning-tree stp <STG number> **bridge maximum-age** <6-40>

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 reconfigures the STG network. The range is 6 to 40 seconds, and the default is 20 seconds.

This command does not apply to MSTP.

Command mode: Global configuration

Table 198 Bridge Spanning Tree Configuration Options

Command Syntax and Usage

spanning-tree stp <STG number> **bridge forward-delay** <4-30>

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.

This command does not apply to MSTP

Command mode: Global configuration

show spanning-tree stp <STG number> **bridge**

Displays the current bridge STG parameters.

Command mode: All

When configuring STG bridge parameters, the following formulas must be used:

- $2*(fwd-1) \geq mxage$
- $2*(hello+1) \leq mxage$

Spanning Tree 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

For more information about port Spanning Tree commands, see [“Port Spanning Tree Configuration” on page 275](#).

Table 199 Spanning Tree Port Options

Command Syntax and Usage

spanning-tree stp <STG number> **priority** <0-255>

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.

RSTP/MSTP: The range is 0 to 240, in steps of 16 (0, 16, 32...) and the default is 128.

Command mode: Interface port

spanning-tree stp <STG number> **path-cost** <1-65535, 0 for default>

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:

- 1Gbps = 4
- 10Gbps = 2

The default value of 0 (zero) indicates that the default path cost will be computed for an auto negotiated link speed.

Command mode: Interface port

spanning-tree stp link-type {auto|p2p|shared}

Defines the type of link connected to the port, as follows:

- **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).

Command mode: Interface port

Table 199 Spanning Tree Port Options

Command Syntax and Usage

[no] spanning-tree stp <STG number> fastforward

Disables or enables Port Fast Forwarding, which permits a port that participates in Spanning Tree to bypass the Listening and Learning states and enter directly into the Forwarding state. While in the Forwarding state, the port listens to the BPDUs to learn if there is a loop and, if dictated by normal STG behavior (following priorities, etc.), the port transitions into the Blocking state.

Note: This feature is used only when the switch is in STP/PVST+ mode, and permits the switch to interoperate well within Rapid Spanning Tree networks.

The default setting is disabled.

Command mode: Interface port

spanning-tree stp <STG number> enable

Enables STG on the port.

Command mode: Interface port

no spanning-tree stp <STG number> enable

Disables STG on the port.

Command mode: Interface port

show interface port <port alias or number> spanning-tree stp <STG number>

Displays the current STG port parameters.

Command mode: All

Forwarding Database Configuration

Use the following commands to configure the Forwarding Database (FDB).

Table 200 FDB Configuration Options

Command Syntax and Usage

mac-address-table aging *<0-65535>*

Configures the aging value for FDB entries, in seconds. The default value is 300.

Command mode: Global configuration

show mac-address-table

Display current FDB configuration.

Command mode: All except User EXEC

Static FDB Configuration

Use the following commands to configure static entries in the Forwarding Database (FDB).

Table 201 FDB Configuration Options

Command Syntax and Usage

mac-address-table static *<MAC address>* **vlan** *<VLAN number>*
 {**port** *<port alias or number>* | **portchannel** *<trunk number>* |
adminkey *<0-65535>*}

Adds a permanent FDB entry. Enter the MAC address using the following format,
 xx:xx:xx:xx:xx:xx

For example, 08:00:20:12:34:56

You can also enter the MAC address as follows:

xxxxxxxxxxxx

For example, 080020123456

Command mode: Global configuration

no mac-address-table static [*<MAC address>*] [*<VLAN number>*] | **all**

Deletes permanent FDB entries.

Command mode: Global configuration

Table 201 FDB Configuration Options

Command Syntax and Usage

```
clear mac-address-table multicast {all|mac <MAC address> |  
  vlan <VLAN number> | port <port alias or number> }
```

Clears static multicast entries.

Command mode: Global configuration

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

Display current FDB configuration.

Command mode: All except User EXEC

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 202 Static Multicast MAC Configuration Options

Command Syntax and Usage

mac-address-table multicast *<MAC address>* *<VLAN number>*
 {**port** *<port alias or number>*}

Adds a static multicast entry. You can list ports separated by a comma, or enter a range of ports separated by a hyphen (-). For example:

mac-address-table multicast 01:00:00:23:3f:01 200 1-4

Command mode: Global configuration

no mac-address-table multicast {**all** | *<MAC address>* *<VLAN number>*}

Deletes a static multicast entry.

Command mode: Global configuration

show mac-address-table multicast

Display the current static multicast entries.

Command mode: All

LLDP Configuration

Use the following commands to configure Link Layer Detection Protocol (LLDP).

Table 203 LLDP Configuration Options

Command Syntax and Usage

lldp refresh-interval *<5-32768>*

Configures the message transmission interval, in seconds. The default value is 30.

Command mode: Global configuration

lldp holdtime-multiplier *<2-10>*

Configures the message hold time multiplier. The hold time is configured as a multiple of the message transmission interval.

The default value is 4.

Command mode: Global configuration

Table 203 LLDP Configuration Options

Command Syntax and Usage

lldp trap-notification-interval <1-3600>

Configures the trap notification interval, in seconds. The default value is 5.

Command mode: Global configuration

lldp transmission-delay <1-8192>

Configures the transmission delay interval. The transmit delay timer represents the minimum time permitted between successive LLDP transmissions on a port.

The default value is 2.

Command mode: Global configuration

lldp reinit-delay <1-10>

Configures the re-initialization delay interval, in seconds. The re-initialization delay allows the port LLDP information to stabilize before transmitting LLDP messages.

The default value is 2.

Command mode: Global configuration

lldp enable

Globally turns LLDP on. The default setting is **off**.

Command mode: Global configuration

no lldp enable

Globally turns LLDP off.

Command mode: Global configuration

show lldp

Display current LLDP configuration.

Command mode: All

LLDP Port Configuration

Use the following commands to configure LLDP port options.

Table 204 LLDP Port Options

Command Syntax and Usage

lldp admin-status {**disabled**|**tx_only**|**rx_only**|**tx_rx**}

Configures the LLDP transmission type for the port, as follows:

- Transmit only
- Receive only
- Transmit and receive
- Disabled

The default setting is **tx_rx**.

Command mode: Interface port

[no] lldp trap-notification

Enables or disables SNMP trap notification for LLDP messages.

Command mode: Interface port

show interface port <*port alias or number*> **lldp**

Display current LLDP port configuration.

Command mode: All

LLDP Optional TLV configuration

Use the following commands to configure LLDP port TLV (Type, Length, Value) options for the selected port.

Table 205 Optional TLV Options

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

Table 205 Optional TLV Options

Command Syntax and Usage

[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

[no] lldp tlv powermdi

Enables or disables the Power via MDI information type.

Command mode: Interface port

Table 205 Optional TLV Options

Command Syntax and Usage

[no] lldp tlv linkaggr

Enables or disables the Link Aggregation information type.

Command mode: Interface port

[no] lldp tlv framesz

Enables or disables the Maximum Frame Size information type.

Command mode: Interface port

[no] lldp tlv dcbx

Enables or disables the Maximum Frame Size information type.

Command mode: Interface port

[no] lldp tlv all

Enables or disables all optional TLV information types.

Command mode: Interface port

show interface port *<port alias or number>* **lldp**

Display current LLDP port configuration.

Command mode: All

Trunk Configuration

Trunk groups can provide super-bandwidth connections between RackSwitch G8264s 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 static trunk groups can be configured on the G8264, with the following restrictions:

- Any physical switch port can belong to no more than one trunk group.
- Up to 16 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-BLADE devices must comply with Cisco® EtherChannel® technology.

By default, each trunk group is empty and disabled.

Table 206 Trunk Configuration Options

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 <1-36>

Displays current trunk group parameters.

Command mode: All

IP Trunk Hash Configuration

Use the following commands to configure IP trunk hash settings for the G8264. Trunk hash parameters are set globally for the G8264. 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 207](#) combined with the hash parameters listed in [Table 208](#) and [Table 209](#).

Table 207 Trunk Hash Settings

Command Syntax and Usage

[no] portchannel thash ingress

Enables or disables use of the ingress port to compute the trunk hash value. The default setting is disabled.

Command mode: Global configuration

[no] portchannel thash L4port

Enables or disables use of Layer 4 service ports (TCP, UDP, etc.) to compute the hash value. The default setting is disabled.

Command mode: Global configuration

show portchannel hash

Display current trunk hash configuration.

Command mode: All

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 208 Layer 2 Trunk Hash Options

Command Syntax and Usage

[no] portchannel thash l2hash l2-source-mac-address

Enables or disables Layer 2 trunk hashing on the source MAC.

Command mode: Global configuration

[no] portchannel thash l2hash l2-destination-mac-address

Enables or disables Layer 2 trunk hashing on the destination MAC.

Command mode: Global configuration

[no] portchannel thash l2hash l2-source-destination-mac

Enables or disables Layer 2 trunk hashing on both the source and destination MAC.

Command mode: Global configuration

show portchannel hash

Displays the current trunk hash settings.

Command mode: All

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 209 Layer 3 Trunk Hash Options

Command Syntax and Usage

[no] portchannel thash l3thash l3-use-l2-hash

Enables or disables use of Layer 2 hash parameters only. When enabled, Layer 3 hashing parameters are cleared.

Command mode: Global configuration

[no] portchannel thash l3thash l3-source-ip-address

Enables or disables Layer 3 trunk hashing on the source IP address.

Command mode: Global configuration

[no] portchannel thash l3thash l3-destination-ip-address

Enables or disables Layer 3 trunk hashing on the destination IP address.

Command mode: Global configuration

[no] portchannel thash l3thash l3-source-destination-ip

Enables or disables Layer 3 trunk hashing on both the source and the destination IP address.

Command mode: Global configuration

show portchannel hash

Displays the current trunk hash settings.

Command mode: All

Virtual Link Aggregation Control Protocol Configuration

vLAG groups allow you to enhance redundancy and prevent implicit loops without using STP. The vLAG group acts as a single virtual entity for the purpose of establishing a multi-port trunk.

Table 210 vLAG Configuration Options

Command Syntax and Usage

[no] vlag portchannel <trunk group number> **enable**

Enables or disables vLAG on the selected trunk group.

Command mode: Global configuration

[no] vlag adminkey <1-65535> **enable**

Enables or disables vLAG on the selected LACP *admin key*. LACP trunks formed with this *admin key* will be included in the vLAG configuration.

Command mode: Global configuration

vlag priority <0-65535>

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.

Command mode: Global configuration

vlag peer-ip <IP address>

Configures the IP address of the vLAG peer.

Command mode: Global configuration

vlag hlthchk-peer-ip <IP address>

Configures the IP address of the peer switch, used for health checks. Use the management IP address of the peer switch.

Command mode: Global configuration

show vlag information

Displays current vLAG parameters.

Command mode: All

vLAG ISL Configuration

These commands allow you to configure a dedicated inter-switch link (ISL) for synchronization between vLAG peers.

Table 211 vLAG ISL Configuration Options

Command Syntax and Usage

[no] vlag isl portchannel <trunk group number>

Enables or disables vLAG Inter-Switch Link (ISL) on the selected trunk group.

Command mode: Global configuration

[no] vlag isl adminkey <1-65535>

Enables or disables vLAG Inter-Switch Link (ISL) on the selected LACP *admin key*. LACP trunks formed with this *admin key* will be included in the ISL.

Command mode: Global configuration

[no] vlag isl vlan <VLAN number>

Enables or disables vLAG Inter-Switch Link (ISL) on the VLAN. This VLAN is used to carry VLAG protocol data.

Command mode: Global configuration

show vlag information

Displays current vLAG parameters.

Command mode: All

Link Aggregation Control Protocol Configuration

Use the following commands to configure Link Aggregation Control Protocol (LACP) for the G8264.

Table 212 Link Aggregation Control Protocol Options

Command Syntax and Usage

lACP system-priority <1-65535>

Defines the priority value for the G8264. Lower numbers provide higher priority. The default value is 32768.

Command mode: Global configuration

lACP timeout {short|long}

Defines the timeout period before invalidating LACP data from a remote partner. Choose `short` (3 seconds) or `long` (90 seconds). The default value is `long`.

Note: It is recommended that you use a timeout value of `long`, to reduce LACPDU processing. If your G8264's CPU utilization rate remains at 100% for periods of 90 seconds or more, consider using static trunks instead of LACP.

Command mode: Global configuration

no lACP <1-65535>

Deletes a selected LACP trunk, based on its *admin key*. This command is equivalent to disabling LACP on each of the ports configured with the same *admin key*.

Command mode: Global configuration

show lACP

Display current LACP configuration.

Command mode: All

LACP Port Configuration

Use the following commands to configure Link Aggregation Control Protocol (LACP) for the selected port.

Table 213 LACP Port Options

Command Syntax and Usage

lACP mode {**off**|**active**|**passive**}

Set the LACP mode for this port, as follows:

- **off**
Turn LACP off for this port. You can use this port to manually configure a static trunk. The default value is **off**.
- **active**
Turn LACP on and set this port to active. Active ports initiate LACPDU.
- **passive**
Turn LACP on and set this port to passive. Passive ports do not initiate LACPDU, but respond to LACPDU from active ports.

Command mode: Interface port

lACP priority <1-65535>

Sets the priority value for the selected port. Lower numbers provide higher priority. The default value is 32768.

Command mode: Interface port

lACP key <1-65535>

Set the *admin key* for this port. Only ports with the same *admin key* and *oper key* (operational state generated internally) can form a LACP trunk group.

Command mode: Interface port

show interface port <port alias or number> **lACP**

Displays the current LACP configuration for this port.

Command mode: All

Layer 2 Failover Configuration

Use these commands to configure Layer 2 Failover. For more information about Layer 2 Failover, see “High Availability” in the *BLADEOS Application Guide*.

Table 214 Layer 2 Failover Configuration Options

Command Syntax and Usage

failover enable

Globally turns Layer 2 Failover on.

Command mode: Global configuration

no failover enable

Globally turns Layer 2 Failover off.

Command mode: Global configuration

show failover trigger

Displays current Layer 2 Failover parameters.

Command mode: All

Failover Trigger Configuration

Table 215 Failover Trigger Configuration Options

Command Syntax and Usage

[no] failover trigger <1-8> enable

Enables or disables the Failover trigger.

Command mode: Global configuration

no failover trigger <1-8>

Deletes the Failover trigger.

Command mode: Global configuration

failover trigger <1-8> limit <0-1024>

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

show failover trigger <1-8>

Displays the current failover trigger settings.

Command mode: All

Failover Manual Monitor Port Configuration

Use these commands to define the port link(s) to monitor. The Manual Monitor Port configuration accepts any non-management port.

Table 216 Failover Manual Monitor Port Options

Command Syntax and Usage

failover trigger <1-8> mmon monitor member <port alias or number>

Adds the selected port to the Manual Monitor Port configuration.

Command mode: Global configuration

no failover trigger <1-8> mmon monitor member <port alias or number>

Removes the selected port from the Manual Monitor Port configuration.

Command mode: Global configuration

Table 216 Failover Manual Monitor Port Options

Command Syntax and Usage

failover trigger <1-8> **mmon monitor portchannel** <trunk number>

Adds the selected trunk group to the Manual Monitor Port configuration.

Command mode: Global configuration

no failover trigger <1-8> **mmon monitor portchannel** <trunk number>

Removes the selected trunk group from the Manual Monitor Port configuration.

Command mode: Global configuration

failover trigger <1-8> **mmon monitor adminkey** <1-65535>

Adds an LACP *admin key* to the Manual Monitor Port configuration. LACP trunks formed with this admin key will be included in the Manual Monitor Port configuration.

Command mode: Global configuration

no failover trigger <1-8> **mmon monitor adminkey** <1-65535>

Removes an LACP *admin key* from the Manual Monitor Port configuration.

Command mode: Global configuration

show failover trigger <1-8>

Displays the current Failover settings.

Command mode: All

Failover Manual Monitor Control Configuration

Use these commands to define the port link(s) to control. The Manual Monitor Control configuration accepts any non-management port.

Table 217 Failover Manual Monitor Control Options

Command Syntax and Usage

failover trigger <1-8> **mmon control member** <port alias or number>

Adds the selected port to the Manual Monitor Control configuration.

Command mode: Global configuration

no failover trigger <1-8> **mmon control member** <port alias or number>

Removes the selected port from the Manual Monitor Control configuration.

Command mode: Global configuration

failover trigger <1-8> **mmon control portchannel** <trunk number>

Adds the selected trunk group to the Manual Monitor Control configuration.

Command mode: Global configuration

no failover trigger <1-8> **mmon control portchannel** <trunk number>

Removes the selected trunk group from the Manual Monitor Control configuration.

Command mode: Global configuration

failover trigger <1-8> **mmon control adminkey** <1-65535>

Adds an LACP *admin key* to the Manual Monitor Control configuration. LACP trunks formed with this admin key will be included in the Manual Monitor Control configuration.

Command mode: Global configuration

no failover trigger <1-8> **mmon control adminkey** <1-65535>

Removes an LACP *admin key* from the Manual Monitor Control configuration.

Command mode: Global configuration

show failover trigger <1-8>

Displays the current Failover settings.

Command mode: All

Hot Links Configuration

Use these commands to configure Hot Links. For more information about Hot Links, see “Hot Links” in the *BLADEOS 6.6 Application Guide*.

Table 218 Hot Links Configuration Options

Command Syntax and Usage

[no] hotlinks bpdu

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 `off`. This feature can prevent unintentional loop scenarios (for example, if two uplinks come up at the same time).

The default setting is `disabled`.

Command mode: Global configuration

[no] hotlinks fdb-update

Enables or disables FDB Update, which allows the switch to send FDB and MAC update packets over the active interface.

The default value is `disabled`.

Command mode: Global configuration

hotlinks fdb-update-rate <10-1000>

Configures the FDB Update rate, in packets per second.

Command mode: Global configuration

hotlinks enable

Globally enables Hot Links.

Command mode: Global configuration

no hotlinks enable

Globally disables Hot Links.

Command mode: Global configuration

show hotlinks

Displays current Hot Links parameters.

Command mode: All

Hot Links Trigger Configuration

Table 219 Hot Links Trigger Configuration Options

Command Syntax and Usage

hotlinks trigger <1-25> **forward-delay** <0-3600>

Configures the Forward Delay interval, in seconds. The default value is 1.

Command mode: Global configuration

[no] hotlinks trigger <1-25> **name** <1-32 characters>

Defines a name for the Hot Links trigger.

Command mode: Global configuration

[no] hotlinks trigger <1-25> **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 <1-25> **enable**

Enables or disables the Hot Links trigger.

Command mode: Global configuration

no hotlinks trigger <1-25>

Deletes the Hot Links trigger.

Command mode: Global configuration

show hotlinks trigger <1-25>

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 220 Hot Links Master Configuration Options

Command Syntax and Usage

[no] hotlinks trigger <1-25> master port <port alias or number>

Adds or removes the selected port to the Hot Links Master interface.

Command mode: Global configuration

[no] hotlinks trigger <1-25> master portchannel <trunk group number>

Adds or removes the selected trunk group to the Master interface.

Command mode: Global configuration

[no] hotlinks trigger <1-25> master adminkey <0-65535>

Adds or removes an LACP *admin key* to the Master interface. LACP trunks formed with this *admin key* will be included in the Master interface.

Command mode: Global configuration

show hotlinks trigger <1-25>

Displays the current Hot Links trigger settings.

Command mode: All

Hot Links Backup Configuration

Use the following commands to configure the Hot Links Backup interface.

Table 221 Hot Links Backup Configuration Options

Command Syntax and Usage

[no] hotlinks trigger <1-25> backup port <port alias or number>

Adds or removes the selected port to the Hot Links Backup interface.

Command mode: Global configuration

[no] hotlinks trigger <1-25> backup portchannel <trunk group number>

Adds or removes the selected trunk group to the Backup interface.

Command mode: Global configuration

[no] hotlinks trigger <1-25> backup adminkey <0-65535>

Adds or removes an LACP *admin key* to the Backup interface. LACP trunks formed with this *admin key* will be included in the Backup interface.

Command mode: Global configuration

show hotlinks trigger <1-25>

Displays the current Hot Links trigger settings.

Command mode: All

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. All ports are members of VLAN 1 by default. Up to 2048 VLANs can be configured on the G8264.

VLANs can be assigned any number between 1 and 4094. VLAN 4095 is reserved for switch management.

Table 222 VLAN Configuration Options

Command Syntax and Usage

vlan <VLAN number>

Enter VLAN configuration mode.

Command mode: Global configuration

name <1-32 characters>

Assigns a name to the VLAN or changes the existing name. The default VLAN name is the first one.

Command mode: VLAN

stg <STG number>

Assigns a VLAN to a Spanning Tree Group.

Command mode: VLAN

[no] vmap <1-256> [**serverports** | **non-serverports**]

Adds or removes a VLAN Map to the VLAN membership. You can choose to limit operation of the VLAN Map to server ports only or non-server ports only. If you do not select a port type, the VMAP is applied to the entire VLAN.

Command mode: VLAN

member <port alias or number>

Adds port(s) to the VLAN membership.

Command mode: VLAN

no member <port alias or number>

Removes port(s) from this VLAN.

Command mode: VLAN

Table 222 VLAN Configuration Options

Command Syntax and Usage

enable

Enables this VLAN.

Command mode: VLAN

no enable

Disables this VLAN without removing it from the configuration.

Command mode: VLAN

no vlan <VLAN number>

Deletes this VLAN.

Command mode: VLAN

show vlan information

Displays the current VLAN configuration.

Command mode: All

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 223 Protocol VLAN Configuration Options

Command Syntax and Usage

protocol-vlan <1-8> **frame-type** {ether2|llc|snap} <Ethernet type>

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).

Command mode: VLAN

protocol-vlan <1-8> **protocol** <protocol type>

Selects a pre-defined protocol, as follows:

- 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

Command mode: VLAN

protocol-vlan <1-8> **priority** <0-7>

Configures the priority value for this PVLAN.

Command mode: VLAN

protocol-vlan <1-8> **member** <port alias or number>

Adds a port to the selected PVLAN.

Command mode: VLAN

Table 223 Protocol VLAN Configuration Options

Command Syntax and Usage

no protocol-vlan <1-8> **member** <port alias or number>

Removes a port from the selected PVLAN.

Command mode: VLAN

[**no**] **protocol-vlan** <1-8> **tag-pvlan** <port alias or number>

Defines a port that will be tagged by the selected protocol on this VLAN.

Command mode: VLAN

protocol-vlan <1-8> **enable**

Enables the selected protocol on the VLAN.

Command mode: VLAN

no protocol-vlan <1-8> **enable**

Disables the selected protocol on the VLAN.

Command mode: VLAN

no protocol-vlan <1-8>

Deletes the selected protocol configuration from the VLAN.

Command mode: VLAN

show protocol-vlan <1-8>

Displays current parameters for the selected PVLAN.

Command mode: All

Private VLAN Configuration

Use the following commands to configure Private VLANs.

Table 224 Private VLAN Options

Command Syntax and Usage

private-vlan type primary

Configures the VLAN type as a Primary VLAN.

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.

Command mode: VLAN

private-vlan type community

Configures the VLAN type as a community VLAN.

Community VLANs carry upstream traffic from host ports. A Private VLAN may have multiple community VLANs.

Command mode: VLAN

private-vlan type isolated

Configures the VLAN type as an isolated VLAN.

The isolated VLAN carries unidirectional traffic from host ports. A Private VLAN may have only one isolated VLAN.

Command mode: VLAN

no private-vlan type

Clears the private-VLAN type.

Command mode: VLAN

[no] private-vlan map [<2-4094>]

Configures Private VLAN mapping between a secondary VLAN and a primary VLAN. Enter the primary VLAN ID. Secondary VLANs have the *type* defined as *isolated* or *community*. Use the **no** form to remove the mapping between the secondary VLAN and the primary VLAN.

Command mode: VLAN

Table 224 Private VLAN Options

Command Syntax and Usage

private-vlan enable

Enables the private VLAN.

Command mode: VLAN

no private-vlan enable

Disables the Private VLAN.

Command mode: VLAN

show private-vlan [<2-4094>]

Displays current parameters for the selected Private VLAN(s).

Command mode: VLAN

Layer 3 Configuration

The following table describes basic Layer 3 Configuration commands. The following sections provide more detailed information and commands.

Table 225 Layer 3 Configuration Commands

Command Syntax and Usage

interface ip <interface number>

Configures the IP Interface. The G8264 supports up to 128 IP interfaces. However, IP interface 127 and 128 are reserved for switch management. To view command options, see [page 357](#).

Command mode: Global configuration

route-map {<1-32>}

Enters IP Route Map mode. To view command options, see [page 370](#).

Command mode: Global configuration

router rip

Enters the Routing Interface Protocol (RIP) configuration mode. To view command options, see [page 374](#).

Command mode: Global configuration

router ospf

Enters OSPF configuration mode. To view command options, see [page 378](#).

Command mode: Global configuration

ipv6 router ospf

Enters OSPFv3 configuration mode. To view command options, see [page 390](#).

Command mode: Global configuration

router bgp

Enters Border Gateway Protocol (BGP) configuration mode. To view command options, see [page 403](#).

Command mode: Global configuration

Table 225 Layer 3 Configuration Commands

Command Syntax and Usage

router vrrp

Enters Virtual Router Redundancy (VRRP) configuration mode. To view command options, see [page 427](#).

Command mode: Global configuration

ip pim component <1-2>

Enters Protocol Independent Multicast (PIM) component configuration mode. To view command options, see [page 437](#).

Command mode: Global configuration

ip router-id <IP address>

Sets the router ID.

Command mode: Global configuration

show layer3

Displays the current IP configuration.

Command mode: All

IP Interface Configuration

The G8264 supports up to 128 IP interfaces. Each IP interface represents the G8264 on an IP subnet on your network. The Interface option is disabled by default.

Interface 128 is reserved for switch management.

Table 226 IP Interface Configuration Options

Command Syntax and Usage

interface ip <interface number>

Enter IP interface mode.

Command mode: Global configuration

ip address <IP address> [<IP netmask>]

Configures the IP address of the switch interface, using dotted decimal notation.

Command mode: Interface IP

ip netmask <IP netmask>

Configures the IP subnet address mask for the interface, using dotted decimal notation.

Command mode: Interface IP

ipv6 address <IP address (such as 3001:0:0:0:0:abcd:12)>
[anycast | enable | no enable]

Configures the IPv6 address of the switch interface, using hexadecimal format with colons.

Command mode: Interface IP

ipv6 secaddr6 address <IP address (such as 3001:0:0:0:0:abcd:12)>
<prefix length> [anycast]

Configures the secondary IPv6 address of the switch interface, using hexadecimal format with colons.

Command mode: Interface IP

ipv6 prefixlen <IPv6 prefix length (1-128)>

Configures the subnet IPv6 prefix length. The default value is 0 (zero).

Command mode: Interface IP

Table 226 IP Interface Configuration Options

Command Syntax and Usage

vlan <VLAN number>

Configures the VLAN number for this interface. Each interface can belong to one VLAN.

IPv4: Each VLAN can contain multiple IPv4 interfaces.

IPv6: Each VLAN can contain only one IPv6 interface.

Command mode: Interface IP

[no] relay

Enables or disables the BOOTP relay on this interface. The default setting is enabled.

Command mode: Interface IP

[no] ip6host

Enables or disables the IPv6 Host Mode on this interface. The default setting is disabled for data interfaces, and enabled for the management interface.

Command mode: Interface IP

[no] ipv6 unreachable

Enables or disables sending of ICMP Unreachable messages. The default setting is enabled.

Command mode: Interface IP

enable

Enables this IP interface.

Command mode: Interface IP

no enable

Disables this IP interface.

Command mode: Interface IP

Table 226 IP Interface Configuration Options

Command Syntax and Usage

no interface ip <interface number>

Removes this IP interface.

Command mode: Interface IP

show interface ip <interface number>

Displays the current interface settings.

Command mode: All

IPv6 Neighbor Discovery Configuration

The following table describes the IPv6 Neighbor Discovery Configuration commands.

Table 227 IPv6 Neighbor Discovery Configuration Options

Command Syntax and Usage

[no] ipv6 nd suppress-raEnables or disables IPv6 Router Advertisements on the interface. The default setting is `disabled` (suppress Router Advertisements).**Command mode:** Interface IP

[no] ipv6 nd managed-config

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`.**Command mode:** Interface IP

[no] ipv6 nd other-configEnables or disables the other stateful configuration flag, which allows the interface to use DHCP for other stateful configuration. The default setting is `disabled`.**Command mode:** Interface IP

Table 227 IPv6 Neighbor Discovery Configuration Options

Command Syntax and Usage

ipv6 nd ra-lifetime <0-9000>

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.

Command mode: Interface IP

[no] ipv6 nd dad-attempts <1-10>

Configures the maximum number of duplicate address detection attempts.

The default value is 1.

Command mode: Interface IP

[no] ipv6 nd reachable-time <1-3600>**[no] ipv6 nd reachable-time** <1-3600000> **ms**

Configures the advertised reachability time, in seconds or milliseconds (ms). The default value is 30 seconds.

Command mode: Interface IP

[no] ipv6 nd ra-interval <4-1800>

Configures the Router Advertisement maximum interval. The default value is 600 seconds.

Note: Set the maximum RA interval to a value greater than or equal to 4/3 of the minimum RA interval.

Command mode: Interface IP

[no] ipv6 nd ra-intervalmin <3-1800>

Configures the Router Advertisement minimum interval. The default value is 198 seconds.

Note: Set the minimum RA interval to a value less than or equal to 0.75 of the maximum RA interval.

Command mode: Interface IP

[no] ipv6 nd retransmit-time <0-4294967>**[no] ipv6 nd retransmit-time** <0-4294967295> **ms**

Configures the Router Advertisement re-transmit timer, in seconds or milliseconds (ms). The default value is 1 second.

Command mode: Interface IP

Table 227 IPv6 Neighbor Discovery Configuration Options

Command Syntax and Usage

[no] ipv6 nd hops-limit <0-255>

Configures the Router Advertisement hop limit.

The default value is 64.

Command mode: Interface IP

[no] ipv6 nd advmtu

Enables or disables the MTU option in Router Advertisements. The default setting is enabled.

Command mode: Interface IP

Default Gateway Configuration

The switch can be configured with up to four IPv4 gateways, as follows:

- Gateway 1, 2 and 3: data traffic
- Gateway 4: Management traffic

This option is disabled by default.

Table 228 IPv4 Default Gateway Options

Command Syntax and Usage

ip gateway <1-4> **address** <IP address>

Configures the IP address of the default IP gateway using dotted decimal notation.

Command mode: Global configuration

ip gateway <1-4> **interval** <0-60>

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

ip gateway <1-4> **retry** <1-120>

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

Table 228 IPv4 Default Gateway Options

Command Syntax and Usage

[no] ip gateway <1-4> arp-health-check

Enables or disables Address Resolution Protocol (ARP) health checks. The default setting is **disabled**. The **arp** option does not apply to management gateways.

Command mode: Global configuration

ip gateway <1-4> enable

Enables the gateway for use.

Command mode: Global configuration

no ip gateway <1-4> enable

Disables the gateway.

Command mode: Global configuration

no ip gateway <1-4>

Deletes the gateway from the configuration.

Command mode: Global configuration

show ip gateway <1-4>

Displays the current gateway settings.

Command mode: All

IPv4 Static Route Configuration

Up to 128 IPv4 static routes can be configured.

Table 229 IPv4 Static Route Configuration Options

Command Syntax and Usage

ip route *<IP subnet>* *<IP netmask>* *<IP nexthop>* [*<interface number>*]

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

no ip route *<IP subnet>* *<IP netmask>* [*<interface number>*]

Removes a static route. The destination address of the route to remove must be specified using dotted decimal notation.

Command mode: Global configuration

no ip route destination-address *<IP address>*

Clears all IP static routes with this destination.

Command mode: Global configuration

no ip route gateway *<IP address>*

Clears all IP static routes that use this gateway.

Command mode: Global configuration

ip route ecmphash [**dipsip**][**sip**]

Configures ECMP hashing parameters. You may choose one or more of the following parameters:

- dipsip**: Destination IP and source IP address
- sip**: Source IP address

Command mode: Global configuration

ip route interval *<1-60>*

Configures the ECMP health-check ping interval, in seconds. The default value is 1 second.

Command mode: Global configuration

ip route retries *<1-60>*

Configures the number of ECMP health-check retries. The default value is 3.

Command mode: Global configuration

Table 229 IPv4 Static Route Configuration Options

Command Syntax and Usage

[no] ip route healthcheck

Enables or disables static route health checks. The default setting is disabled.

Command mode: Global configuration

show ip route static

Displays the current IP static routes.

Command mode: All

IP Multicast Route Configuration

The following table describes the IP Multicast (IPMC) route commands. Before you can add an IPMC route, IGMP must be turned on, IGMP Snooping must be enabled, and the required VLANs must be added to IGMP Snooping.

Table 230 IP Multicast Route Configuration Commands

Command Syntax and Usage

ip mroute <IPMC destination> <VLAN number> <port alias or number>]
 [(p)ri:m:ary:(b)ackup:(h)ost] [<VR ID>]

Adds a static multicast route. The destination address, VLAN, and member port of the route must be specified.

Command mode: Global configuration

no ip mroute <IPMC destination> <VLAN number> <port alias or number>
 [(p)ri:m:ary:(b)ackup:(h)ost] [<VR ID>]

Removes a static multicast route. The destination address, VLAN, and member port of the route to remove must be specified.

Command mode: Global configuration

ip mroute <IP address> <VLAN number> **portchannel** <trunk group number>
 [(p)ri:m:ary:(b)ackup:(h)ost] [<VR ID>]

Adds a static multicast route. The destination address, VLAN, and member trunk group of the route must be specified.

Command mode: Global configuration

no ip mroute <IP address> <VLAN number> **portchannel** <trunk group number>
 [(p)ri:m:ary:(b)ackup:(h)ost] [<VR ID>]

Removes a static multicast route. The destination address, VLAN, and member trunk group of the route to remove must be specified.

Command mode: Global configuration

ip mroute <IP address> <VLAN number> **adminkey** <1-65535>
 [(p)ri:m:ary:(b)ackup:(h)ost] [<VR ID>]

Adds a static multicast route. The destination address, VLAN, and LACP *admin key* of the route must be specified.

Command mode: Global configuration

Table 230 IP Multicast Route Configuration Commands**Command Syntax and Usage**

```
no ip mroute <IP address> <VLAN number> adminkey <1-65535>
  [(p)rietary:(b)ackup:(h)ost] [<VR ID>]
```

Removes a static multicast route. The destination address, VLAN, and LACP *admin key* of the route to remove must be specified.

Command mode: Global configuration

```
show ip mroute
```

Displays the current IP multicast routes.

Command mode: All except User EXEC

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 231 ARP Configuration Options**Command Syntax and Usage**

```
ip arp rearp <2-120>
```

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. The default value is 5 minutes.

Command mode: Global configuration

```
show ip arp
```

Displays the current ARP configurations.

Command mode: All except User EXEC

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 232 ARP Static Configuration Options

Command Syntax and Usage

ip arp <IP address> <MAC address> **vlan** <vlan number>
port <port alias or number>

Adds a permanent ARP entry.

Command mode: Global configuration

no ip arp <IP address>

Deletes a permanent ARP entry.

Command mode: Global configuration

no ip arp all

Deletes all static ARP entries.

Command mode: Global configuration

show ip arp static

Displays current static ARP configuration.

Command mode: All

IP Forwarding Configuration

Table 233 IP Forwarding Configuration Options

Command Syntax and Usage

[no] ip routing directed-broadcasts

Enables or disables forwarding directed broadcasts. The default setting is disabled.

Command mode: Global configuration

[no] ip routing no-icmp-redirect

Enables or disables ICMP re-directs. The default setting is disabled.

Command mode: Global configuration

[no] ip routing icmp6-redirect

Enables or disables IPv6 ICMP re-directs. The default setting is disabled.

Command mode: Global configuration

ip routing

Enables IP forwarding (routing) on the G8264. Forwarding is turned on by default.

Command mode: Global configuration

no ip routing

Disables IP forwarding (routing) on the G8264.

Command mode: Global configuration

show ip routing

Displays the current IP forwarding settings.

Command mode: All except User EXEC

Network Filter Configuration

Table 234 IP Network Filter Configuration Options

Command Syntax and Usage

ip match-address <1-256> <IP address> <IP netmask>

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

Command mode: Global configuration.

ip match-address <1-256> **enable**

Enables the Network Filter configuration.

Command mode: Global configuration

no ip match-address <1-256> **enable**

Disables the Network Filter configuration.

Command mode: Global configuration

no ip match-address <1-256>

Deletes the Network Filter configuration.

Command mode: Global configuration

show ip match-address [<1-256>]

Displays the current the Network Filter configuration.

Command mode: All except User EXEC

Routing Map Configuration

Note – The *map number* (1-64) represents the routing map you wish to configure.

Routing maps control and modify routing information.

Table 235 Routing Map Configuration Options

Command Syntax and Usage

route-map <1-64>

Enter route map configuration mode.

Command mode: Global configuration

[no] **access-list** <1-8>

Configures the Access List.

Command mode: Route map

For more information, see [page 372](#).

[no] **as-path-list** <1-8>

Configures the Autonomous System (AS) Filter.

Command mode: Route map

For more information, see [page 373](#).

[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

Table 235 Routing Map Configuration Options

Command Syntax and Usage

[no] metric-type {1|2}

Assigns the type of OSPF metric. The default is type 1.

- 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

[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 <1-64>

Deletes the route map.

Command mode: Route map

show route-map [<1-64>]

Displays the current route configuration.

Command mode: All except User EXEC

IP Access List Configuration

Note – The *route map number* (1-64) and the *access list number* (1-8) represent the IP access list you wish to configure.

Table 236 IP Access List Configuration Options

Command Syntax and Usage

[no] access-list <1-8> match-address <1-256>

Sets the network filter number.

Command mode: Route map

See “[Network Filter Configuration](#)” on page 369 for details.

[no] access-list <1-8> metric <1-4294967294>

Sets the metric value in the AS-External (ASE) LSA.

Command mode: Route map

access-list <1-8> action {permit|deny}

Permits or denies action for the access list.

Command mode: Route map

access-list <1-8> enable

Enables the access list.

Command mode: Route map

no access-list <1-8> enable

Disables the access list.

Command mode: Route map

no access-list <1-8>

Deletes the access list.

Command mode: Route map

show route-map <1-64> access-list <1-8>

Displays the current Access List configuration.

Command mode: All

Autonomous System Filter Path Configuration

Note – The *rmap number* and the *path number* represent the AS path you wish to configure.

Table 237 AS Filter Configuration Options

Command Syntax and Usage

as-path-list <1-8> **as-path** <1-65535>

Sets the Autonomous System filter's path number.

Command mode: Route map

as-path-list <1-8> **action** {**permit** | **deny**}

Permits or denies Autonomous System filter action.

Command mode: Route map

as-path-list <1-8> **enable**

Enables the Autonomous System filter.

Command mode: Route map

no as-path-list <1-8> **enable**

Disables the Autonomous System filter.

Command mode: Route map

no as-path-list <1-8>

Deletes the Autonomous System filter.

Command mode: Route map

show route-map <1-64> **as-path-list** <1-8>

Displays the current Autonomous System filter configuration.

Command mode: All

Routing Information Protocol Configuration

RIP commands are used for configuring Routing Information Protocol parameters. This option is turned off by default.

Table 238 Routing Information Protocol Options

Command Syntax and Usage

router rip

Enter Router RIP configuration mode.

Command mode: Router RIP

timers update <1-120>

Configures the time interval for sending for RIP table updates, in seconds.
The default value is 30 seconds.

Command mode: Router RIP

enable

Globally turns RIP **on**.

Command mode: Router RIP

no enable

Globally turns RIP **off**.

Command mode: Router RIP

show ip rip

Displays the current RIP configuration.

Command mode: All except User EXEC

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 239 RIP Interface Options

Command Syntax and Usage

ip rip version {1|2|both}

Configures the RIP version used by this interface. The default value is version 2.

Command mode: Interface IP

[no] **ip rip supply**

When enabled, the switch supplies routes to other routers. The default value is enabled.

Command mode: Interface IP

[no] **ip rip listen**

When enabled, the switch learns routes from other routers. The default value is enabled.

Command mode: Interface IP

[no] **ip rip poison**

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

[no] **ip rip split-horizon**

Enables or disables split horizon. The default value is **enabled**.

Command mode: Interface IP

[no] **ip rip triggered**

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

Table 239 RIP Interface Options

Command Syntax and Usage

[no] ip rip multicast-updates

Enables or disables multicast updates of the routing table (using address 224.0.0.9). The default value is enabled.

Command mode: Interface IP

[no] ip rip default-action {listen|supply|both}

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

[no] ip rip metric [<1-15>]

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 [<password>]

Configures the authentication type. The default is none.

Command mode: Interface IP

[no] ip rip authentication key <password>

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 <interface number> rip

Displays the current RIP configuration.

Command mode: All

RIP Route Redistribution Configuration

The following table describes the RIP Route Redistribution commands.

Table 240 RIP Redistribution Options

Command Syntax and Usage

redistribute {**fixed**|**static**|**ospf**|**eospf**|**ebgp**|**ibgp**} <I-32>

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 **all**.

The routes of the redistribution protocol matched by the route maps in the route redistribution list will be redistributed.

Command mode: Router RIP

no redistribute {**fixed**|**static**|**ospf**|**eospf**|**ebgp**|**ibgp**} <I-32>

Removes the route map from the RIP route redistribution list.

To remove specific route maps, enter routing map numbers, separated by a comma (,). To remove all 32 route maps, type **all**.

Command mode: Router RIP

redistribute {**fixed**|**static**|**ospf**|**eospf**|**ebgp**|**ibgp**} **export** <I-15>

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 **none**.

Command mode: Router RIP

show ip rip redistribute

Displays the current RIP route redistribute configuration.

Command mode: All

Open Shortest Path First Configuration

Table 241 OSPF Configuration Options

Command Syntax and Usage

router ospf

Enter Router OSPF configuration mode.

Command mode: Global configuration

area-range <1-16>

Configures summary routes for up to 16 IP addresses. See [page 382](#) to view command options.

Command mode: Router OSPF

ip ospf <interface number>

Configures the OSPF interface. See [page 383](#) to view command options.

Command mode: Interface IP

area-virtual-link <1-3>

Configures the Virtual Links used to configure OSPF for a Virtual Link. See [page 386](#) to view command options.

Command mode: Router OSPF

message-digest-key <1-255> **md5-key** <text string>

Assigns a string to MD5 authentication key.

Command mode: Router OSPF

host <1-128>

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 388](#) to view command options.

Command mode: Router OSPF

lsdb-limit <LSDB limit (0-27648, 0 for no limit)>

Sets the link state database limit.

Command mode: Router OSPF

Table 241 OSPF Configuration Options

Command Syntax and Usage

[no] default-information <1-16777214> {<AS value (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 G8264.

Command mode: Router OSPF

no enable

Disables OSPF on the G8264.

Command mode: Router OSPF

show ip ospf

Displays the current OSPF configuration settings.

Command mode: All except User EXEC

Area Index Configuration

Table 242 Area Index Configuration Options

Command Syntax and Usage

area <0-5> **area-id** <IP address>

Defines the IP address of the OSPF area number.

Command mode: Router OSPF

area <0-5> **type** {**transit** | **stub** | **nssa**}

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.

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.

Stub area: is an area where external routing information is not distributed. Typically, a stub area is connected to only one other area.

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.

Command mode: Router OSPF

area <0-5> **stub-metric** <1-65535>

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.

Metric value assigns the priority for choosing the switch for default route. Metric type determines the method for influencing routing decisions for external routes.

Command mode: Router OSPF

[no] **area** <0-5> **authentication-type** {**password** | **md5**}

None: No authentication required.

Password: Authenticates simple passwords so that only trusted routing devices can participate.

MD5: This parameter is used when MD5 cryptographic authentication is required.

Command mode: Router OSPF

Table 242 Area Index Configuration Options

Command Syntax and Usage

area <0-5> **spf-interval** <1-255>

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.

Command mode: Router OSPF

area <0-5> **enable**

Enables the OSPF area.

Command mode: Router OSPF

no area <0-5> **enable**

Disables the OSPF area.

Command mode: Router OSPF

no area <0-5>

Deletes the OSPF area.

Command mode: Router OSPF

show ip ospf area <0-5>

Displays the current OSPF configuration.

Command mode: All except User EXEC

OSPF Summary Range Configuration

Table 243 OSPF Summary Range Configuration Options

Command Syntax and Usage

area-range <1-16> **address** <IP address> <IP netmask>

Displays the base IP address or the IP address mask for the range.

Command mode: Router OSPF

area-range <1-16> **area** <0-5>

Displays the area index used by the G8264.

Command mode: Router OSPF

[no] **area-range** <1-16> **hide**

Hides the OSPF summary range.

Command mode: Router OSPF

area-range <1-16> **enable**

Enables the OSPF summary range.

Command mode: Router OSPF

no area-range <1-16> **enable**

Disables the OSPF summary range.

Command mode: Router OSPF

no area-range <1-16>

Deletes the OSPF summary range.

Command mode: Router OSPF

show ip ospf area-range <1-16>

Displays the current OSPF summary range.

Command mode: Router OSPF

OSPF Interface Configuration

Table 244 OSPF Interface Configuration Options

Command Syntax and Usage

ip ospf area <0-5>

Configures the OSPF area index.

Command mode: Interface IP

ip ospf priority <0-255>

Configures the priority value for the G8264'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).

Command mode: Interface IP

ip ospf cost <1-65535>

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.

Command mode: Interface IP

ip ospf hello-interval <1-65535>

ip ospf hello-interval <50-65535ms>

Configures the interval, in seconds or milliseconds, between the hello packets for the interfaces.

Command mode: Interface IP

ip ospf dead-interval <1-65535>

ip ospf dead-interval <1000-65535ms>

Configures the health parameters of a hello packet, in seconds or milliseconds, before declaring a silent router to be down.

Command mode: Interface IP

ip ospf transit-delay <1-3600>

Configures the transit delay in seconds.

Command mode: Interface IP

Table 244 OSPF Interface Configuration Options

Command Syntax and Usage

ip ospf retransmit-interval <1-3600>

Configures the retransmit interval in seconds.

Command mode: Interface IP

[no] ip ospf key <key string>

Sets the authentication key to clear the password.

Command mode: Interface IP

[no] ip ospf message-digest-key <1-255>

Assigns an MD5 key to the interface.

Command mode: Interface IP

[no] ip ospf passive-interface

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.

Command mode: Interface IP

[no] ip ospf point-to-point

Sets the interface as point-to-point.

Command mode: Interface IP

ip ospf enable

Enables OSPF interface.

Command mode: Interface IP

no ip ospf enable

Disables OSPF interface.

Command mode: Interface IP

Table 244 OSPF Interface Configuration Options

Command Syntax and Usage

no ip ospf

Deletes the OSPF interface.

Command mode: Interface IP

show interface ip *<interface number>* **ospf**

Displays the current settings for OSPF interface.

Command mode: All except User EXEC

OSPF Virtual Link Configuration

Table 245 OSPF Virtual Link Configuration Options

Command Syntax and Usage

area-virtual-link <1-3> **area** <0-5>

Configures the OSPF area index for the virtual link.

Command mode: Router OSPF

area-virtual-link <1-3> **hello-interval** <1-65535>
area-virtual-link <1-3> **hello-interval** <50-65535ms>

Configures the authentication parameters of a hello packet, in seconds or milliseconds. The default value is 10 seconds.

Command mode: Router OSPF

area-virtual-link <1-3> **dead-interval** <1-65535>
area-virtual-link <1-3> **dead-interval** <1000-65535ms>

Configures the health parameters of a hello packet, in seconds or milliseconds. The default value is 60 seconds.

Command mode: Router OSPF

area-virtual-link <1-3> **transit-delay** <1-3600>

Configures the delay in transit, in seconds. The default value is one second.

Command mode: Router OSPF

area-virtual-link <1-3> **retransmit-interval** <1-3600>

Configures the retransmit interval, in seconds. The default value is five seconds.

Command mode: Router OSPF

area-virtual-link <1-3> **neighbor-router** <IP address>

Configures the router ID of the virtual neighbor. The default value is 0.0.0.0.

Command mode: Router OSPF

[no] **area-virtual-link** <1-3> **key** <password>

Configures the password (up to eight characters) for each virtual link. The default setting is none.

Command mode: Router OSPF

Table 245 OSPF Virtual Link Configuration Options

Command Syntax and Usage

area-virtual-link <1-3> **message-digest-key** <1-255>

Sets MD5 key ID for each virtual link. The default setting is none.

Command mode: Router OSPF

area-virtual-link <1-3> **enable**

Enables OSPF virtual link.

Command mode: Router OSPF

no area-virtual-link <1-3> **enable**

Disables OSPF virtual link.

Command mode: Router OSPF

no area-virtual-link <1-3>

Deletes OSPF virtual link.

Command mode: Router OSPF

show ip ospf area-virtual-link <1-3>

Displays the current OSPF virtual link settings.

Command mode: All except User EXEC

OSPF Host Entry Configuration

Table 246 OSPF Host Entry Configuration Options

Command Syntax and Usage

host <1-128> **address** <IP address>

Configures the base IP address for the host entry.

Command mode: Router OSPF

host <1-128> **area** <0-5>

Configures the area index of the host.

Command mode: Router OSPF

host <1-128> **cost** <1-65535>

Configures the cost value of the host.

Command mode: Router OSPF

host <1-128> **enable**

Enables OSPF host entry.

Command mode: Router OSPF

no host <1-128> **enable**

Disables OSPF host entry.

Command mode: Router OSPF

no host <1-128>

Deletes OSPF host entry.

Command mode: Router OSPF

show ip ospf host <1-128>

Displays the current OSPF host entries.

Command mode: All except User EXEC

OSPF Route Redistribution Configuration.

Table 247 OSPF Route Redistribution Configuration Options

Command Syntax and Usage

redistribute {**fixed**|**static**|**rip**} <*rmap ID (1-32)*>

Adds selected routing map to the rmap list.

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.

Command mode: Router OSPF

no redistribute {**fixed**|**static**|**rip**} <*rmap ID (1-32)*>

Removes the route map from the route redistribution list.

Removes routing maps from the rmap list.

Command mode: Router OSPF

[no] redistribute {**fixed**|**static**|**rip**} **export metric**
<*1-16777214*> **metric-type** {**type1**|**type2**}

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.

Command mode: Router OSPF

show ip ospf redistribute

Displays the current route map settings.

Command mode: All except User EXEC

OSPF MD5 Key Configuration

Table 248 OSPF MD5 Key Options

Command Syntax and Usage

message-digest-key <1-255> **md5-key** <1-16 characters>

Sets the authentication key for this OSPF packet.

Command mode: Router OSPF

no message-digest-key <1-255>

Deletes the authentication key for this OSPF packet.

Command mode: Router OSPF

show ip ospf message-digest-key <1-255>

Displays the current MD5 key configuration.

Command mode: All except User EXEC

Open Shortest Path First Version 3 Configuration

Table 249 OSPFv3 Configuration Options

Command Syntax and Usage

[no] ipv6 router ospf

Enter OSPFv3 configuration mode. Enables or disables OSPFv3 routing protocol.

Command mode: Global configuration

abr-type [**standard**|**cisco**|**ibm**]

Configures the Area Border Router (ABR) type, as follows:

- Standard
- Cisco
- IBM

The default setting is `standard`.

Command mode: Router OSPF3

as-external lsdb-limit <LSDB limit (0-2147483647, -1 for no limit)>

Sets the link state database limit.

Command mode: Router OSPF3

Table 249 OSPFv3 Configuration Options

Command Syntax and Usage

exit-overflow-interval <0-4294967295>

Configures the number of seconds that a router takes to exit Overflow State. The default value is 0 (zero).

Command mode: Router OSPF3

reference-bandwidth <0-4294967295>

Configures the reference bandwidth, in kilobits per second, used to calculate the default interface metric. The default value is 100,000.

Command mode: Router OSPF3

timers spf {<SPF delay (0-65535)>} {<SPF hold time (0-65535)>}

Configures the number of seconds that SPF calculation is delayed after a topology change message is received. The default value is 5.

Configures the number of seconds between SPF calculations. The default value is 10.

Command mode: Router OSPF3

router-id <IPv4 address>

Defines the router ID.

Command mode: Router OSPF3

[no] nssaAsbrDfRtTrans

Enables or disables setting of the P-bit in the default Type 7 LSA generated by an NSSA internal ASBR. The default setting is disabled.

Command mode: Router OSPF3

enable

Enables OSPFv3 on the switch.

Command mode: Router OSPF3

Table 249 OSPFv3 Configuration Options

Command Syntax and Usage

no enable

Disables OSPFv3 on the switch.

Command mode: Router OSPF3

show ipv6 ospf

Displays the current OSPF configuration settings.

Command mode: All

OSPFv3 Area Index Configuration**Table 250** OSPFv3 Area Index Configuration Options

Command Syntax and Usage

area <area index> **area-id** <IP address>

Defines the IP address of the OSPFv3 area number.

Command mode: Router OSPF3

area <area index> **type** {transit|stub|nssa} {no-summary}

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.

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.

Stub area: is an area where external routing information is not distributed. Typically, a stub area is connected to only one other area.

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.

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.

The default setting is disabled.

Command mode: Router OSPF3

Table 250 OSPFv3 Area Index Configuration Options

Command Syntax and Usage

area <area index> **default-metric** <metric value (1-16777215)>

Configures the cost for the default summary route in a stub area or NSSA.

Command mode: Router OSPF3

area <area index> **default-metric type** <1-3>

Configures the default metric type applied to the route.

This command applies only to area type of Stub/NSSA.

Command mode: Router OSPF3

area <area index> **stability-interval** <1-255>

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.

Command mode: Router OSPF3

area <area index> **translation-role** **always**|**candidate**

Configures the translation role for an NSSA area, as follows:

- Always: Type 7 LSAs are always translated into Type 5 LSAs.
- Candidate: An NSSA border router participates in the translator election process.

The default setting is `candidate`.

Command mode: Router OSPF3

area <area index> **enable**

Enables the OSPF area.

Command mode: Router OSPF3

area <area index> **no enable**

Disables the OSPF area.

Command mode: Router OSPF3

Table 250 OSPFv3 Area Index Configuration Options

Command Syntax and Usage

no area <area index>

Deletes the OSPF area.

Command mode: Router OSPF3

show ipv6 ospf areas

Displays the current OSPFv3 area configuration.

Command mode: All

OSPFv3 Summary Range Configuration**Table 251** OSPFv3 Summary Range Configuration Options

Command Syntax and Usage

area-range <1-16> **address** <IPv6 address> <prefix length (1-128)>

Configures the base IPv6 address and subnet prefix length for the range.

Command mode: Router OSPF3

area-range <1-16> **area** <area index (0-2)>

Configures the area index used by the switch.

Command mode: Router OSPF3

area-range <1-16> **lsa-type** **summary**|**Type7**

Configures the LSA type, as follows:

- Summary LSA
- Type7 LSA

Command mode: Router OSPF3

area-range <1-16> **tag** <0-4294967295>

Configures the route tag.

Command mode: Router OSPF3

[no] area-range <1-16> **hide**

Hides the OSPFv3 summary range.

Command mode: Router OSPF3

Table 251 OSPFv3 Summary Range Configuration Options

Command Syntax and Usage

area-range <1-16> **enable**

Enables the OSPFv3 summary range.

Command mode: Router OSPF3

area-range <1-16> **no enable**

Disables the OSPFv3 summary range.

Command mode: Router OSPF3

no area-range <1-16>

Deletes the OSPFv3 summary range.

Command mode: Router OSPF3

show ipv6 ospf area-range

Displays the current OSPFv3 summary range.

Command mode: All

OSPFv3 AS-External Range Configuration**Table 252** OSPFv3 AS_External Range Configuration Options

Command Syntax and Usage

summary-prefix <1-16> **address** <IPv6 address> <IPv6 prefix length (1-128)>

Configures the base IPv6 address and the subnet prefix length for the range.

Command mode: Router OSPF3

summary-prefix <1-16> **area** <area index (0-2)>

Configures the area index used by the switch.

Command mode: Router OSPF3

Table 252 OSPFv3 AS_External Range Configuration Options

Command Syntax and Usage

summary-prefix <1-16> **aggregation-effect** {**allowAll** | **denyAll** | **advertise** | **not-advertise**}

Configures the aggregation effect, as follows:

- ❑ **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.

Command mode: Router OSPF3

[no] summary-prefix <1-16> **translation**

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

summary-prefix <1-16> **enable**

Enables the OSPFv3 AS-external range.

Command mode: Router OSPF3

summary-prefix <1-16> **no enable**

Disables the OSPFv3 AS-external range.

Command mode: Router OSPF3

no summary-prefix <1-16>

Deletes the OSPFv3 AS-external range.

Command mode: Router OSPF3

show ipv6 ospf summary-prefix <1-16>

Displays the current OSPFv3 AS-external range.

Command mode: All

OSPFv3 Interface Configuration

Table 253 OSPFv3 Interface Configuration Options

Command Syntax and Usage

interface ip <interface number>

Enter Interface IP mode, from Global Configuration mode.

Command mode: Global configuration

ipv6 ospf area <area index (0-2)>

Configures the OSPFv3 area index.

Command mode: Interface IP

ipv6 ospf area <area index (0-2)> **instance** <0-255>

Configures the instance ID for the interface.

Command mode: Interface IP

[no] ipv6 ospf priority <priority value (0-255)>

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

[no] ipv6 ospf cost <1-65535>

Configures the metric value for sending a packet on the interface.

Command mode: Interface IP

[no] ipv6 ospf hello-interval <1-65535>

Configures the indicated interval, in seconds, between the hello packets, that the router sends on the interface.

Command mode: Interface IP

[no] ipv6 ospf dead-interval <1-65535>

Configures the time period, in seconds, for which the router waits for hello packet from the neighbor before declaring this neighbor down.

Command mode: Interface IP

Table 253 OSPFv3 Interface Configuration Options

Command Syntax and Usage

[no] ipv6 ospf transmit-delay <1-1800>

Configures the estimated time, in seconds, taken to transmit LS update packet over this interface.

Command mode: Interface IP

[no] ipv6 ospf retransmit-interval <1-1800>

Configures the interval in seconds, between LSA retransmissions for adjacencies belonging to interface.

Command mode: Interface IP

[no] ipv6 ospf passive-interface

Enables or disables the `passive` setting on the interface. On a passive interface, OSPFv3 protocol packets are suppressed.

Command mode: Interface IP

ipv6 ospf enable

Enables OSPFv3 on the interface.

Command mode: Interface IP

ipv6 ospf no enable

Disables OSPFv3 on the interface.

Command mode: Interface IP

no ipv6 ospf

Deletes OSPFv3 from interface.

Command mode: Interface IP

show ipv6 ospf interface

Displays the current settings for OSPFv3 interface.

Command mode: Interface IP

OSPFv3 Virtual Link Configuration

Table 254 OSPFv3 Virtual Link Configuration Options

Command Syntax and Usage

area-virtual-link <1-3> **area** <area index (0-2)>

Configures the OSPF area index.

Command mode: Router OSPF3

area-virtual-link <1-3> **hello-interval** <1-65535>

Configures the indicated interval, in seconds, between the hello packets, that the router sends on the interface.

Command mode: Router OSPF3

area-virtual-link <1-3> **dead-interval** <1-65535>

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 <1-3> **transmit-delay** <1-1800>

Configures the estimated time, in seconds, taken to transmit LS update packet over this interface.

Command mode: Router OSPF3

area-virtual-link <1-3> **retransmit-interval** <1-1800>

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 <1-3> **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 <1-3> **enable**

Enables OSPF virtual link.

Command mode: Router OSPF3

Table 254 OSPFv3 Virtual Link Configuration Options**Command Syntax and Usage****area-virtual-link** <1-3> **no enable**

Disables OSPF virtual link.

Command mode: Router OSPF3**no area-virtual-link** <1-3>

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 255** OSPFv3 Host Entry Configuration Options**Command Syntax and Usage****host** <1-128> **address** <IPv6 address> <prefix length (1-128)>

Configures the base IPv6 address and the subnet prefix length for the host entry.

Command mode: Router OSPF3**host** <1-128> **area** <area index (0-2)>

Configures the area index of the host.

Command mode: Router OSPF3**host** <1-128> **cost** <1-65535>

Configures the cost value of the host.

Command mode: Router OSPF3**host** <1-128> **enable**

Enables the host entry.

Command mode: Router OSPF3

Table 255 OSPFv3 Host Entry Configuration Options**Command Syntax and Usage**

host <I-I28> **no enable**

Disables the host entry.

Command mode: Router OSPF3

no host <I-I28>

Deletes the host entry.

Command mode: Router OSPF3

show ipv6 ospf host [<I-I28>]

Displays the current OSPFv3 host entries.

Command mode: All

OSPFv3 Redist Entry Configuration**Table 256** OSPFv3 Redist Entry Configuration Options**Command Syntax and Usage**

redist-config <I-I28> **address** <IPv6 address> <IPv6 prefix length (I-I28)>

Configures the base IPv6 address and the subnet prefix length for the redistribution entry.

Command mode: Router OSPF3

redist-config <I-I28> **metric-value** <I-16777215>

Configures the route metric value applied to the route before it is advertised into the OSPFv3 domain.

Command mode: Router OSPF3

redist-config <I-I28> **metric-type** asExtttype1|asExtttype2

Configures the metric type applied to the route before it is advertised into the OSPFv3 domain.

Command mode: Router OSPF3

[no] redist-config <I-I28> **tag** <0-4294967295>

Configures the route tag.

Command mode: Router OSPF3

Table 256 OSPFv3 Redist Entry Configuration Options

Command Syntax and Usage

redist-config <1-128> **enable**

Enables the OSPFv3 redistribution entry.

Command mode: Router OSPF3

redist-config <1-128> **no enable**

Disables the OSPFv3 redistribution entry.

Command mode: Router OSPF3

no redist-config <1-128>

Deletes the OSPFv3 redistribution entry.

Command mode: Router OSPF3

show ipv6 ospf redist-config

Displays the current OSPFv3 redistribution configuration entries.

Command mode: Router OSPF3

OSPFv3 Redistribute Configuration

Table 257 OSPFv3 Redistribute Configuration Options

Command Syntax and Usage

[no] redistribute {**connected**|**static**} **export** <metric value (1-16777215)>
<metric type (1-2)> <tag (0-4294967295)>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 **no** form of the command.**Command mode:** Router OSPF3

show ipv6 ospf

Displays the current OSPFv3 route redistribution settings.

Command mode: All

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 BLADEOS implementation, the RackSwitch G8264 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 258 Border Gateway Protocol Options

Command Syntax and Usage

router **bgp**

Enter Router BGP configuration mode.

Command mode: Global configuration

neighbor *<peer number (1-16)>*

Configures each BGP *peer*. Each border router, within an autonomous system, exchanges routing information with routers on other external networks.

To view command options, see [page 405](#).

Command mode: Router BGP

as *<0-65535>*

Set Autonomous System number.

Command mode: Router BGP

Table 258 Border Gateway Protocol Options

Command Syntax and Usage

local-preference <0-4294967294>

Sets the local preference. The path with the higher value is preferred.

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.

Command mode: Router BGP

maximum-paths <0-32>

Set maximum paths allowed for an external route.

By default, BGP will install only one path to the IP routing table.

Command mode: Router BGP

maximum-paths ibgp <0-32>

Set maximum paths allowed for an internal route.

By default, BGP will install only one path to the IP routing table.

Command mode: Router BGP

enable

Globally turns BGP on.

Command mode: Router BGP

no enable

Globally turns BGP off.

Command mode: Router BGP

show ip bgp

Displays the current BGP configuration.

Command mode: All

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 259 BGP Peer Configuration Options

Command Syntax and Usage

neighbor *<peer number>* **remote-address** *<IP address>*

Defines the IP address for the specified peer (border router), using dotted decimal notation. The default address is 0.0.0.0.

Command mode: Router BGP

neighbor *<peer number>* **remote-as** *<1-65535>*

Sets the remote autonomous system number for the specified peer.

Command mode: Router BGP

neighbor *<peer number>* **timers hold-time** *<0, 3-65535>*

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.

Command mode: Router BGP

neighbor *<peer number>* **timers keep-alive** *<0, 1-21845>*

Sets the keep-alive time for the specified peer, in seconds. The default value is 60 seconds.

Command mode: Router BGP

neighbor *<peer number>* **advertisement-interval** *<1-65535>*

Sets time, in seconds, between advertisements. The default value is 60 seconds.

Command mode: Router BGP

neighbor *<peer number>* **retry-interval** *<1-65535>*

Sets connection retry interval, in seconds. The default value is 120 seconds.

Command mode: Router BGP

neighbor *<peer number>* **route-origination-interval** *<1-65535>*

Sets the minimum time between route originations, in seconds. The default value is 15 seconds.

Command mode: Router BGP

Table 259 BGP Peer Configuration Options**Command Syntax and Usage**

```
neighbor <peer number> time-to-live <1-255>
```

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.

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.

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).

Command mode: Router BGP

```
neighbor <peer number> route-map in <1-32>
```

Adds route map into in-route map list.

Command mode: Router BGP

```
neighbor <peer number> route-map out <1-32>
```

Adds route map into out-route map list.

Command mode: Router BGP

```
no neighbor <peer number> route-map in <1-32>
```

Removes route map from in-route map list.

Command mode: Router BGP

```
no neighbor <peer number> route-map out <1-32>
```

Removes route map from out-route map list.

Command mode: Router BGP

```
no neighbor <peer number> shutdown
```

Enables this peer configuration.

Command mode: Router BGP

Table 259 BGP Peer Configuration Options

Command Syntax and Usage

neighbor *<peer number>* **shutdown**

Disables this peer configuration.

Command mode: Router BGP

no neighbor *<peer number>*

Deletes this peer configuration.

Command mode: Router BGP

[no] neighbor *<peer number>* **password** *<1-16 characters>*

Configures the BGP peer password.

Command mode: Router BGP

[no] neighbor *<peer number>* **passive**

Enables or disables BGP passive mode, which prevents the switch from initiating BGP connections with peers.

Instead, the switch waits for the peer to send an open message first.

Command mode: Router BGP

show ip bgp neighbor [*<peer number>*]

Displays the current BGP peer configuration.

Command mode: All

BGP Redistribution Configuration

Table 260 BGP Redistribution Configuration Options

Command Syntax and Usage

[no] neighbor <peer number> redistribute default-metric <1-4294967294>

Sets default metric of advertised routes.

Command mode: Router BGP

**[no] neighbor <peer number> redistribute default-action
{import|originate|redistribute}**

Sets default route action.

Defaults routes can be configured as import, originate, redistribute, or none.

None: No routes are configured

Import: Import these routes.

Originate: The switch sends a default route to peers if it does not have any default routes in its routing table.

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.

Command mode: Router BGP

[no] neighbor <peer number> redistribute rip

Enables or disables advertising RIP routes.

Command mode: Router BGP

[no] neighbor <peer number> redistribute ospf

Enables or disables advertising OSPF routes.

Command mode: Router BGP

[no] neighbor <peer number> redistribute fixed

Enables or disables advertising fixed routes.

Command mode: Router BGP

Table 260 BGP Redistribution Configuration Options

Command Syntax and Usage

[no] neighbor *<peer number>* **redistribute static**

Enables or disables advertising static routes.

Command mode: Router BGP

show ip bgp neighbor *<peer number>* **redistribute**

Displays current redistribution configuration.

Command mode: All except User EXEC

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 261 BGP Aggregation Configuration Options

Command Syntax and Usage

aggregate-address *<1-16>* *<IP address>* *<IP netmask>*

Defines the starting subnet IP address for this aggregation, using dotted decimal notation. The default address is 0.0.0.0.

Command mode: Router BGP

aggregate-address *<1-16>* **enable**

Enables this BGP aggregation.

Command mode: Router BGP

no aggregate-address *<1-16>* **enable**

Disables this BGP aggregation.

Command mode: Router BGP

Table 261 BGP Aggregation Configuration Options

Command Syntax and Usage

no aggregate-address <1-16>

Deletes this BGP aggregation.

Command mode: Router BGP

show ip bgp aggregate-address [<1-16>]

Displays the current BGP aggregation configuration.

Command mode: All

IGMP Configuration

Table 262 describes the commands used to configure basic IGMP parameters.

Table 262 IGMP Configuration Options

Command Syntax and Usage

ip igmp enable

Globally turns IGMP on.

Command mode: Global configuration

no ip igmp enable

Globally turns IGMP off.

Command mode: Global configuration

show ip igmp

Displays the current IGMP configuration parameters.

Command mode: All

The following sections describe the IGMP configuration options.

- [“IGMP Snooping Configuration” on page 411](#)
- [“IGMP Relay Configuration” on page 413](#)
- [“IGMP Static Multicast Router Configuration” on page 416](#)
- [“IGMP Filtering Configuration” on page 417](#)
- [“IGMP Advanced Configuration” on page 419](#)
- [“IGMP Querier Configuration” on page 421](#)

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 263 describes the commands used to configure IGMP Snooping.

Table 263 IGMP Snooping Configuration Options

Command Syntax and Usage

ip igmp snoop mrouter-timeout *<1-600>*

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

[no] ip igmp snoop aggregate

Enables or disables IGMP Membership Report aggregation.

Command mode: Global configuration

ip igmp snoop source-ip *<IP address>*

Configures the source IP address used as a proxy for IGMP Group Specific Queries.

Command mode: Global configuration

ip igmp snoop vlan *<VLAN number>*

Adds the selected VLAN(s) to IGMP Snooping.

Command mode: Global configuration

no ip igmp snoop vlan *<VLAN number>*

Removes the selected VLAN(s) from IGMP Snooping.

Command mode: Global configuration

no ip igmp snoop vlan all

Removes all VLANs from IGMP Snooping.

Command mode: Global configuration

Table 263 IGMP Snooping Configuration Options

Command Syntax and Usage

ip igmp snoop enable

Enables IGMP Snooping.

Command mode: Global configuration

no ip igmp snoop enable

Disables IGMP Snooping.

Command mode: Global configuration

default ip igmp snoop

Resets IGMP Snooping parameters to their default values.

Command mode: Global configuration

show ip igmp snoop

Displays the current IGMP Snooping parameters.

Command mode: All

IGMPv3 Configuration

[Table 267](#) describes the commands used to configure IGMP version 3.

Table 264 IGMP Version 3 Configuration Options

Command Syntax and Usage

ip igmp snoop igmpv3 sources <1-64>

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.

Command mode: Global configuration

[no] ip igmp snoop igmpv3 v1v2

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.

Command mode: Global configuration

Table 264 IGMP Version 3 Configuration Options

Command Syntax and Usage

[no] ip igmp snoop igmpv3 exclude

Enables or disables snooping on IGMPv3 Exclude Reports. When disabled, the switch ignores Exclude Reports. The default value is enabled.

Command mode: Global configuration

ip igmp snoop igmpv3 enable

Enables IGMP version 3. The default value is disabled.

Command mode: Global configuration

no ip igmp snoop igmpv3 enable

Disables IGMP version 3.

Command mode: Global configuration

show ip igmp snoop igmpv3

Displays the current IGMP v3 Snooping configuration.

Command mode: All except User EXEC

IGMP Relay Configuration

When you configure IGMP Relay, also configure the IGMP Relay multicast routers.

[Table 267](#) describes the commands used to configure IGMP Relay.

Table 265 IGMP Relay Configuration Options

Command Syntax and Usage

ip igmp relay enable

Enables IGMP Relay.

Command mode: Global configuration

no ip igmp relay enable

Disables IGMP Relay.

Command mode: Global configuration

Table 265 IGMP Relay Configuration Options

Command Syntax and Usage

ip igmp relay vlan <VLAN number>

Adds the VLAN to the list of IGMP Relay VLANs.

Command mode: Global configuration

no ip igmp relay vlan <VLAN number>

Removes the VLAN from the list of IGMP Relay VLANs.

Command mode: Global configuration

ip igmp relay report <0-150>

Configures the interval between unsolicited Join reports sent by the switch, in seconds.

The default value is 10.

Command mode: Global configuration

show ip igmp relay

Displays the current IGMP Relay configuration.

Command mode: All

IGMP Relay Multicast Router Configuration

[Table 267](#) describes the commands used to configure multicast routers for IGMP Relay.

Table 266 IGMP Relay Mrouter Configuration Options

Command Syntax and Usage

ip igmp relay mrouter <1-2> **address** <IP address>

Configures the IP address of the IGMP multicast router used for IGMP Relay.

Command mode: Global configuration

ip igmp relay mrouter <1-2> **interval** <1-60>

Configures the time interval between ping attempts to the upstream Mrouters, in seconds. The default value is 2.

Command mode: Global configuration

Table 266 IGMP Relay Mrouter Configuration Options

Command Syntax and Usage

ip igmp relay mrouter <1-2> retry <1-120>

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

ip igmp relay mrouter <1-2> attempt <1-128>

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

ip igmp relay mrouter <1-2> version <1-2>

Configures the IGMP version (1 or 2) of the multicast router.

Command mode: Global configuration

ip igmp relay mrouter <1-2> enable

Enables the multicast router.

Command mode: Global configuration

no ip igmp relay mrouter <1-2> enable

Disables the multicast router.

Command mode: Global configuration

no ip igmp relay mrouter <1-2>

Deletes the multicast router from IGMP Relay.

Command mode: Global configuration

IGMP Static Multicast Router Configuration

Table 267 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 267 IGMP Static Multicast Router Configuration Options

Command Syntax and Usage

ip igmp mrouter *<port alias or number>* *<VLAN number>* *<version (1-3)>*

Selects a port/VLAN combination on which the static multicast router is connected, and configures the IGMP version of the multicast router.

Command mode: Global configuration

no ip igmp mrouter *<port alias or number>* *<VLAN number>* *<version (1-3)>*

Removes a static multicast router from the selected port/VLAN combination.

Command mode: Global configuration

no ip igmp mrouter all

Removes all static multicast routers.

Command mode: Global configuration

clear ip igmp mrouter

Clears the multicast router port table.

Command mode: Global configuration

show ip igmp mrouter

Displays the current IGMP Static Multicast Router parameters.

Command mode: All except User EXEC

IGMP Filtering Configuration

Table 268 describes the commands used to configure an IGMP filter.

Table 268 IGMP Filtering Configuration Options

Command Syntax and Usage

ip igmp profile <1-16>

Configures the IGMP filter.

Command mode: Global configuration

To view command options, see [page 417](#).

ip igmp filtering

Enables IGMP filtering globally.

Command mode: Global configuration

no ip igmp filtering

Disables IGMP filtering globally.

Command mode: Global configuration

show ip igmp filtering

Displays the current IGMP Filtering parameters.

Command mode: All

IGMP Filter Definition

Table 269 describes the commands used to define an IGMP filter.

Table 269 IGMP Filter Definition Options

Command Syntax and Usage

ip igmp profile <1-16> **range** <IP address 1> <IP address 2>

Configures the range of IP multicast addresses for this filter.

Command mode: Global configuration

ip igmp profile <1-16> **action** {allow|deny}

Allows or denies multicast traffic for the IP multicast addresses specified. The default action is deny.

Command mode: Global configuration

Table 269 IGMP Filter Definition Options

Command Syntax and Usage

ip igmp profile <1-16> **enable**

Enables this IGMP filter.

Command mode: Global configuration

no ip igmp profile <1-16> **enable**

Disables this IGMP filter.

Command mode: Global configuration

no ip igmp profile <1-16>

Deletes this filter's parameter definitions.

Command mode: Global configuration

show ip igmp profile <1-16>

Displays the current IGMP filter.

Command mode: All

IGMP Filtering Port Configuration

[Table 270](#) describes the commands used to configure a port for IGMP filtering.

Table 270 IGMP Filter Port Configuration Options

Command Syntax and Usage

[no] ip igmp filtering

Enables or disables IGMP filtering on this port.

Command mode: Interface port

ip igmp profile <1-16>

Adds an IGMP filter to this port.

Command mode: Interface port

Table 270 IGMP Filter Port Configuration Options

Command Syntax and Usage

no ip igmp profile <1-16>

Removes an IGMP filter from this port.

Command mode: Interface port

show interface port <port alias or number> **igmp-filtering**

Displays the current IGMP filter parameters for this port.

Command mode: All except User EXEC

IGMP Advanced Configuration

[Table 267](#) describes the commands used to configure advanced IGMP parameters.

Table 271 IGMP Advanced Configuration Options

Command Syntax and Usage

ip igmp query-interval <1-600>

Sets the IGMP router query interval, in seconds. The default value is 125.

Command mode: Global configuration

ip igmp robust <2-10>

Configures the IGMP 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.

Command mode: Global configuration

ip igmp timeout <1-255>

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.

Command mode: Global configuration

[no] ip igmp fastleave <VLAN number>

Enables or disables Fastleave processing. Fastleave allows the switch to 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.

Command mode: Global configuration

Table 271 IGMP Advanced Configuration Options

Command Syntax and Usage

[no] ip igmp flood

Configures the switch to flood unregistered IP multicast traffic to all ports. The default setting is **enabled**.

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.

Command mode: Global configuration

[no] ip igmp cpu

Configures the switch to forward unregistered IP multicast traffic to the MP, which adds an entry in the IPMC table, as follows:

- 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.

The default setting is **enabled**.

Note: If both **flood** and **cpu** are disabled, then the switch drops all unregistered IPMC traffic.

Command mode: Global configuration

[no] ip igmp snoop rtralert

Enables or disables the Router Alert option in IGMP messages.

Command mode: Global configuration

IGMP Querier Configuration

Table 268 describes the commands used to configure IGMP Querier.

Table 272 IGMP Querier Configuration Options

Command Syntax and Usage

ip igmp querier vlan <VLAN number> **source-ip** <IP address>

Configures the IGMP source IP address for the selected VLAN.

Command mode: Global configuration

ip igmp querier vlan <VLAN number> **max-response** <1-256>

Configures the maximum time, in tenths of a second, allowed before responding to a Membership Query message. The default value is 100.

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.

Command mode: Global configuration

ip igmp querier vlan <VLAN number> **query-interval** <1-608>

Configures the interval between IGMP Query broadcasts. The default value is 125 seconds.

Command mode: Global configuration

ip igmp querier vlan <VLAN number> **robustness** <2-10>

Configures the IGMP Robustness variable, which is the number of times that the switch sends each IGMP message. The default value is 2.

Command mode: Global configuration

ip igmp querier vlan <VLAN number> **election-type** [ipv4|mac]

Sets the IGMP Querier election criteria as IP address or Mac address. The default setting is IPv4.

Command mode: Global configuration

ip igmp querier vlan <VLAN number> **startup-interval** <1-608>

Configures the Startup Query Interval, which is the interval between General Queries sent out at startup.

Command mode: Global configuration

Table 272 IGMP Querier Configuration Options

Command Syntax and Usage

ip igmp querier vlan <VLAN number> **startup-count** <1-10>

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.

Command mode: Global configuration

ip igmp querier vlan <VLAN number> **version** [v1|v2|v3]

Configures the IGMP version. The default version is v3.

Command mode: Global configuration

ip igmp querier enable

Enables IGMP Querier.

Command mode: Global configuration

no ip igmp querier enable

Disables IGMP Querier.

Command mode: Global configuration

show ip igmp querier vlan <VLAN number>

Displays IGMP Querier information for the selected VLAN.

Command mode: Global configuration

show ip igmp querier

Displays the current IGMP Querier parameters.

Command mode: All

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`, `tracert`, and `tftp` commands.

Table 273 Domain Name Service Options

Command Syntax and Usage

[no] ip dns primary-server *<IP address>* [**mgt-port** | **data-port**]

You are prompted to set the IPv4 address for your primary DNS server, using dotted decimal notation.

Command mode: Global configuration

[no] ip dns secondary-server *<IP address>* [**mgt-port** | **data-port**]

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.

Command mode: Global configuration

[no] ip dns domain-name *<string>*

Sets the default domain name used by the switch.
For example: `mycompany.com`

Command mode: Global configuration

show ip dns

Displays the current Domain Name System settings.

Command mode: All except User EXEC

Bootstrap Protocol Relay Configuration

The Bootstrap Protocol (BOOTP) Relay commands are used to allow hosts to obtain 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 DHCP/BOOTP servers with IP addresses that have been configured on the G8264.

BOOTP relay is turned off by default.

Table 274 Global BOOTP Relay Configuration Options

Command Syntax and Usage

[no] ip bootp-relay server <1-5> address <IP address>

Sets the IP address of the selected global BOOTP server.

Command mode: Global configuration

ip bootp-relay enable

Globally turns on BOOTP relay.

Command mode: Global configuration

no ip bootp-relay enable

Globally turns off BOOTP relay.

Command mode: Global configuration

BOOTP Relay Broadcast Domain Configuration

This menu allows you to configure a BOOTP server for a specific broadcast domain, based on its associated VLAN.

Table 275 BOOTP Relay Broadcast Domain Configuration Options

Command Syntax and Usage

ip bootp-relay bcast-domain <1-10> **vlan** <VLAN number>

Configures the VLAN of the broadcast domain. Each broadcast domain must have a unique VLAN.

Command mode: Global configuration

ip bootp-relay bcast-domain <1-10> **server** <1-5>
address <IPv4 address>

Sets the IP address of the BOOTP server.

Command mode: Global configuration

ip bootp-relay bcast-domain <1-10> **enable**

Enables BOOTP Relay for the broadcast domain.

Command mode: Global configuration

no ip bootp-relay bcast-domain <1-10> **enable**

Disables BOOTP Relay for the broadcast domain. When disabled, BOOTP Relay is performed by one of the global BOOTP servers.

Command mode: Global configuration

no ip bootp-relay bcast-domain <1-10>

Deletes the selected broadcast domain configuration.

Command mode: Global configuration

show ip bootp-relay

Displays the current parameters for the BOOTP Relay broadcast domain.

Command mode: All

Option 82 Configuration

These commands allow you to configure DHCP option 82 information. The switch can use the following DHCP option 82 sub-options to allocate server addresses.

- **Circuit ID:** Identifies the host name or MAC addresses of the switch making the DHCP request.
- **Remote ID:** Identifies the port that receives the DHCP request.

DHCP Relay Agent (Option 82) is defined in RFC 3046.

Table 276 Option 82 Configuration Options

Command Syntax and Usage

ip bootp-relay information enable

Turns BOOTP Option 82 on.

Command mode: Global configuration

[no] ip bootp-relay information enable

Turns BOOTP Option 82 off.

Command mode: Global configuration

ip bootp-relay information policy {keep|drop|replace}

Configures the DHCP re-forwarding policy, as follows:

- Keep:** Retains requests that contain relay information if the option 82 information is also present.
- Drop:** Discards requests that contain relay information if the option 82 information is also present.
- Replace:** Replace the relay information in requests that also contain option 82 information.

Command mode: Global configuration

show ip bootp-relay

Displays the current BOOTP Option 82 parameters.

Command mode: All

VRRP Configuration

Virtual Router Redundancy Protocol (VRRP) support on the G8264 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. BLADEOS 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 *BLADEOS 6.6 Application Guide*.

Table 277 Virtual Router Redundancy Protocol Options

Command Syntax and Usage

router vrrp

Enter Router VRRP configuration mode.

Command mode: Global configuration

enable

Globally enables VRRP on this switch.

Command mode: Router VRRP

no enable

Globally disables VRRP on this switch.

Command mode: Router VRRP

show ip vrrp

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 278 VRRP Virtual Router Configuration Options

Command Syntax and Usage

virtual-router <1-128> **virtual-router-id** <1-255>

Defines the virtual router ID (VRID). This is used in conjunction with the `[no] virtual-router <VRID> address <IP address>` 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.

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.

All VRID values must be unique within the VLAN to which the virtual router's IP interface belongs.

Command mode: Router VRRP

[no] virtual-router <1-128> **address** <IP address>

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.

Command mode: Router VRRP

virtual-router <1-128> **interface** <interface number>

Selects a switch IP interface. If the IP interface has the same IP address as the `addr` 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 `preem` option below is disabled. The default value is 1.

Command mode: Router VRRP

Table 278 VRRP Virtual Router Configuration Options

Command Syntax and Usage

virtual-router <1-128> **priority** <1-254>

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.

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).

When priority tracking is used, this base priority value can be modified according to a number of performance and operational criteria.

Command mode: Router VRRP

virtual-router <1-128> **timers advertise** <1-255>

Defines the time interval between VRRP master advertisements. This can be any integer between 1 and 255 seconds. The default value is 1.

Command mode: Router VRRP

virtual-router <1-128> **timers preempt-delay-time** <0-255>

Configures the preempt delay interval. This timer is configured on the VRRP Owner and prevents the switch from transitioning back to Master state until the preempt delay interval has expired. Ensure that the interval is long enough for OSPF or other routing protocols to converge.

Command mode: Router VRRP

[no] virtual-router <1-128> **preemption**

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 `preemption` 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 `addr` are the same). By default, this option is enabled.

Command mode: Router VRRP

Table 278 VRRP Virtual Router Configuration Options

Command Syntax and Usage

[no] virtual-router <1-128> fast-advertise

Enables or disables Fast Advertisements. When enabled, the VRRP master advertisements interval is calculated in units of centiseconds, instead of seconds. For example, if **adver** is set to 1 and **fadver** is enabled, master advertisements are sent every .01 second.

When you disable fast advertisement, the advertisement interval is set to the default value of 1 second. To support Fast Advertisements, set the interval between 20-100 centiseconds.

Command mode: Router VRRP

virtual-router <1-128> enable

Enables this virtual router.

Command mode: Router VRRP

no virtual-router <1-128> enable

Disables this virtual router.

Command mode: Router VRRP

no virtual-router <1-128>

Deletes this virtual router from the switch configuration.

Command mode: Router VRRP

show ip vrrp virtual-router <1-128>

Displays the current configuration information for this virtual router.

Command mode: All except User EXEC

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 279 VRRP Priority Tracking Configuration Options

Command Syntax and Usage

[no] virtual-router <1-128> track virtual-routers

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.

Command mode: Router VRRP

[no] virtual-router <1-128> track interfaces

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.

Command mode: Router VRRP

[no] virtual-router <1-128> track ports

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.

Command mode: Router VRRP

show ip vrrp virtual-router <1-128> track

Displays the current configuration for priority tracking for this virtual router.

Command mode: All except User EXEC

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 G8264 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 G8264s in a hot-standby failover configuration, where only one switch is active at any time.

Table 280 VRRP Virtual Router Group Configuration Options

Command Syntax and Usage

group virtual-router-id <1-255>

Defines the virtual router ID (VRID).

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 `interface` below) belongs. The default virtual router ID is 1.

Command mode: Router VRRP

group interface <interface number>

Selects a switch IP interface. The default switch IP interface number is 1.

Command mode: Router VRRP

group priority <1-254>

Defines the election priority bias for this virtual router group. This can be any integer between 1 and 254. The default value is 100.

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 (`addr`) is the same as the one used by the IP interface, the priority for this virtual router will automatically be set to 255 (highest).

When priority tracking is used, this base priority value can be modified according to a number of performance and operational criteria.

Command mode: Router VRRP

Table 280 VRRP Virtual Router Group Configuration Options

Command Syntax and Usage

group advertisement <1-255>

Defines the time interval between VRRP master advertisements. This can be any integer between 1 and 255 seconds. The default is 1.

Command mode: Router VRRP

[no] group preemption

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 `preemption` 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.

Command mode: Router VRRP

[no] group fast-advertise

Enables or disables Fast Advertisements. When enabled, the VRRP master advertisements interval is calculated in units of centiseconds, instead of seconds. For example, if `adver` is set to 1 and `fastadver` is enabled, master advertisements are sent every .01 second.

When you disable fast advertisement, the advertisement interval is set to the default value of 1 second. To support Fast Advertisements, set the interval between 20-100 centiseconds.

Command mode: Router VRRP

group enable

Enables the virtual router group.

Command mode: Router VRRP

no group enable

Disables the virtual router group.

Command mode: Router VRRP

Table 280 VRRP Virtual Router Group Configuration Options

Command Syntax and Usage

no group

Deletes the virtual router group from the switch configuration.

Command mode: Router VRRP

show ip vrrp group

Displays the current configuration information for the virtual router group.

Command mode: All except User EXEC

Virtual Router Group Priority Tracking Configuration

Note – If *Virtual Router Group Tracking* is enabled, then the tracking option will be available only under *group* option. The tracking setting for the other individual virtual routers will be ignored.

Table 281 Virtual Router Group Priority Tracking Configuration Options

Command Syntax and Usage

[no] group track interfaces

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.

Command mode: Router VRRP

[no] group track ports

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.

Command mode: Router VRRP

show ip vrrp group track

Displays the current configuration for priority tracking for this virtual router.

Command mode: All except User EXEC

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 282 VRRP Interface Options

Command Syntax and Usage

interface <interface number> **authentication** {**password** | **none**}

Defines the type of authentication that will be used: **none** (no authentication) or **password** (password authentication).

Command mode: Router VRRP

[**no**] **interface** <interface number> **password** <password>

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 **interface authentication** above).

Command mode: Router VRRP

no interface <interface number>

Clears the authentication configuration parameters for this IP interface. The IP interface itself is not deleted.

Command mode: Router VRRP

show ip vrrp interface <interface number>

Displays the current configuration for this IP interface's authentication parameters.

Command mode: All except User EXEC

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 431](#)), the priority level for the virtual router is increased by a defined amount.

Table 283 VRRP Tracking Configuration Options

Command Syntax and Usage

tracking-priority-increment virtual-routers <0-254>

Defines the priority increment value (0 through 254) for virtual routers in master mode detected on this switch. The default value is 2.

Command mode: Router VRRP

tracking-priority-increment interfaces <0-254>

Defines the priority increment value for active IP interfaces detected on this switch. The default value is 2.

Command mode: Router VRRP

tracking-priority-increment ports <0-254>

Defines the priority increment value for active ports on the virtual router’s VLAN. The default value is 2.

Command mode: Router VRRP

show ip vrrp tracking-priority-increment

Displays the current configuration of priority tracking increment values.

Command mode: All except User EXEC

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 431](#)) are enabled.

Protocol Independent Multicast Configuration

Table 284 PIM Configuration Options

Command Syntax and Usage

ip pim component <1-2>

Enter PIM component mode. See [page 438](#) to view options.

ip pim regstop-ratelimit-period <0-2147483647>

Configures the register stop rate limit, in seconds. The default value is 5.

Command mode: Global configuration

[no] ip pim static-rp enable

Enables or disables static RP configuration. The default setting is disabled.

Command mode: Global configuration

[no] ip pim pabr enable

Enables or disables PIM border router. The default setting is disabled.

Command mode: Global configuration

ip pim enable

Globally turns PIM on.

Command mode: Global configuration

no ip pim enable

Globally turns PIM off.

Command mode: Global configuration

clear ip pim mroute

Clears PIM multicast router entries.

Command mode: Global configuration

PIM Component Configuration

Table 285 PIM Component Configuration Options

Command Syntax and Usage

ip pim component <1-2>

Enter PIM component mode.

Command mode: Global configuration

mode {**dense** | **sparse**}

Configures the operational mode of the PIM router (dense or sparse).

Command mode: PIM Component

show ip pim component [<1-2>]

Displays the current PIM component configuration settings.

Command mode: All

RP Candidate Configuration

Use these commands to configure a PIM router Rendezvous Point (RP) candidate.

Table 286 RP Candidate Configuration Options

Command Syntax and Usage

rp-candidate rp-address <group multicast address> <group subnet mask>
<IP address>

Adds an RP candidate.

Command mode: PIM Component

no rp-candidate rp-address <group multicast address> <group subnet mask>
<IP address>

Removes the specified RP candidate.

Command mode: PIM Component

rp-candidate holdtime <0-255>

Configures the hold time of the RP candidate, in seconds.

Command mode: PIM Component

RP Static Configuration

Use these commands to configure a static PIM router Rendezvous Point (RP).

Table 287 RP Static Configuration Options

Command Syntax and Usage

rp-static rp-address <group multicast address> <group subnet mask> <IP address>

Adds a static RP.

Command mode: PIM Component

no rp-static rp-address <group multicast address> <group subnet mask>
<IP address>

Removes the specified static RP.

Command mode: PIM Component

PIM Interface Configuration

Table 288 PIM Interface Configuration Options

Command Syntax and Usage

interface ip <interface number>

Enter Interface IP mode.

Command mode: Global Configuration

ip pim hello-interval <0-65535>

Configures the time interval, in seconds, between PIM Hello packets. The default value is 30.

Command mode: Interface IP

ip pim join-prune-interval <0-65535>

Configures the interval between Join Prune messages, in seconds. The default value is 60.

Command mode: Interface IP

ip pim cbsr-preference <-1-255>

Configures the candidate bootstrap router preference.

Command mode: Interface IP

Table 288 PIM Interface Configuration Options

Command Syntax and Usage

ip pim component-id <1-2>

Defines the component ID for the interface.

Command mode: Interface IP

ip pim hello-holdtime <1-65535>

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

ip pim dr-priority <0-4294967294>

Configures the designated router priority. The default value is 1.

Command mode: Interface IP

ip pim override-interval <0-65535>

Configures the override interval for the router interface, in seconds.

Command mode: Interface IP

ip pim lan-delay <0-32767>

Configures the LAN delay value for the router interface, in seconds.

Command mode: Interface IP

[no] ip pim border-bit

Enables or disables the interface as a border router. The default setting is disabled.

Command mode: Interface IP

[no] ip pim lan-prune-delay

Enables or disables LAN delay advertisements on the interface. The default setting is disabled.

Command mode: Interface IP

ip pim neighbor-addr <IP address> **allow|deny**

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.

Command mode: Interface IP

Table 288 PIM Interface Configuration Options

Command Syntax and Usage

[no] ip pim neighbor-filter

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:

ip pim neighbor-addr *<IP address>*

Command mode: Interface IP

ip pim enable

Enables PIM on the interface.

Command mode: Interface IP

no ip pim enable

Disables PIM on the interface.

Command mode: Interface IP

show ip pim neighbor-filters

Displays the configured PIM neighbor filters.

Command mode: All

show ip pim interface [*<interface number>* | **detail**]

Displays the current PIM interface parameters.

Command mode: All

IPv6 Default Gateway Configuration

The switch supports IPv6 default gateways, as follows:

- Gateway 1: data traffic
- Gateway 4: management port

[Table 289](#) describes the IPv6 Default Gateway Configuration commands.

Table 289 IPv6 Default Gateway Configuration Options

Command Syntax and Usage

ip gateway6 {1|4} address <IPv6 address>

Configures the IPv6 address of the default gateway, in hexadecimal format with colons (such as 3001:0:0:0:0:abcd:12).

Command mode: Global configuration

[no] ip gateway6 {1|4} enable

Enables or disables the default gateway.

Command mode: Global configuration

no ip gateway6 {1|4}

Deletes the default gateway.

Command mode: Global configuration

show ipv6 gateway6 {1|4}

Displays the current IPv6 default gateway configuration.

Command mode: All

IPv6 Static Route Configuration

Table 290 describes the IPv6 static route configuration commands.

Table 290 IPv6 Static Route Configuration Options

Command Syntax and Usage

ip route6 *<IPv6 address>* *<prefix length>* *<IPv6 gateway address>*
 [*<interface number>*]

Adds an IPv6 static route.

Command mode: Global configuration

no ip route6 *<IPv6 address>* *<prefix length>*

Removes the selected route.

Command mode: Global configuration

no ip route6 [**destination-address** *<IPv6 address>* |
gateway *<default gateway address>* | **all**]

Clears the selected IPv6 static routes.

Command mode: Global configuration

show ipv6 route static

Displays the current static route configuration.

Command mode: All

IPv6 Neighbor Discovery Cache Configuration

Table 291 describes the IPv6 Neighbor Discovery cache configuration commands.

Table 291 IPv6 Neighbor Discovery Cache Configuration Options

Command Syntax and Usage

ip neighbors <IPv6 address> <MAC address> **vlan** <VLAN number>
port <port number or alias>

Adds a static entry to the Neighbor Discovery cache table.

Command mode: Global configuration

no ip neighbors {<IPv6 address> | **all**}

Deletes the selected entry from the static Neighbor Discovery cache table.

Command mode: Global configuration

no ip neighbors [**all if** | **all interface port** | **all vlan** | **all**]

Clears the selected static entries in the Neighbor Discovery cache table.

Command mode: Global configuration

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 292 IPv6 Path MTU Options

Command Syntax and Usage

ip pmtu6 timeout 0 | <10-100>

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

Table 292 IPv6 Path MTU Options

Command Syntax and Usage

clear ipv6 pmtu

Clears all entries in the Path MTU cache.

Command mode: All Except User EXEC

show ipv6 pmtu

Displays the current Path MTU configuration.

Command mode: All

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 293 IPv6 Neighbor Discovery Prefix Options

Command Syntax and Usage

interface ip <I-127>

Enters Interface IP mode.

Command mode: Global configuration

ipv6 nd prefix {<IPv6 prefix> <prefix length>} [no-advertise]

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 `no-advertise` option.

Additional prefix options are listed below.

Command mode: Interface IP

no ipv6 nd prefix [<IPv6 prefix> <prefix length>] | interface | all

Removes a Neighbor Discovery prefix. If you specify an interface number, all prefixes for the interface are removed.

Command mode: Interface IP

Table 293 IPv6 Neighbor Discovery Prefix Options**Command Syntax and Usage**

```
ipv6 nd prefix {<IPv6 prefix> <prefix length>}
valid-lifetime <0-4294967295> [infinite|variable]
preferred-lifetime <0-4294967295> [infinite|variable]
```

Configures the Valid Lifetime and (optionally) the Preferred Lifetime of the prefix, in seconds.

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.

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.

Note: The Preferred Lifetime value must not exceed the Valid Lifetime value.

Command mode: Interface IP

```
ipv6 nd prefix {<IPv6 prefix> <prefix length>} off-link
```

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.

To clear the off-link flag, omit the off-link parameter when you issue this command.

Command mode: Interface IP

```
ipv6 nd prefix {<IPv6 prefix> <prefix length>} no-autoconfig
```

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.

Command mode: Interface IP

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

Displays current Neighbor Discovery prefix parameters.

Command mode: All

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 294 IPv6 Prefix Policy Table Options

Command Syntax and Usage

ip prefix-policy *<IPv6 prefix>* *<prefix length>* *<precedence (0-100)>*
<label (0-100)>

Adds a Prefix Policy Table entry. Enter the following parameters:

- 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.

Command mode: Global configuration

no ip prefix-policy *<IPv6 prefix>* *<prefix length>* *<precedence (0-100)>*
<label (0-100)>

Removes a prefix policy table entry.

Command mode: Global configuration

show ip prefix-policy

Displays the current Prefix Policy Table configuration.

Command mode: All

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 295 IP Loopback Interface Configuration Options

Command Syntax and Usage

interface loopback <1-5>

Enter Interface loopback mode.

Command mode: Global configuration

no interface loopback <1-5>

Deletes the selected loopback interface.

Command mode: Global configuration

ip address <IP address>

Defines the loopback interface IP address.

Command mode: Interface loopback

ip netmask <subnet mask>

Defines the loopback interface subnet mask.

Command mode: Interface loopback

enable

Enables the loopback interface.

Command mode: Interface loopback

no enable

Disables the loopback interface.

Command mode: Interface loopback

show interface loopback <1-5>

Displays the current IP loopback interface parameters.

Command mode: All

DHCP Snooping

DHCP Snooping provides security by filtering untrusted DHCP packets and by maintaining a binding table of trusted interfaces.

Table 296 DHCP Snooping Options

Command Syntax and Usage

ip dhcp snooping vlan <VLAN number>

Adds the selected VLAN to DHCP Snooping. Member ports participate in DHCP Snooping.

Command mode: Global configuration

[no] ip dhcp snooping vlan <VLAN number>

Removes the selected VLAN from DHCP Snooping.

Command mode: Global configuration

ip dhcp snooping binding <MAC address> **vlan** <VLAN number> <IP address>
port <port alias or number> **expiry** <lease>

Adds a manual entry to the binding table.

Command mode: Global configuration

no ip dhcp snooping binding {<MAC address> | **all**
[**interface port** <port alias or number> | **vlan** <VLAN number>]}

Removes an entry from the binding table.

Command mode: Global configuration

ip dhcp snooping

Turns on DHCP Snooping.

Command mode: Global configuration

no ip dhcp snooping

Turns off DHCP Snooping.

Command mode: Global configuration

Table 296 DHCP Snooping Options

Command Syntax and Usage

[no] ip dhcp snooping information option-insert

Enables or disables option 82 support for DHCP Snooping.

When enabled, DHCP Snooping performs the following functions:

- If a DHCP packet from a client contains option 82 information, the information is retained.
- When DHCP Snooping forwards a DHCP packet from a client, option 82 information is added to the packet;
- When DHCP snooping forward a DHCP packet from a server, option 82 information is removed from the packet.

Command mode: Global configuration

show ip dhcp snooping

Displays the current DHCP Snooping parameters.

Command mode: All

Converged Enhanced Ethernet Configuration

Table 297 describes the Converged Enhanced Ethernet (CEE) configuration commands.

Table 297 CEE Configuration Options

Command Syntax and Usage

cee enable

Globally turns CEE on.

Command mode: Global configuration

no cee enable

Globally turns CEE off.

Command mode: Global configuration

[no] cee iscsi enable

Enables or disables ISCSI TLV advertisements.

Command mode: Global configuration

show cee iscsi

Displays the current ISCSI TLV parameters.

Command mode: All

show cee

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 and commands. When ETS is enabled, you cannot configure the 802.1p options.

ETS Global Priority Group Configuration

Table 298 describes the global ETS Priority Group configuration options.

Table 298 Global ETS Priority Group Options

Command Syntax and Usage

[no] cee global ets priority-group pgid <0-7, 15>
bandwidth <802.1p priority (0-7)> <bandwidth percentage (0, 10-100)>

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.

Command mode: Global configuration

[no] cee global ets priority-group pgid <0-7, 15>
description <1-31 characters>

Enter text that describes this Priority Group.

Command mode: Global configuration

cee global ets priority-group pgid <0-7, 15> **priority** <0-7>

Adds one or more 802.1p priority values to the Priority Group. Enter one value per line, null to end.

Command mode: Global configuration

show cee global ets priority-group <0-7, 15>

Displays the current global ETS Priority Group parameters.

Command mode: All

show cee global ets

Displays the current global ETS parameters.

Command mode: All

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.

802.1p PFC Configuration

[Table 300](#) describes the 802.1p Priority Flow Control (PFC) configuration options.

Table 299 PFC 802.1p commands

Command Syntax and Usage

cee port *<port alias or number>* **pfc priority** *<0-7>* **enable**

Enables Priority Flow Control on the selected 802.1p priority.

Command mode: Global configuration

no cee port *<port alias or number>* **pfc priority** *<0-7>* **enable**

Disables Priority Flow Control on the selected 802.1p priority.

Command mode: Global configuration

cee cee port *<port alias or number>* **pfc priority** *<0-7>*
description *<1-31 characters>*

Enter text to describe the priority value.

Command mode: Global configuration

show cee port *<port alias or number>* **pfc priority** *<0-7>*

Displays the current 802.1p Priority Flow Control parameters.

Command mode: All

DCBX Port Configuration

Table 300 describes the port DCB Capability Exchange Protocol (DCBX) configuration options.

Table 300 Port DCBX Configuration Options

Command Syntax and Usage

cee port <port alias or number> **dcbx app_proto advertise**

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).

Command mode: Global configuration

cee port <port alias or number> **dcbx app_proto willing**

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).

Command mode: Global configuration

cee port <port alias or number> **dcbx ets advertise**

Enables or disables DCBX ETS advertisements of configuration data. When enabled, the Advertisement flag is set to 1 (advertise data to the peer device).

Command mode: Global configuration

cee port <port alias or number> **dcbx ets willing**

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).

Command mode: Global configuration

cee port <port alias or number> **dcbx pfc advertise**

Enables or disables DCBX PFC advertisements of configuration data. When enabled, the Advertisement flag is set to 1 (advertise data to the peer device).

Command mode: Global configuration

cee port <port alias or number> **dcbx pfc willing**

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).

Command mode: Global configuration

Table 300 Port DCBX Configuration Options

Command Syntax and Usage

no cee port *<port alias or number>* **dcbx enable**

Disables DCBX on the port.

Command mode: Global configuration

cee port *<port alias or number>* **dcbx enable**

Enables DCBX on the port.

Command mode: Global configuration

show cee port *<port alias or number>* **dcbx**

Displays the current port DCBX parameters.

Command mode: All

Fiber Channel over Ethernet Configuration

Fiber Channel over Ethernet (FCoE) transports Fiber Channel frames over an Ethernet fabric. The CEE features and FCoE features allow you to create a lossless Ethernet transport mechanism.

[Table 301](#) describes the FCoE configuration options.

Table 301 FCoE Configuration Options

Command Syntax and Usage

fcoe fips enable

Globally turns FIP Snooping on.

Command mode: Global configuration

no fcoe fips enable

Globally turns FIP Snooping off.

Command mode: Global configuration

Table 301 FCoE Configuration Options

Command Syntax and Usage

fcoe fips timeout-acl

Enables or disables ACL time-out removal. When enabled, ACLs associated with expired FCFs and FCoE connections are removed from the system.

Command mode: Global configuration

show fcoe

Displays the current FCoE parameters.

Command mode: All

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 302](#) describes the port Fiber Channel over Ethernet Initialization Protocol (FIP) Snooping configuration options.

Table 302 Port FIP Snooping Options

Command Syntax and Usage

fcoe fips port *<port alias or number>* **fcf-mode** [**auto**|**on**|**off**]

Configures FCoE Forwarding (FCF) on the port, as follows:

- on**: Configures the port as a Fiber 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.

Command mode: Global configuration

[no] fcoe fips automatic-vlan

Enables or disables automatic VLAN creation, based on response received from the connected device.

Command mode: Global configuration

Table 302 Port FIP Snooping Options

Command Syntax and Usage

fcoe fips port <port alias or number> **enable**

Enables FIP Snooping on the port. The default setting is enabled.

Command mode: Global configuration

no fcoe fips port <port alias or number> **enable**

Disables FIP Snooping on the port.

Command mode: Global configuration

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 458](#)
- [“RMON Event Configuration” on page 459](#)
- [“RMON Alarm Configuration” on page 460](#)

RMON History Configuration

Table 303 describes the RMON History commands.

Table 303 RMON History Configuration Options

Command Syntax and Usage

rmon history <1-65535> **interface-oid** <1-127 characters>

Configures the interface MIB Object Identifier. The IFOID must correspond to the standard interface OID, as follows:

1.3.6.1.2.1.2.2.1.1.x

where x is the ifIndex

Command mode: Global configuration

rmon history <1-65535> **requested-buckets** <1-65535>

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.

The maximum number of buckets that can be granted is 50.

Command mode: Global configuration

rmon history <1-65535> **polling-interval** <1-3600>

Configures the time interval over which the data is sampled for each bucket.

The default value is 1800.

Command mode: Global configuration

rmon history <1-65535> **owner** <1-127 characters>

Enter a text string that identifies the person or entity that uses this History index.

Command mode: Global configuration

no rmon history <1-65535>

Deletes the selected History index.

Command mode: Global configuration

show rmon history

Displays the current RMON History parameters.

Command mode: All

RMON Event Configuration

Table 304 describes the RMON Event commands.

Table 304 RMON Event Configuration Options

Command Syntax and Usage

rmon event <1-65535> **description** <1-127 characters>

Enter a text string to describe the event.

Command mode: Global configuration

[no] **rmon event** <1-65535> **type** log|trap|both

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

rmon event <1-65535> **owner** <1-127 characters>

Enter a text string that identifies the person or entity that uses this event index.

Command mode: Global configuration

no rmon event <1-65535>

Deletes the selected RMON Event index.

Command mode: Global configuration

show rmon event

Displays the current RMON Event parameters.

Command mode: All

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 305 describes the RMON Alarm commands.

Table 305 RMON Alarm Configuration Options

Command Syntax and Usage

rmon alarm <1-65535> **oid** <1-127 characters>

Configures an alarm MIB Object Identifier.

Command mode: Global configuration

rmon alarm <1-65535> **interval** <1-65535>

Configures the time interval over which data is sampled and compared with the rising and falling thresholds. The default value is 1800.

Command mode: Global configuration

rmon alarm <1-65535> **sample abs|delta**

Configures the method of sampling the selected variable and calculating the value to be compared against the thresholds, as follows:

- **abs**—absolute value, the value of the selected variable is compared directly with the thresholds at the end of the sampling interval.
- **delta**—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.

Command mode: Global configuration

rmon alarm <1-65535> **alarm-type rising|falling|either**

Configures the alarm type as rising, falling, or either (rising or falling).

Command mode: Global configuration

rmon alarm <1-65535> **rising-limit** <-2147483647 - 2147483647>

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.

Command mode: Global configuration

Table 305 RMON Alarm Configuration Options

Command Syntax and Usage

rmon alarm <1-65535> **falling-limit** <-2147483647 - 214748364)

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.

Command mode: Global configuration

rmon alarm <1-65535> **rising-crossing-index** <1-65535>

Configures the rising alarm event index that is triggered when a rising threshold is crossed.

Command mode: Global configuration

rmon alarm <1-65535> **falling-crossing-index** <1-65535>

Configures the falling alarm event index that is triggered when a falling threshold is crossed.

Command mode: Global configuration

rmon alarm <1-65535> **owner** <1-127 characters>

Enter a text string that identifies the person or entity that uses this alarm index.

Command mode: Global configuration

no rmon alarm <1-65535>

Deletes the selected RMON Alarm index.

Command mode: Global configuration

show rmon alarm

Displays the current RMON Alarm parameters.

Command mode: All

Virtualization Configuration

Table 306 describes the virtualization configuration options.

Table 306 Virtualization Configuration Options

Command Syntax and Usage

virt enable

Enables VMready. Before you enable VMready, you must define one or more server ports. See “[Server Port Configuration](#)” on page 265.

Command mode: Global configuration

no virt enable

Disables VMready.

Note: This command deletes all configured VM groups.

Command mode: Global configuration

show virt

Displays the current virtualization parameters.

Command mode: All

VM Policy Bandwidth Management

Table 307 describes the bandwidth management options for the selected VM. Use these commands to limit the bandwidth used by each VM.

Table 307 VM Bandwidth Management Options

Command Syntax and Usage

```
virt vmpolicy vmbwidth [<MAC address> | <UUID> | <name> |
  <IP address> | <index number>] txrate <64-1000000> <max. burst (32-4096)>
  <ACL number>
```

The first value configures Committed Rate—the amount of bandwidth available to traffic transmitted from the VM to the switch, in megabits per second. Enter the value in multiples of 64.

The second values configures the maximum burst size, in kilobits. Enter one of the following values: 32, 64, 128, 256, 512, 1024, 2048, 4096.

The third value represents the ACL assigned to the transmission rate. The ACL is added 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.

Command mode: Global configuration

```
virt vmpolicy vmbwidth [<MAC address> | <UUID> | <name> |
  <IP address> | <index number>] rxrate <64-1000000>
```

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.

The second values configures the maximum burst size, in Kilobits. Enter one of the following values: 32, 64, 128, 256, 512, 1024, 2048, 4096.

Command mode: Global configuration

```
[no] virt vmpolicy vmbwidth [<MAC address> | <UUID> | <name> |
  <IP address> | <index number>] bwctrl
```

Enables or disables bandwidth control on the VM policy.

Command mode: Global configuration

Table 307 VM Bandwidth Management Options

Command Syntax and Usage

[no] virt vmpolicy vmbwidth [*<MAC address>* | *<UUID>* | *<name>* | *<IP address>* | *<index number>*]

Deletes the bandwidth management settings from this VM policy.

Command mode: Global configuration

show virt vmpolicy vmbandwidth [*<MAC address>* | *<UUID>* | *<name>* | *<IP address>* | *<index number>*]

Displays the current VM bandwidth management parameters.

Command mode: All

Virtual NIC Configuration

[Table 308](#) describes the Virtual NIC (vNIC) configuration options.

Table 308 Virtual NIC Options

Command Syntax and Usage

vnic enable

Globally turns vNIC on.

Command mode: Global configuration

no vnic enable

Globally turns vNIC off.

Command mode: Global configuration

show vnic

Displays the current vNIC parameters.

Command mode: Global configuration

vNIC Port Configuration

Table 309 describes the Virtual NIC (vNIC) port configuration options.

Table 309 vNIC Port Configuration Options

Command Syntax and Usage

vnic port <port alias or number> **index** <1-4>

Enters vNIC Configuration mode.

Note: This command is valid for internal server ports only.

Command mode: Global configuration

bandwidth <1-100>

Configures the maximum bandwidth allocated to this vNIC, in increments of 100 Mbps. For example:

- 1 = 100 Mbps
- 10 = 1000 Mbps

Command mode: vNIC configuration

enable

Enables the vNIC.

Command mode: vNIC configuration

no enable

Disables the vNIC.

Command mode: vNIC configuration

Virtual NIC Group Configuration

Table 310 describes the Virtual NIC (vNIC) Group configuration options.

Table 310 vNIC Group Configuration Options

Command Syntax and Usage

vnic vnicgroup <1-32>

Enters vNIC Group Configuration mode.

Command mode: Global Configuration

vlan <VLAN number>

Assigns a VLAN to the vNIC Group.

Command mode: vNIC Group configuration

[no] failover

Enables or disables uplink failover for the vNIC Group. Uplink Failover for the vNIC Group will disable only the affected vNIC links on the port. Other port functions continue to operate normally.

The default setting is disabled.

Command mode: vNIC Group configuration

member <vNIC number>

Adds a vNIC to the vNIC Group. The vNIC ID is comprised of the port number and the vNIC number. For example: 1 . 1

Command mode: vNIC Group configuration

no member <vNIC number>

Removes the selected vNIC from the vNIC Group.

Command mode: vNIC Group configuration

port <port number or alias>

Adds the selected switch port to the vNIC Group.

Command mode: vNIC Group configuration

no port <port number or alias>

Removes the selected switch port from the vNIC Group.

Command mode: vNIC Group configuration

Table 310 vNIC Group Configuration Options

Command Syntax and Usage

trunk <*trunk number*>

Adds the selected trunk group to the vNIC Group.

Command mode: vNIC Group configuration

no trunk <*trunk number*>

Removes the selected trunk group from the vNIC Group.

Command mode: vNIC Group configuration

enable

Enables the vNIC Group.

Command mode: vNIC Group configuration

no enable

Disables the vNIC Group.

Command mode: vNIC Group configuration

no vnic vnicgroup <*1-32*>

Deletes the selected vNIC Group.

Command mode: Global configuration

show vnicgroup

Displays the current vNIC Group parameters.

Command mode: All

VM Group Configuration

[Table 311](#) 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 311 VM Group Configuration Options

Command Syntax and Usage

virt vmgroup <1-1024> **vlan** <VLAN number>

Assigns a VLAN to this VM group. If you do not assign a VLAN to the VM group, the switch automatically assigns the first unused VLAN when adding a port or a VM to the VM Group.

Note: If you add a VM profile to this group, the group will use the VLAN assigned to the profile.

Command mode: Global configuration

[no] virt vmgroup <1-1024> **vmap** <VMAP number>
serverports | **non-serverports**

Assigns the selected VLAN Map to this group. You can choose to limit operation of the VLAN Map to server ports only or non-server ports only. If you do not select a port type, the VMAP is applied to the entire VM Group.

For more information about configuring VLAN Maps, see [“VMAP Configuration” on page 306](#).

Command mode: Global configuration

[no] virt vmgroup <1-1024> **tag**

Enables or disables VLAN tagging on ports in this VM group.

Command mode: Global configuration

virt vmgroup <1-1024> **vm** [**<MAC address>** | **<UUID>** | **<name>** | **<IP address>** | **<index number>**]

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**).

The VM index number is found in the VM information dump (**show virt vm**).

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.

Command mode: Global configuration

Table 311 VM Group Configuration Options

Command Syntax and Usage

no virt vmgroup <1-1024> **vm** [*<MAC address>* | *<UUID>* | *<name>* | *<IP address>* | *<index number>*]

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**).

Command mode: Global configuration

virt vmgroup <1-1024> **profile** *<profile name (1-39 characters)>*

Adds the selected VM profile to the VM group.

Command mode: Global configuration

no virt vmgroup <1-1024> **profile**

Removes the VM profile assigned to the VM group.

Command mode: Global configuration

virt vmgroup <1-1024> **port** *<port alias or number>*

Adds the selected port to the VM group.

Note: A port can be added to a VM group only if no VMs on that port are members of the VM group.

Command mode: Global configuration

no virt vmgroup <1-1024> **port** *<port alias or number>*

Removes the selected port from the VM group.

Command mode: Global configuration

virt vmgroup <1-1024> **portchannel** *<trunk number>*

Adds the selected trunk group to the VM group.

Command mode: Global configuration

no virt vmgroup <1-1024> **portchannel** *<trunk number>*

Removes the selected trunk group from the VM group.

Command mode: Global configuration

Table 311 VM Group Configuration Options**Command Syntax and Usage**

```
virt vmgroup <1-1024> key <1-65535>
```

Adds an LACP *admin key* to the VM group. LACP trunks formed with this *admin key* will be included in the VM group.

Command mode: Global configuration

```
no virt vmgroup <1-1024> key <1-65535>
```

Removes an LACP *admin key* from the VM group.

Command mode: Global configuration

```
virt vmgroup <1-1024> stg <STG number>
```

Assigns the VM group to a Spanning Tree Group (STG).

Command mode: Global configuration

```
no virt vmgroup <1-1024>
```

Deletes the VM group.

Command mode: Global configuration

```
show virt vmgroup <1-1024>
```

Displays the current VM group parameters.

Command mode: All

VM Profile Configuration

[Table 312](#) describes the VM Profiles configuration options.

Table 312 VM Profile Configuration Options**Command Syntax and Usage**

```
virt vmprofile <profile name (1-39 characters)>
```

Defines a name for the VM profile. The switch supports up to 32 VM profiles.

Command mode: Global configuration

```
no virt vmprofile <profile name (1-39 characters)>
```

Deletes the selected VM profile.

Command mode: Global configuration

Table 312 VM Profile Configuration Options

Command Syntax and Usage

virt vmprofile edit *<profile name (1-39 characters)>* **vlan** *<VLAN number>*

Assigns a VLAN to the VM profile.

Command mode: Global configuration

[no] virt vmprofile edit *<profile name (1-39 characters)>* **shaping**
[*<average (1-1000000000)>* *<burst (1-1000000000)>* *<peak (1-1000000000)>*]

Configures traffic shaping parameters implemented in the hypervisor, as follows:

- Average traffic, in Kilobits per second
- Maximum burst size, in Kilobytes
- Peak traffic, in Kilobits per second
- Delete traffic shaping parameters.

Command mode: Global configuration

show virt vmprofile [*<profile name>*]

Displays the current VM Profile parameters.

Command mode: All

VM Ware Configuration

[Table 313](#) 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 313 VM Ware Configuration Options

Command Syntax and Usage

virt vmware hbport *<1-65535>*

Configures the UDP port number used for heartbeat communication from the VM host to the Virtual Center. The default value is port 902.

Command mode: Global configuration

Table 313 VM Ware Configuration Options

Command Syntax and Usage

[no] virt vmware vcspec [*<IP address>*] [*<username>* **noauth**]

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:

- IP address of the Virtual Center
- User name and password for the Virtual Center
- Whether to authenticate the SSL security certificate (yes or no)

Command mode: Global configuration

show virt vmware

Displays the current VMware parameters.

Command mode: All

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 473](#).

Saving the Active Switch Configuration

When the `copy running-config {ftp|tftp}` 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 server. To start the switch configuration upload, at the prompt, enter:

```
Router(config)# copy running-config ftp  
  
    or  
  
Router(config)# copy running-config tftp
```

The switch prompts you for the server address and filename.

Note – 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).

Note – 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} 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  
  
    or  
  
Router(config)# copy tftp running-config
```

The switch prompts you for the server address and filename.

USB Copy

If a USB drive is inserted into the USB port, you can copy files from the switch to the USB drive, or from the USB drive to the switch. You also can boot the switch using software or configuration files found on the USB drive (see [“USB Boot Configuration” on page 413](#)).

Copy to USB

Use the following command to copy a file from the switch to the USB drive:

```
usbcopy tousb <filename> {boot|image1|active|syslog|crashdump}
```

Command mode: Privileged EXEC

In this example, the active configuration file is copied to a directory on the USB drive:

```
G8264(config)# usbcopy tousb a_folder/myconfig.cfg active
```

Copy from USB

Use the following command to copy a file from the USB drive to the switch:

```
usbcopy fromusb <filename> {boot|image1|active}
```

Command mode: Privileged EXEC

In this example, the active configuration file is copied from a directory on the USB drive:

```
G8264(config)# usbcopy fromusb a_folder/myconfig.cfg active
```

The new file replaces the current file.

Note – Do not use two consecutive dot characters (..). Do not use a slash character (/) to begin a 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 314 General Operations Commands

Command Syntax and Usage

password *<1-128 characters>*

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.

Command Mode: Privileged EXEC

access tnetsshc

Closes all open Telnet and SSH connections.

Command Mode: Global configuration

clear logging

Clears all Syslog messages.

Command Mode: Privileged EXEC

ntp send

Allows the user to send requests to the NTP server.

Command Mode: Privileged EXEC

Operations-Level Port Commands

Operations-level port options are used for temporarily disabling or enabling a port, and for re-setting the port.

Table 315 Port Operations

Command Syntax and Usage

no interface port *<port number or alias>* **shutdown**

Temporarily enables the port. The port will be returned to its configured operation mode when the switch is reset.

Command Mode: Privileged EXEC

interface port *<port number or alias>* **shutdown**

Temporarily disables the port. The port will be returned to its configured operation mode when the switch is reset.

Command Mode: Privileged EXEC

interface port *<port number or alias>* **learning**

Temporarily enables FDB learning on the port.

Command Mode: Privileged EXEC

no interface port *<port number or alias>* **learning**

Temporarily disables FDB learning on the port.

Command Mode: Privileged EXEC

show interface port *<port number or alias>* **operation**

Displays the port interface operational state.

Command Mode: Privileged EXEC

Operations-Level FCoE Commands

Fiber Channel over Ethernet (FCoE) operations commands are listed in the following table.

Table 316 FCoE Operations

Command Syntax and Usage

no fcoe fips fcf <MAC address>

Deletes the selected FCoE Forwarder (FCF), and any associated ACLs.

Command Mode: Privileged EXEC

Operations-Level VRRP Commands

Table 317 Virtual Router Redundancy Operations

Command Syntax and Usage

router vrrp backup {<virtual router number (1-255)> | **group**}

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:

- 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.

Command Mode: Privileged EXEC

Operations-Level BGP Commands

Table 318 IP BGP Operations

Command Syntax and Usage

router bgp start *<peer number>*

Starts the peer session.

Command Mode: Privileged EXEC

router bgp stop *<peer number>*

Stops the peer session.

Command Mode: Privileged EXEC

show ip bgp state

Displays the current BGP operational state.

Command Mode: Privileged EXEC

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 319 VMware Operations

Command Syntax and Usage

virt vmware pg [*<Port Group name>* *<host ID>* *<VSwitch name>* *<VLAN number>*
<shaping-enabled> *<average-Kbps>* *<burst-KB>* *<peak-Kbps>*]

Adds a Port Group to a VMware host. You are prompted for the following information:

- 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.

Command Mode: Privileged EXEC

Table 319 VMware Operations

Command Syntax and Usage

virt vmware vsw *<host ID>* *<Virtual Switch name>*

Adds a Virtual Switch to a VMware host. Use one of the following identifiers to specify the host:

- UUID
- IP address
- Host name

Command Mode: Privileged EXEC

no virt vmware pg *<Port Group name>* *<host ID>*

Removes a Port Group from a VMware host. Use one of the following identifiers to specify the host:

- UUID
- IP address
- Host name

Command Mode: Privileged EXEC

no virt vmware vsw *<host ID>* *<Virtual Switch name>*

Removes a Virtual Switch from a VMware host. Use one of the following identifiers to specify the host:

- UUID
- IP address
- Host name

Command Mode: Privileged EXEC

virt vmware export *<VM profile name>* *<VMware host ID>* *<Virtual Switch name>*

Exports a VM Profile to a VMware host.

Use one of the following identifiers to specify each host:

- UUID
- IP address
- Host name

You may enter a Virtual Switch name, or enter a new name to create a new Virtual Switch.

Command Mode: Privileged EXEC

Table 319 VMware Operations

Command Syntax and Usage

virt vmware scan

Performs a scan of the VM Agent, and updates VM information.

Command Mode: Privileged EXEC

virt vmware vmacpg <MAC address> <Port Group name>

Changes a VM NIC's configured Port Group.

Command Mode: Privileged EXEC

virt vmware updpkg <Port Group name> <host ID> <VLAN number>
[<shaping enabled> <average Kbps> <burst KB> <peak Kbps>]

Updates a VMware host's Port Group parameters. Use one of the following identifiers for the host ID:

- UUID
- IP address
- Host name

Enter the traffic shaping parameters as follows:

- Shaping enabled
- Average traffic, in Kilobits per second
- Maximum burst size, in Kilobytes
- Peak traffic, in Kilobits per second

Delete traffic shaping parameters.

Command Mode: Privileged EXEC

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.

Scheduled Reboot of the Switch

This feature allows the switch administrator to schedule a reboot to occur at a particular time in 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 current reboot schedule.

Table 320 Scheduled Reboot Options

Command Syntax and Usage

boot schedule <day> <time (hh:mm)>

Configures the switch reset time. The following options are valid for the day value:

```
monday
tuesday
wednesday
thursday
friday
saturday
sunday
```

Command Mode: Global configuration

no boot schedule

Cancels the switch reset time.

Command Mode: Global configuration

show boot

Displays the current switch reboot schedule.

Command Mode: All except User EXEC

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 321 Netboot Options

Command Syntax and Usage

boot netboot enable

Enables Netboot. When enabled, the switch boots into factory-default configuration, and attempts to download a new configuration file.

Command Mode: Global configuration

no boot netboot enable

Disables Netboot.

Command Mode: Global configuration

[no] boot netboot tftp <IP address>

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

Table 321 Netboot Options

Command Syntax and Usage

[no] boot netboot cfgfile <1-31 characters>

Defines the file path for the configuration file on the TFTP server. For example:

/directory/sub/config.cfg

Command Mode: Global configuration

show boot

Displays the current Netboot parameters.

Command Mode: All

QSFP Port Configuration

Table 322 QSFP Port Options

Command Syntax and Usage

boot qsfp-40gports <1, 5, 9, 13>

Enables 40GbE mode on the selected QSFP+ ports. When enabled, each QSFP+ port is set as a single 40GbE port.

You must reboot the switch for this change to take effect.

Command Mode: Global configuration

no boot qsfp-40gports <1, 5, 9, 13>

Disables 40GbE mode on the selected QSFP+ ports. When disabled, each QSFP+ port is configured to breakout into four 10GbE ports.

You must reboot the switch for this change to take effect.

Command Mode: Global configuration

show boot qsfp-port-modes

Displays the current QSFP parameters.

Command Mode: All

USB Boot Configuration

USB Boot allows you to boot the switch with a software image file, boot file, or configuration file that resides on a USB drive inserted into the USB port. Use the following command to enable or disable USB Boot:

```
[no] boot usbboot enable
```

Command mode: Global configuration

When enabled, the switch checks the USB port when it is reset. If a USB drive is inserted into the port, the switch checks the drive for software and image files. If a valid file is present on the USB drive, the switch loads the file and boots using the file.

The following list describes the valid file names, and describes the switch behavior when it recognizes them. The file names must be exactly as shown, or the switch will not recognize them.

- `RS8264_Boot.img`
The switch replaces the current boot image with the new image, and boots with the new image.
- `RS8264_OS.img`
The switch boots with the new software image. The existing images are not affected.
- `RS8264_replace1_OS.img`
The switch replaces the current software image1 with the new image, and boots with the new image.
- `RS8264_replace2_OS.img`
The switch replaces the current software image2 with the new image, and boots with the new image.
- `RS8264.cfg`
The switch boots with the new configuration file. The existing configuration files (active and backup) are not affected.
- `RS8264_replace.cfg`
The switch replaces the active configuration file with the new file, and boots with the new file. This file takes precedence over any other configuration files that may be present on the USB drive.

If more than one valid file is present, the switch loads all valid files and boots with them. For example, you may simultaneously load a new boot file, image file, and configuration file from the USB drive.

The switch ignores any files that do not match the valid file names or that have the wrong format.

You also can copy files to and from the USB drive. See [“USB Copy” on page 401](#).

Updating the Switch Software Image

The switch software image is the executable code running on the RackSwitch G8264. 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.

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.

To load a new software image to your switch, you need the following:

- The image or boot software loaded on a 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}
```

2. Select a port to use for downloading the image

```
Port type [DATA|MGT]:
```

3. Enter the hostname or IP address of the FTP or TFTP server.

```
Address or name of remote host: <IP address or hostname>
```

4. 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`).

5. Enter your username and password for the server, if applicable.

```
User name: {<username> | <Enter>}
```

6. The system prompts you to confirm your request.

You should next select a software image to run, as described below.

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}
```

2. Select a port type to use for uploading the image.

```
Port type [DATA|MGT]:
```

3. Enter the name or the IP address of the FTP or TFTP server:

```
Address or name of remote host: <IP address or hostname>
```

4. Enter the name of the file into which the image will be uploaded on the FTP or TFTP server:

```
Destination file name: <filename>
```

5. Enter your username and password for the server, if applicable.

```
User name: {<username>|<Enter>}
```

6. The system then requests confirmation of what you have entered. To have the file uploaded, enter **Y**.

```
image2 currently contains Software Version 6.6.0
that was downloaded at 0:23:39 Thu Jan 3, 2011.
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 RackSwitch G8264, 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 RackSwitch G8264 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 RackSwitch G8264 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 BLADEOS CLI

The default command-line interface for the G8264 is the ISCLI. To access the BLADEOS CLI, enter the following command from the ISCLI:

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

To access the ISCLI, enter the following command from the BLADEOS CLI and reset the G8264:

```
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.

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 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.

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 RackSwitch G8264 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 323 General Maintenance Commands

Command Syntax and Usage

show flash-dump-uuencode

Displays dump information in uuencoded format. For details, see [page 507](#).

Command mode: All

copy flash-dump tftp {data|mgt}

Saves the system dump information via TFTP. For details, see [page 507](#).

Command mode: Privileged EXEC

copy flash-dump ftp {data|mgt}

Saves the system dump information via FTP.

Command mode: Privileged EXEC

clear flash-dump

Clears dump information from flash memory.

Command mode: Privileged EXEC

Table 323 General Maintenance Commands

Command Syntax and Usage

copy log tftp {data|mgt}

Saves the system log file (SYSLOG) via TFTP.

Command mode: Privileged EXEC

clear log

Clears the system log file (SYSLOG).

Command mode: Privileged EXEC

show tech-support

Dumps all G8264 information, statistics, and configuration. You can log the output (tsdmp) into a file.

Command mode: All except User EXEC

copy tech-support tftp {data|mgt}

Redirects the technical support dump (tsdmp) to an external TFTP server.

Command mode: Privileged EXEC

copy tech-support ftp {data|mgt}

Redirects the technical support dump (tsdmp) to an external FTP server.

Command mode: Privileged EXEC

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 324 FDB Manipulation Options

Command Syntax and Usage

show mac-address-table address <MAC address>

Displays a single database entry by its MAC address. Enter the MAC address using one of the following formats:

- xx:xx:xx:xx:xx:xx (such as 08:00:20:12:34:56)
- xxxxxxxxxxxxxx (such as 080020123456)

Command mode: All

show mac-address-table interface port <port number or alias>

Displays all FDB entries for a particular port.

Command mode: All

show mac-address-table vlan <VLAN number>

Displays all FDB entries on a single VLAN.

Command mode: All

show mac-address-table multicast

Displays all Multicast MAC entries in the FDB.

Command mode: All

show mac-address-table static

Displays static entries in the FDB.

Command mode: All except User EXEC

**no mac-address-table {static|multicast} {all|<MAC address>
<VLAN number>}**

Removes static FDB entries.

Command mode: Global configuration

Table 324 FDB Manipulation Options

Command Syntax and Usage

clear mac-address-table

Clears the entire Forwarding Database from switch memory.

Command mode: Privileged EXEC

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

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 325 Miscellaneous Debug Options

Command Syntax and Usage

debug debug-flags

This command sets the flags that are used for debugging purposes.

Command mode: Privileged EXEC

debug mp-trace

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: Privileged EXEC

debug dumpbt

Displays the backtrace log.

Command mode: Privileged EXEC

debug mp-snap

Displays the Management Processor snap (or post-mortem) trace buffer. This buffer contains information traced at the time that a reset occurred.

Command mode: Privileged EXEC

clear flash-config

Deletes all flash configuration blocks.

Command mode: Privileged EXEC

Table 325 Miscellaneous Debug Options

Command Syntax and Usage

debug pstat *<port alias or number>*

Displays all port statistics for the selected port.

Command mode: Privileged EXEC

LLDP Cache Manipulation

[Table 326](#) describes the LLDP cache manipulation commands.

Table 326 LLDP Cache Manipulation Options

Command Syntax and Usage

show lldp port *<port alias or number>*

Displays Link Layer Discovery Protocol (LLDP) port information.

Command mode: All

show lldp receive

Displays information about the LLDP receive state machine.

Command mode: All

show lldp transmit

Displays information about the LLDP transmit state machine.

Command mode: All

show lldp remote-device *<1-256>*

Displays information received from LLDP -capable devices.

Command mode: All

show lldp

Displays all LLDP information.

Command mode: All

clear lldp

Clears the LLDP cache.

Command mode: Privileged EXEC

ARP Cache Maintenance

Table 327 Address Resolution Protocol Maintenance Options

Command Syntax and Usage

show ip arp find *<IP address>*

Shows a single ARP entry by IP address.

Command mode: All

show ip arp interface port *<port number or alias>*

Shows ARP entries on selected ports.

Command mode: All

show ip arp vlan *<VLAN number>*

Shows ARP entries on a single VLAN.

Command mode: All

show ip arp reply

Shows the list of IP addresses which the switch will respond to for ARP requests.

Command mode: All

show ip arp

Shows all ARP entries.

Command mode: All

clear arp

Clears the entire ARP list from switch memory.

Command mode: Privileged EXEC

Note – To display all or a portion of ARP entries currently held in the switch, you can also refer to “ARP Information” on [page 79](#).

IP Route Manipulation

Table 328 IP Route Manipulation Options

Command Syntax and Usage

show ip route address <IP address>

Shows a single route by destination IP address.

Command mode: All

show ip route gateway <IP address>

Shows routes to a default gateway.

Command mode: All

show ip route type {indirect|direct|local|broadcast|
martian|multicast}

Shows routes of a single type. For a description of IP routing types, see [Table 35 on page 77](#)

Command mode: All

show ip route tag {fixed|static|address|rip|ospf|broadcast|
martian|multicast}

Shows routes of a single tag. For a description of IP routing tags, see [Table 36 on page 78](#)

Command mode: All

show ip route interface <IP interface>

Shows routes on a single interface.

Command mode: All

show ip route

Shows all routes.

Command mode: All

clear ip route

Clears the route table from switch memory.

Command mode: Privileged EXEC

Note – To display all routes, you can also refer to [“IP Routing Information” on page 76](#).

IGMP Snooping Maintenance

Table 329 describes the IGMP Snooping maintenance commands.

Table 329 IGMP Multicast Group Maintenance Options

Command Syntax and Usage

show ip igmp groups address *<IP address>*

Displays a single IGMP multicast group by its IP address.

Command mode: All

show ip igmp groups vlan *<VLAN number>*

Displays all IGMP multicast groups on a single VLAN.

Command mode: All

show ip igmp groups interface port *<port number or alias>*

Displays all IGMP multicast groups on selected ports.

Command mode: All

show ip igmp groups portchannel *<trunk number>*

Displays all IGMP multicast groups on a single trunk group.

Command mode: All

show ip igmp groups detail *<IP address>*

Displays detailed information about a single IGMP multicast group.

Command mode: All

show ip igmp groups

Displays information for all multicast groups.

Command mode: All

clear ip igmp groups

Clears the IGMP group table.

Command mode: Privileged EXEC

IGMP Multicast Routers Maintenance

The following table describes the maintenance commands for IGMP multicast routers (Mrouters).

Table 330 IGMP Multicast Router Maintenance Options

Command Syntax and Usage

show ip igmp mrouter vlan *<VLAN number>*

Displays IGMP Mrouter information for a single VLAN.

Command mode: All

show ip igmp mrouter

Displays information for all Mrouters.

Command mode: All

clear ip igmp mrouter

Clears the IGMP Mrouter port table.

Command mode: Privileged EXEC

IPv6 Neighbor Discovery Cache Manipulation

Table 331 describes the IPv6 Neighbor Discovery cache manipulation commands.

Table 331 IPv6 Neighbor Discovery Cache Manipulation Options

Command Syntax and Usage

show ipv6 neighbors find *<IPv6 address>*

Shows a single IPv6 Neighbor Discovery cache entry by IP address.

Command mode: All

show ipv6 neighbors interface port *<port number or alias>*

Shows IPv6 Neighbor Discovery cache entries on a single port.

Command mode: All

show ipv6 neighbors vlan *<VLAN number>*

Shows IPv6 Neighbor Discovery cache entries on a single VLAN.

Command mode: All

show ipv6 neighbors static

Shows static IPv6 Neighbor Discovery cache entries.

Command mode: All

show ipv6 neighbors

Shows all IPv6 Neighbor Discovery cache entries.

Command mode: All

clear ipv6 neighbors

Clears all IPv6 Neighbor Discovery cache entries from switch memory.

Command mode: Privileged EXEC

IPv6 Route Maintenance

Table 331 describes the IPv6 route maintenance commands.

Table 332 IPv6 Route Maintenance Options

Command Syntax and Usage

show ipv6 route address *<IPv6 address>*

Show a single route by destination IP address.

Command mode: All

show ipv6 route gateway *<IPv6 gateway number>*

Show routes to a single gateway.

Command mode: All

show ipv6 route interface *<interface number>*

Show routes on a single IP interface.

Command mode: All

show ipv6 route type {**connected|static|ospf**}

Show routes of a single type.

Command mode: All

show ipv6 route static

Show static IPv6 routes.

Command mode: All

show ipv6 route summary

Shows a summary of IPv6 route information.

Command mode: All

show ipv6 route

Shows all IPv6 routes.

Command mode: All

clear ipv6 route

Clears all IPv6 routes.

Command mode: Privileged EXEC

Uencode Flash Dump

Using this command, dump information is presented in uencoded 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-uencode` command. This will ensure that you do not lose any information. Once entered, the `show flash-dump-uencode` 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-uencode` 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 508](#).

To access dump information, enter:

```
Router# show flash-dump-uencode
```

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 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 <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 FTP, enter:

```
Router# copy flash-dump ftp <server filename>
```

You are prompted for the FTP server IPv4 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, 2011. 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

BLADEOS System Log Messages

The RackSwitch G8264 (G8264) uses the following syntax when outputting system log (syslog) messages:

<Time stamp><Log Label>BLADEOS<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
BGP	session with <IP address> failed <reason type> : <reason> Reason Types: <ul style="list-style-type: none"> ■ FSM Error ■ Hold Timer Expired ■ Message Header Error ■ OPEN Message Error ■ UPDATE Message Error Reasons: <ul style="list-style-type: none"> ■ AS Routing Loop ■ Attr Flags Error ■ Attr Length Error ■ Auth Failure ■ Bad BGP Identifier ■ Bad HoldTime ■ Bad Length ■ Bad Peer AS ■ Bad Type ■ Conn Not Synced ■ Invalid Network Field ■ Invalid NEXTHOP Attr ■ Invalid ORIGIN Attr ■ Malformed AS_PATH ■ Malformed Attr List ■ Missing Well Known Attr ■ None ■ Optional Attr Error ■ Unrecognized Well Known Attr ■ Unsupported Opt Param ■ Unsupported Version
HOTLINKS	LACP trunk <trunk ID> and <trunk ID> formed with admin key <key>

Thread	LOG_ALERT Message (continued)
IP	cannot contact default gateway <IP address>
IP	cannot contact gateway <IP address>
IP	Dynamic Routing table is full
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
RMON	Event.<description>
STP	CIST new root bridge
STP	CIST topology change detected
STP	CIST, interface port <port> [moved into leave from] loop-inconsistent state
STP	CIST, interface port <port> [moved into leave from] root-inconsistent state
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 leaving from] into loop-inconsistent state
STP	Port <port>, [putting port leaving from] into root-inconsistent state
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
STP	Setting STG <STG> Fast Uplink primary port <port> forwarding and backup port <port> blocking

Thread	LOG_ALERT Message (continued)
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>, interface port <port> [moved into leave from] loop-inconsistent state
STP	STG <STG>, interface port <port> [moved into leave from] root-inconsistent state
STP	STG <STG>, new root bridge
STP	STG <STG>, topology change detected
STP	Too many BPDUs flooded in VLAN <VLAN>. Some of them will be discarded!
SYSTEM	Ingress PVST+ BPDU's spotted from port <port>
SYSTEM	LACP trunk <trunk ID> and <trunk ID> formed with admin key <key>
VLAG	vLAG Health check is Down
VLAG	vLAG Health check is Up
VLAG	vLAG ISL down
VLAG	vLAG ISL is up
VLAG	vLAG on LACP key <key> is [up down]
VLAG	vLAG on portchannel <trunk ID> is [up down]
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 adver type 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	Can't assign a port with same protocol to different VLANs.
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	ERROR: Cannot enable/disable RMON for Mgmt Port <port>
CFG	ERROR: More than <maximum> VLAN(s) in downstream
CFG	Error writing active config to FLASH! Another save is in progress
CFG	Maximum allowed number (30) of Alarm groups have already been created.
CFG	Maximum allowed number (30) of Event groups have already been created.
CFG	Maximum allowed number (5) of History groups have already been created.
CFG	Need to enable port's tag for tagging pvlan.
CFG	Overflow! Port has more than 16 protocols.
CFG	Port is not for this protocol.
CFG	Switch rem port fails when disable {protocol vlan}.
CFG	TFTP {Copy cfgRcv} attempting to redirect a previously redirected output
CFG	WARN: Have not defined protocol type for VLAN <VLAN> Protocol <protocol>!
DCBX	Duplicate DCBX Application Protocol Sub-TLV detected on port <port>
DCBX	Duplicate DCBX Control Sub-TLV detected on port <port>
DCBX	Duplicate DCBX PFC Sub-TLV detected on port <port>
DCBX	Duplicate DCBX PG Sub-TLV detected on port <port>
DCBX	Duplicate DCBX VNIC Sub-TLV detected on port <port>
IP6	EXCEPTIONAL CASE Trying to create IP6 Interface after the Ip6Shutdown

Thread	LOG_ERR Message (continued)
IP6	Ip6SetAddr(failed):if=<interface>, rc=<reason code>
IP6	IPv6 route table full
IP6	ipv6_add_interface_immediate: Buffer Non Linear for ip6_cfa_params
IP6	ipv6_add_nbrcache_immediate: Buffer Non Linear for ip6_cfa_params
IP6	ipv6_add_prefix_immediate: Buffer Non Linear for ip6_cfa_params
IP6	ipv6_rem_prefix_immediate: Buffer Non Linear for ip6_cfa_params
IP6	ipv6_rem_route_immediate: Buffer Non Linear for ip6_cfa_params
IP6	ipv6_vlan_change_immediate: Buffer Non Linear for ip6_cfa_params
LLDP	Error: Port <port> has the PVID <PVID> that is different from the PVID <PVID> configured on the peer
LLDP	Port <port>: Cannot add new entry. MSAP database is full!
MGMT	Apply is issued by another user. Try later
MGMT	cannot contact {primary secondary} DNS server <IP address> - {Mgmt Ext-mgt} port unavailable
MGMT	Critical Error. Failed to add Interface <interface>
MGMT	Critical Error. Failed to {add attach} Loopback Interface <interface>
MGMT	Critical Error. Failed to detach Loopback 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: Pushed {image1 image2} size <bytes> bigger than the capacity <maximum bytes>.
MGMT	Error: Invalid {image1 image2}
MGMT	Error: Pushed {image1 image2} size <bytes> bigger than the capacity <maximum bytes>.
MGMT	Error: Save not done.
MGMT	Firmware download failed (insufficient memory)
MGMT	Invalid CRC value. Boot image rejected

Thread	LOG_ERR Message (continued)
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
MGT	You are attempting to load an image that has been corrupted or belongs to another switch type. Please verify you have the correct file for this switch and try again. [Error: Invalid header magic value <value>.] Boot image rejected
NTP	unable to listen to NTP port
RMON	Maximum {Alarm Event History} groups exceeded when trying to add group <group> via SNMP
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	Error: DHCP Offer was found invalid by ip configuration checking; please see system log for details.
SYSTEM	I2C device <ID> <description> set to access state <state> [from CLI]
SYSTEM	Not enough memory!
SYSTEM	Port <port> disabled. Link params(speed/mode) mismatch with <trunk name> <trunk ID>
SYSTEM	Port <port> disabled. Same LACP admin_key with port "PORT_INT_<port> rent link params(speed/mode)"
SYSTEM	{PortChannel Trunk group} creation failed for {IntPortChannel PortChannel Internal Trunk group Trunk group} <trunk ID>. Only <maximum trunks> {PortChannels Trunk groups} supported by hardware.
VRRP	Virtual Router Group is disabled due to no enabled virtual routers.

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 image changed
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	boot kernel Firmware uploaded.
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: Static FDB entry on inexistent VLAN
MGMT	Error in setting the new config
MGMT	Failed to allocate buffer for diff track.

Thread	LOG_INFO Message (continued)
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 <hostname>:<filename>
MGMT	FLASH ERROR - invalid address used
MGMT	Flash Read Error. Failed to read flash into holding structure. Quitting
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	image1 2 Firmware uploaded.
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	invalid image Firmware uploaded.
MGMT	NETBOOT: Config successfully downloaded and applied from <hostname>:<filename>
MGMT	New config set

Thread	LOG_INFO Message (continued)
MGMT	new configuration applied [from BBI EM NETBOOT SCP SNMP Stacking Master]
MGMT	new configuration saved from { BBI BladeOS ISCLI SNMP }
MGMT	Revert failed: configuration is dumped or modified by another user.
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	SP boot kernel Firmware uploaded.
MGMT	Starting Firmware download for {invalid image image1 image2 boot kernel undefined SP boot kernel}.
MGMT	Static FDB entry on disabled VLAN
MGMT	Static FDB entry on invalid 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.
MGMT	Unable to do revert apply. The current configuration is in ISCLI format, it needs to be saved in BladeOS format.
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	undefined Firmware uploaded.
MGMT	unsaved changes reverted [from BBI from SNMP]

Thread	LOG_INFO Message (continued)
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
NETCONF	<username> (<user level>) connection closed from address via NETCONF over <connection type>
NETCONF	<username> (<user level>) login from host <IP address> via NETCONF over <connection type>
RMON	RMON {alarm event history} index <ID> was deleted via SNMP
RMON	SNMP configuration for RMON {alarm event history} index <ID> applied
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
SYSTEM	FDB Learning {DISABLED ENABLED} for port <port>
SYSTEM	Insert another transceiver or change configuration and manually enable port <port>
TFTP	Successfully sent {boot image image1 mage2} to switch <MAC address>

LOG_NOTICE

Thread	LOG_NOTICE Message
	<minutes> {minute minutes} until scheduled reboot
	ARP table is full.
	Current config successfully tftp'd <filename> from <hostname>
	Current config successfully tftp'd to <hostname>: <filename>
	ECMP route configured, Gateway health check enabled
	More than one trunk found for LACP adminkey <adminkey>. Static MAC entry <index> was added only to trunk <trunk number>.
	Number of COSqs has been changed since boot. Save and reset the switch to activate the new configuration.
	Port <port> mode is changed to full duplex for 1000 Mbps operation.
	scheduled switch reboot
	switch reset at <time> has been canceled
	switch reset scheduled at <time>
	Warning: DHCP on IF <interface> will be disabled
8021X	Could not create failover checkpoint record for port <port>
8021X	Logoff request on port <port>
8021X	Port <port> {assigned to removed from} vlan <VLAN>
8021X	RADIUS server <IP address> auth response for port <port> has an invalid Tunnel-Type value (<tunnel type>); should be 13 for VLAN assignment
8021X	RADIUS server <IP address> auth response for port <port> has an invalid Tunnel-Medium-Type value (<tunnel type>); should be 6 for VLAN assignment
8021X	RADIUS server <IP address> auth response for port <port> is missing one or more tunneling attributes for VLAN assignment
8021X	RADIUS server <IP address> auth response has a VLAN id (<VLAN>) of a reserved VLAN and cannot be assigned to port <port>
8021X	RADIUS server <IP address> auth response has a VLAN id (<VLAN>) of a non-existent or disabled VLAN, and cannot be assigned to port <port>

Thread	LOG_NOTICE Message (continued)
8021X	RADIUS server <IP address> auth response has an invalid VLAN id (<VLAN>) and cannot be assigned to port <port>
BGP	bad authentication received / no authentication received / authentication receive error from <IP address>
BGP	session established with <IP address>
CONSOLE	RADIUS: authentication timeout. Retrying...
CONSOLE	RADIUS: failed to contact primary secondary server
CONSOLE	RADIUS: No configured RADIUS server
CONSOLE	RADIUS: trying alternate server...
DCBX	Detected DCBX peer on port <port>
DCBX	Feature "{DCBX ETS PFC App Proto VNIC ETS}" not supported by peer on port <port>
DCBX	LLDP [TX &] RX are disabled on port <port>
DCBX	LLDP TX is disabled on port <port>
DCBX	Not able to detect DCBX peer on port <port>
DCBX	Peer on port port stopped responding to DCBX message
FCOE	Failed to create FCOE vlan <VLAN>
FCOE	FCF <MAC address> has been removed.
FCOE	FCF <MAC address> is now operational.
FCOE	FCOE connection between VN_PORT <MAC address> and FCF <MAC address> {has been established is down}.
FCOE	FCOE vlan <VLAN> created.
FCOE	Port <port> has been added to the FCOE vlan <VLAN>.
FCOE	VN_PORT <MAC address> has been reassigned, the old connection will be deleted.
HOTLINKS	"Error" is set to "Standby Active"
HOTLINKS	"Learning" is set to "Standby Active"
HOTLINKS	"None" is set to "Standby Active"

Thread	LOG_NOTICE Message (continued)
HOTLINKS	"Side Max" is set to "Standby Active"
HOTLINKS	has no "{Side Max None Learning Error}" interface
IP	cannot contact multicast router <IP address>
IP	Either Route or Arp table is full. Please check GEA L3 statistics (/stat/l3/gea) to verify.
IP	IGMP - {L3 IPMC L3 IPv4 Multicas Backup UP groups Backup DOWN groups IGMP groups IPMC} table is full!
IP	IGMP - V1 timer is running for group <IP address>, vlan <VLAN>[, port <port>] Ignored leave!
IP	L3 table is full. Please check GEA L3 statistics (/stat/l3/gea) to verify.
IP	mrouter <IP address> has been disabled or deleted
IP	multicast router <IP address> operational
IP	On Vlan <VLAN> IGMP version updated to <version>
IP	Received {IGMPv1 IGMPv2} query from <IP address>
IP	VLAN <VLAN> is not in the igmp relay list. Mrouter <IP address> will be down
IP	Warning: DHCP on IF <interface> will be disabled
IP	Warning: Enabling dhcp will delete IP interface <interface> and IP gateway <gateway>'s configurations.
IP	Warning: gateway (<gateway>) will be deleted
LACP	All supported trunks already created. Port <port> will be disabled by LACP.
LACP	LACP is {up down} on port <port>
LINK	link {down up} on port <port>
LINK	Port <port> disabled by PVST Protection
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}

Thread	LOG_NOTICE Message (continued)
MGMT	ACL <old number> from old configuration file moved to ACL <new number> in new configuration file
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	Boot profile 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
MGMT	Log msg no. <x>
MGMT	Membership for Port <port> in vlan <VLAN> is not effective while the port is assigned with PVID <PVID> by 802.1x
MGMT	MGTA B Gateway <IP address> not in the same subnet as the Mgt IP <IP address>/<netmask>
MGMT	New config set
MGMT	new configuration saved from ISCLI
MGMT	New Management IP Address <IP address> configured
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	Port <port> remains untagged while it is assigned PVID <PVID> by 802.1x

Thread	LOG_NOTICE Message (continued)
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
NETCONF	<username> (<user level>) connection closed from address via NETCONF over <connection type>
NETCONF	<username> (<user level>) login from host <IP address> via NETCONF over <connection type>
NTP	System clock updated

Thread	LOG_NOTICE Message (continued)
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}
OSPFV3	Link state database is FULL.Ignoring LSA.
OSPFV3	nbr <router ID> changes state from {DOWN ATTEMPT INIT 2WAY EXSTART EXCHANGE LOADING FULL} to {DOWN ATTEMPT INIT 2WAY EXSTART EXCHANGE LOADING FULL}[, Neighbor Down: {Interface down or detached Dead timer expired}]
OSPFV3	virtual link nbr <router ID> changes state from {DOWN ATTEMPT INIT 2WAY EXSTART EXCHANGE LOADING FULL} to {DOWN ATTEMPT INIT 2WAY EXSTART EXCHANGE LOADING FULL}[, Neighbor Down: {Interface down or detached Dead timer expired}]
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	<SPF name> TX Fault - <SFP type> is DISABLED
SYSTEM	<SPF name> UnApproved - <SFP type> is DISABLED
SYSTEM	<SFP type> inserted at port <port> is UNAPPROVED ! Device is DISABLED.
SYSTEM	Address for interface <interface> ignored because of mismatch.
SYSTEM	BOOTP Offer (continue): Domain name: <domain>
SYSTEM	BOOTP Offer (continue): Host name: <host>

Thread	LOG_NOTICE Message (continued)
SYSTEM	BOOTP Offer (continue): Primary DNS: <IP address>, Secondary DNS: <IP address>
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	Could not add L2 multicast entry! L2 table is full.
SYSTEM	ECMP route gateway <IP address> [via if <interface>] is {down up}
SYSTEM	Enable auto negotiation for copper GIG port: <port>
SYSTEM	Fan Fault {Detected Cleared}. Fan <fan number> RPM <RPM value>
SYSTEM	Fan Failure Warning Cleared
SYSTEM	I2C device <ID> <description> set to access state <state> [from CLI]
SYSTEM	L2 table is full!
SYSTEM	Mask for interface <interface> ignored because of mismatch.
SYSTEM	**** MAX TEMPERATURE (<temperature>) ABOVE FAIL THRESH ****
SYSTEM	**** MAX TEMPERATURE (<temperature>) ABOVE WARN THRESH ****
SYSTEM	**** PLATFORM THERMAL SHUTDOWN ****
SYSTEM	Port <port> disabled
SYSTEM	Port <port> disabled by BPDU Guard
SYSTEM	Port <port> disabled by OAM (unidirectional TX-RX Loop)
SYSTEM	Port <port> disabled by UDLD (unknown unidirectional bidirectional TX-RX loop neighbor mismatch)
SYSTEM	Port <port> disabled due to reason code <reason code>
SYSTEM	Power Fault {Cleared Detected} - <number>
SYSTEM	Power Supply Warning Cleared

Thread	LOG_NOTICE Message (continued)
SYSTEM	rebooted (<reason>)[, administrator logged in] Reason: <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 ■ 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
SYSTEM	Received BOOTP Offer: IP: <IP address>, Mask: <netmask>, Broadcast <IP address>, GW: <IP address>
SYSTEM	Received DHCP Offer: IP: <IP address>, Mask: <netmask> Broadcast <IP address>, GW: <IP address>
SYSTEM	server with MAC address <MAC address> was {added to removed from} network
SYSTEM	Static route gateway <IP address> is {down up}
SYSTEM	Warning: Fan Failure
SYSTEM	Warning: Power Supply Disconnected or Failure
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

Thread	LOG_NOTICE Message (continued)
VLAN	Default VLAN can not be deleted
VM	<IP address> moved from {port <port> trunk IT <trunk ID>} to {port <port> trunk IT <trunk ID>}
VM	MAC address <MAC address> moved from {port <port> trunk IT <trunk ID>} to {port <port> trunk IT <trunk ID>}
VM	[(Refresh)] VI server unreachable or certificate invalid.
VM	Virtual Machine with {IP address <IP address> MAC address <MAC address>} came online
VM	Virtual Machine with {IP address <IP address> MAC address <MAC address>} changed its VLAN to <new VLAN>. It was previously in VLAN <old VLAN>
VM	Virtual Machine with {IP address <IP address> MAC address <MAC address>} is a member of VLAN <VLAN>
VM	Virtual Machine with {IP address <IP address> MAC address <MAC address>} is not in VLAN <VLAN> anymore
VM	[(Refresh)] VM agent command not implemented.
VM	[(Refresh)] VM agent could not be started.
VM	[(Refresh)] VM agent could not login to server.
VM	[(Refresh)] VM agent could not retrieve {host VM} properties.
VM	[(Refresh)] VM agent encountered a file error.
VM	[(Refresh)] VM agent encountered an IPC error.
VM	[(Refresh)] VM agent file error.
VM	[(Refresh)] VM Agent not active.
VM	[(Refresh)] VM agent operation failed due to a conflict.
VM	[(Refresh)] VM agent operation failed.
VM	[(Refresh)] VM agent operation needs no change.
VM	[(Refresh)] VM agent operation timed out.
VM	[(Refresh)] VM agent protocol error.
VM	VM agent resumed (Refresh).
VM	VM agent resumed (Scan).

Thread	LOG_NOTICE Message (continued)
VM	[(Refresh)] VM agent timed out and could not be stopped.
VM	[(Refresh)] VM agent timed out.
VM	[(Refresh)] VM agent unable to logout from server.
VM	[(Refresh)] VM agent unknown error.
VM	[(Refresh)] VM agent VE limit reached.
VM	[(Refresh)] VM agent: Invalid ID.
VM	VM agent: local table full.
VM	VM MAC <MAC address> NOT added to hash table
VM	VM move detected but failed to move network conf
VRRP	virtual router <IP address> is now {BACKUP MASTER }
WEB	<username> ejected from BBI
WEB	<username> ejected from BBI because username password was changed
WEB	RSA host key is being saved to Flash ROM, please don't reboot the box immediately.

LOG_WARNING

Thread	LOG_WARNING Message
	Static IPMC route group <group number> on vlan <VLAN> [primary backup] has been converted to a host route group because IGMP snooping is enabled.
8021X	Authentication session terminated with {Failure Success} on port <port>
8021X	Could not create failover checkpoint record for port <port>
8021X	Logoff request on port <port>
8021X	Port <port> {assigned to removed from} vlan <VLAN>
8021X	RADIUS server <IP address> auth response for port <port> has an invalid Tunnel-Type value (<tunnel type>); should be 13 for VLAN assignment
8021X	RADIUS server <IP address> auth response for port <port> has an invalid Tunnel-Medium-Type value (<tunnel type>); should be 6 for VLAN assignment
8021X	RADIUS server <IP address> auth response for port <port> is missing one or more tunneling attributes for VLAN assignment
8021X	RADIUS server <IP address> auth response has a VLAN id (<VLAN>) of a reserved VLAN and cannot be assigned to port <port>
8021X	RADIUS server <IP address> auth response has a VLAN id (<VLAN>) of a non-existent or disabled VLAN, and cannot be assigned to port <port>
8021X	RADIUS server <IP address> auth response has an invalid VLAN id (<VLAN>) and cannot be assigned to port <port>
CFG	Authentication should be disabled to run RIPv2 in RIPv1 compatibility mode on interface <interface>.
CFG	Configured {sip dip protocol tcp14 udp14 port dport} hashing without tcp14 or udp14. {sip dip protocol tcp14 udp14 port dport} hashing will be ignored!
CFG	Configured {sip dip protocol tcp14 udp14 port dport} hashing without sport or dport. {sip dip protocol tcp14 udp14 port dport} hashing will be ignored!
CFG	Multicast should be disabled to run RIPv2 in RIPv1 compatibility mode on interface <interface>.
CFG	Static IPMC route group <IP address> on vlan <VLAN> [primary backup] has been converted to a host route group because IGMP snooping is enabled.
CFG	Switch cannot support more than 16 protocols simultaneously!

Thread	LOG_WARNING Message (continued)
CFG	Trunk hash changed, Dataplane L3 hash includes configured Trunk hash and ECMP hash
CFG	Unfit config exists when protocol-vlan apply.
DCBX	Feature "{DCBX ETS PFC App Proto VNIC ETS}" not supported by peer on port <port>
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
IP	<IP address> configured as V<version> and received IGMP V{1 2} query
IP	IGMP: Switch Querier {disabled enabled} on Vlan <VLAN>
IP	IGMP: Switch {became is no longer} a Querier for Vlan <VLAN>
IP	IGMP: Switch is [not] elected as Querier for Vlan <VLAN>
IP	IGMP: Switch Querier election process started for Vlan <VLAN>
IP	IGMP: Switch Querier election type changed for Vlan <VLAN>
IP	IGMP: Warning Querier Source-IP is not configured on Vlan <VLAN> Queries with Source-IP Zero may be ignored in Querier election process.
IP	IGMP: Warning Snooping is not enabled on Vlan <VLAN>, Querier configured only to send queries.
IP	New Multicast router learned on <IP address>, Vlan <VLAN>, Version {V1 V2 V3}
LLDP	ERROR!!! The request port item <item> is invalid
NTP	cannot contact NTP server <IP address> - {Mgmt Ext-mgt} port unavailable
NTP	cannot contact [primary secondary] NTP server <IP address>
SYSTEM	I2C device <ID> <description> set to access state <state> [from CLI]
SYSTEM	Interface <interface> failed to renew DHCP Lease.
TEAMING	error, action is undefined

Thread	LOG_WARNING Message (continued)
TEAMING	is down, but teardown is blocked
TEAMING	is down, control ports are auto disabled
TEAMING	is up, control ports are auto controlled
VNIC	Peer does not support VNIC on port <port>

Index

Numerics

802.1p information	114
802.1X	310

A

abbreviating commands (CLI)	27
access control	
user	258
ACL IPv6	296
ACL Port commands	273
ACL port mirroring	287
ACL re-marking (IPv6)	299
ACL statistics	213
active configuration block	222, 489
active IP interface	434
active port	
VLAN	434
active switch configuration	
gtcfg	473
ptcfg	473
restoring	473
active switch, saving and loading configuration	473
addr	
IP route tag	78
administrator account	29
aging	
STP information	64, 67
autonomous system filter action	373
autonomous system filter path	
action	373
as	373
aspath	373

B

backup configuration block	489
bandwidth allocation	
Priority Groups	452

BGP

configuration	403
eBGP	403
filters, aggregation configuration	409
iBGP	403
in route	406
IP address, border router	405
IP route tag	78
keep-alive time	405
peer	403
peer configuration	405
redistribution configuration	408
remote autonomous system	405
router hops	406
BLOCKING (port state)	65
Boot Management menu	491
Boot options	481
bootstrap protocol	424
Border Gateway Protocol	78
configuration	403
Border Gateway Protocol (BGP)	
operations-level options	478
BPDU	322
bridge priority	64, 70
Bridge Protocol Data Unit	322
Bridge Protocol Data Unit (BPDU)	64, 70
Bridge Spanning-Tree parameters	322
broadcast	
IP route tag	78
IP route type	78

C

capture dump information to a file	507
CEE configuration	451
Cisco Ether Channel	332
CIST information	69
clear	
dump information	508

command (help)	25
commands	
abbreviations	27
conventions used in this manual	16
shortcuts	27
tab completion	28
commands, ISCLI	
modes	22
configuration	
CISTCISTCommon Internal Spanning Tree ...	317
default gateway interval, for health checks	361
default gateway IP address	361
dump command	472
failover	341
flow control	271
IP static route	363
port mirroring	307
port trunking	332
save changes	222
switch IP address	357
VLAN default (PVID)	266
VLAN IP interface	358
VLAN tagging	267
configuration block	
active	489
backup	489
factory	489
selection	489
Configuration commands	221
configuring routing information protocol	375
control plane protection (CoPP)	281
Converged Enhanced Ethernet	451
CoPP (control plane protection)	281
COS queue information	114
cost	
STP information	65, 67, 70
STP port option	324
CPU statistics	210
CPU utilization	210
D	
daylight savings time	223
DCB Capability Exchange Protocol	454
DCBX configuration	454
DCBX information	131
debugging	495
default gateway	
information	75
interval, for health checks	361
default password	29
delete	
FDB entry	497
DHCP Snooping	449
direct (IP route type)	77
directed broadcasts	368
DISABLED (port state)	65
disconnect idle timeout	29
downloading software	486
dump	
configuration command	472
maintenance	495
duplex mode	
link status	31, 122
dynamic routes	502
E	
ECMP hashing configuration	363
ECMP route information	98
ECN (Explicit Congestion Notification)	283
Enhanced Transmission Selection	451
ENode	456
Error disable and recovery	
system	225
error disable and recovery	
port	269
EtherChannel	
as used with port trunking	332
ETS configuration	451
ETS Priority Group	452
Explicit Congestion Notification (ECN)	283
F	
factory configuration block	489
failover	
configuration	341
FCF port	456
FCoE configuration	455
FCoE Forwarding	456
FCoE Initialization Protocol	456
FCoE statistics	214
FDB statistics	162
Fiber Channel over Ethernet	455
FIP Snooping	456
fixed	
IP route tag	78
flag field	80
flow control	31, 122
configuring	271

forwarding configuration		
IP forwarding configuration	368	
forwarding database (FDB)	495	
delete entry	497	
Forwarding Database Information	52	
Forwarding Database maintenance	497	
forwarding state (FWD)	53, 64, 70, 71	
fwd (STP bridge option).....	323	
FwdDel (forward delay), bridge port	64, 67, 70	
G		
gateway		
IPv6	442	
gctfg (TFTP load command).....	473	
H		
health checks		
default gateway interval, retries	361	
retry, number of failed health checks	361	
hello		
STP information	64, 67, 70	
help.....	25	
Hot Links configuration	345	
hot-standby failover.....	432	
hprompt		
system option	224	
HTTPS	261	
I		
ICMP statistics	184	
idle timeout		
overview.....	29	
IEEE standards		
802.1d	64, 321	
802.1s	316	
802.1w	316	
802.1x	50, 63	
IGMP configuration.....	410	
IGMP information	99	
IGMP Relay.....	413	
IGMP Snooping	411	
IGMP statistics.....	189	
image		
downloading	486	
software, selecting	487	
indirect (IP route type).....	77	
Information commands	31	
Interface change stats.....	194, 199	
IP address		
ARP information	79	
configuring default gateway	361	
IP forwarding		
directed broadcasts	368	
IP forwarding information.....	75	
IP Information	75, 106	
IP interface		
active	434	
configuring address.....	357	
configuring VLANs	358	
IP interfaces.....	77	
information.....	75	
IP route tag	78	
priority increment value (ifs) for VRRP	436	
IP network filter configuration.....	369	
IP Route Manipulation.....	502	
IP routing		
tag parameters	78	
IP Static Route commands	363	
IP statistics	174	
IPv6 ACL.....	296	
IPv6 default gateway	442	
IPv6 ND prefix	445	
IPv6 Neighbor Discovery.....	359	
IPv6 Neighbor Discovery cache.....	444	
IPv6 Neighbor Discovery Prefix information	105	
IPv6 Path MTU.....	444	
IPv6 route information.....	96	
IPv6 static route	443	
ISCLI commands		
modes	22	
L		
LACP	339	
Layer 2 commands	47	
Layer 3 commands	74	
LDAP	236	
LEARNING (port state).....	64, 65, 70	
LED, Service Required	225	
Lightweight Directory Access Protocol	236	
Link Aggregation Control Protocolconfiguration		
LACP	339	
Link Flap Dampening (LFD).....	226	
Link Layer Detection Protocol.....	328	
link status	31	
command	122	
duplex mode	31, 122	
port speed.....	31, 122	
Link Status Information	122	

linkt (SNMP option)	241
LISTENING (port state).....	65
LLDP	
configuration.....	328
statistics.....	165
local (IP route type).....	77
log	
syslog messages.....	227

M

MAC	
multicast.....	327
MAC (media access control) address	33, 45, 52, 79, 497
Maintenance commands	495
Management Processor (MP).....	499
display MAC address	33, 45
manual style conventions	16
martian	
IP route tag (filtered)	78
IP route type (filtered out).....	78
MaxAge (STP information).....	64, 67, 70
MD5 cryptographic authentication	380
MD5 key	384
media access control.....	52
meter	
ACLACL port metering.....	292
Miscellaneous Debug commands	499
monitor port.....	307
MP.....	499
mp	
packet.....	205, 207
MRouter information	102
multicast	
IP route type.....	78
multicast MAC.....	327
Multiple Spanning Tree	
configuration.....	316
mxage (STP bridge option).....	322

N

nbr change statistics.....	193, 198
Neighbor Discovery cache configuration	444
Neighbor Discovery prefix	445
Neighbor Discovery, IPv6	359
NETCONF (Network Configuration Protocol)	257
Network Configuration Protocol (NETCONF)	257
notice	223
NTP synchronization	238

O

OAM Discovery	
information.....	61
statistics	166
online help.....	25
Operations commands	475
operations-level BGP options	478
Operations-Level Port Options	476
operations-level VRRP options.....	477
ospf	
area index.....	380
authentication key.....	384
cost of the selected path.....	383
cost value of the host.....	388
dead, declaring a silent router to be down	383, 397
dead, health parameter of a hello packet	386, 399
export	389
fixed routes.....	403
hello, authentication parameter of a hello packet	386, 399
host entry configuration.....	388
host routes	378
interface	378
interface configuration	383
link state database.....	378, 390
Not-So-Stubby Area	380, 392
priority value of the switch interface	383
range number	378
route redistribution configuration.....	389
spf, shortest path first	381
stub area.....	380, 392
summary range configuration.....	382
transit area.....	380, 392
transit delay	383
type	380, 392
virtual link.....	378
virtual link configuration	386
virtual neighbor, router ID	386, 399
OSPF Database Information.....	86
OSPF General Information.....	85
OSPF Information.....	83
OSPF Information Route Codes.....	88
ospfv3	
configuration.....	390
P	
parameters	
tag	78
type	77

Password		re-markACL port re-mark menu	293
user access control	258	re-marking (IPv6 ACL)	299
password		Remote Monitoring (RMON)	457
administrator account	29	Rendezvous Point (RP)	438
default	29	retries	
user account	29	radius server	230
passwords	28	retry	
Path MTU	444	health checks for default gateway	361
PFC configuration	453	RIP	375
PIM mode	438	rip	
ping	25	IP route tag	78
poisoned reverse, as used with split horizon	375	RIP configuration	374
Port configuration	266	RIP Information	95
port configuration	266	RIP information	94
port ECN configuration	277	RMON	
Port Error Disable and Recovery	269	configuration	457
port mirroring		route statistics	181, 182
ACLs	287	router hops	406
configuration	307	Routing Information Protocol	374, 375
Port number	122	routing information protocol	
port speed	31, 122	configuration	375
port states		Routing Information Protocol (RIP)	78
UNK (unknown)	53	poisoned reverse	375
port trunking		split horizon	375
description	332	version 1 parameters	375
port trunking configuration	332	RSTP information	66
port WRED configuration	277	Rx/Tx statistics	192, 197
ports			
disabling (temporarily)	272	S	
information	123	save (global command)	222
membership of the VLAN	48, 73	secret	
priority	65, 70	radius server	229
VLAN ID	32, 123	Secure Shell	228
preemption		Service Required LED	225
assuming VRRP master routing authority	431	shortcuts (CLI)	27
Priority Flow Control	453	snap traces	
Priority Groups		buffer	499
ETS	452	SNMP configuration	239
prisrv		SNMP options	239
primary radius server	229, 236	SNMP statistics	215
Private VLAN	353	SNMPv3	242
Protocol-based VLANPVLAN	351	software	
ptcfg (TFTP save command)	473	image	486
PVID (port VLAN ID)	32, 123	image file and version	33, 45
		software upgrade	
R		recovery	491
Rapid Spanning Tree information	66	spanning tree	
read community string (SNMP option)	240	configuration	321
receive flow control	271	Spanning Tree Protocol	71
reference ports	53		

Spanning-Tree Protocol	
bridge parameters	322
bridge priority	64, 70
port cost option	324
root bridge	64, 70, 322
switch reset effect	489
split horizon	375
state (STP information)	65, 68, 71
static	
IP route tag	78
static multicast MAC	327
static route	
rem	363
static route, IPv6	443
static route	
add	363
statistics	
management processor	204
Statistics commands	143
subnets	
IP interface	357
switch	
name and location	33, 45
resetting	489
system	
contact (SNMP option)	239
date and time	33, 45
information	45
location (SNMP option)	239
System Error Disable and Recovery	225
System Information	33
system options	
hprompt	224
tport	255
wport	255

T

tab completion (CLI)	28
TACACS+	232
TCP statistics	186, 209
Telnet	
configuring switches using	472
telnet	
radius server	230, 237
text conventions	16
TFTP	486
PUT and GET commands	473
TFTP server	473
timeout	
radius server	230

timeouts	
idle connection	29
timers kickoff	195, 199
tport	
system option	255
trace buffer	499
traceroute	26
transceiver status	125
transmit flow control	271
trunk group information	71
trunk hash algorithm	334
type of area	
ospf	380, 392
type parameters	77
typographic conventions, manual	16

U

UCB statistics	210
UDLD	
configuration	272
information	59
UDP statistics	188
UniDirectional Link Detection	272
unknown (UNK) port state	53
Unscheduled System Dump	508
upgrade	
recover from failure	491
upgrade, switch software	486
USB Boot	485
USB Copy	474
USB drive	474, 485
user access control configuration	258
user account	29
Uencode Flash Dump	507

V

Virtual Link Aggregation Control Protocol (VLAG)	337
virtual router	
description	428
tracking criteria	431
virtual router group configuration	432
virtual router group priority tracking	434
Virtual Router Redundancy Protocol	427
Virtual Router Redundancy Protocol (VRRP)	
authentication parameters for IP interfaces	435
operations-level options	477
priority tracking options	405, 409, 431

virtual routers		WRED (Weighted Random Early Detection)	283
increasing priority level of	431		
priority increment values (vrs) for VRRP	436		
virtualization			
configuration	462		
information	125		
VLAG configuration	337		
VLAN			
active port	434		
configuration	349		
VLAN tagging			
port configuration	267		
port restrictions	350		
VLANs			
ARP entry information	79		
information	73		
name	48, 73		
port membership	48, 73		
setting default number (PVID)	266		
tagging	32, 123, 350		
VLAN Number	73		
VM			
bandwidth management	463		
group configuration	468		
information	126		
policy configuration	463		
profile configuration	470		
VMware configuration	471		
VMware information	127		
VMware operations	478		
VNIC			
configuration	464		
group configuration	466		
information	129		
VRRP			
interface configuration	435		
master advertisements	429		
tracking configuration	436		
VRRP configuration	427		
VRRP Information	102		
VRRP master advertisements			
time interval	433		
VRRP statistics	200		
W			
watchdog timer	495		
Weighted Random Early Detection (WRED)	283		
weights			
setting virtual router priority values	436		
wport	255		