

IBM System Networking RackSwitch G8264



# ISCLI—Industry Standard CLI Command Reference

for IBM Networking OS 7.8

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

**First Edition (December 2013)**

**IBM System Networking RackSwitch G8264 ISCLI Command Reference**

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

---

# Contents

<b>Preface</b> . . . . .	<b>xiii</b>
Who Should Use This Book . . . . .	xiii
How This Book Is Organized . . . . .	xiii
Typographic Conventions . . . . .	xiv
How to Get Help . . . . .	xvi
<b>Chapter 1. ISCLI Basics</b> . . . . .	<b>.1</b>
Accessing the ISCLI . . . . .	.2
ISCLI Command Modes . . . . .	.3
Global Commands . . . . .	.7
Command Line Interface Shortcuts . . . . .	.9
CLI List and Range Inputs . . . . .	.9
Command Abbreviation . . . . .	.9
Tab Completion . . . . .	.9
User Access Levels . . . . .	10
Idle Timeout . . . . .	11
<b>Chapter 2. Information Commands</b> . . . . .	<b>13</b>
System Information . . . . .	14
CLI Display Information . . . . .	15
Error Disable and Recovery Information . . . . .	16
SNMPv3 System Information . . . . .	17
SNMPv3 USM User Table Information . . . . .	18
SNMPv3 View Table Information . . . . .	19
SNMPv3 Access Table Information . . . . .	20
SNMPv3 Group Table Information . . . . .	21
SNMPv3 Community Table Information . . . . .	21
SNMPv3 Target Address Table Information . . . . .	22
SNMPv3 Target Parameters Table Information . . . . .	23
SNMPv3 Notify Table Information . . . . .	23
SNMPv3 Dump Information . . . . .	24
General System Information . . . . .	25
Show Specific System Information . . . . .	26
Show Recent Syslog Messages . . . . .	26
User Status . . . . .	27
Stacking Information . . . . .	28
Stacking Switch Information . . . . .	28
Layer 2 Information . . . . .	30
802.1X Information . . . . .	33
FDB Information . . . . .	35
FDB Multicast Information . . . . .	37
Show All FDB Information . . . . .	37
Clearing Entries from the Forwarding Database . . . . .	37
Link Aggregation Control Protocol Information . . . . .	38
Link Aggregation Control Protocol . . . . .	38
Layer 2 Failover Information . . . . .	39
Layer 2 Failover Information . . . . .	39
Hot Links Information . . . . .	41
LLDP Information . . . . .	41
LLDP Remote Device Information . . . . .	42

Unidirectional Link Detection Information . . . . .	43
UDLD Port Information . . . . .	43
802.1x Discovery Information . . . . .	44
802.1x Port Information. . . . .	44
OAM Discovery Information . . . . .	45
OAM Port Information . . . . .	45
vLAG Information . . . . .	46
vLAG Trunk Information . . . . .	46
Spanning Tree Information . . . . .	47
RSTP/PVRST Information . . . . .	49
Spanning Tree Bridge Information . . . . .	51
Spanning Tree Root Information . . . . .	51
Multiple Spanning Tree Information . . . . .	52
Trunk Group Information . . . . .	55
VLAN Information . . . . .	55
Layer 3 Information . . . . .	57
IP Routing Information. . . . .	60
Show All IP Route Information . . . . .	61
ARP Information . . . . .	62
ARP Address List Information . . . . .	63
Show All ARP Entry Information . . . . .	63
BGP Information . . . . .	64
BGP Peer information . . . . .	64
BGP Group information. . . . .	66
BGP Summary information . . . . .	67
Dump BGP Information. . . . .	67
OSPF Information . . . . .	68
OSPF General Information . . . . .	69
OSPF Interface Information . . . . .	70
OSPF Loopback Information. . . . .	70
OSPF Database Information. . . . .	70
OSPF Information Route Codes . . . . .	72
OSPFv3 Information . . . . .	73
OSPFv3 Information Dump . . . . .	74
OSPFv3 Interface Information . . . . .	75
OSPFv3 Database Information. . . . .	75
OSPFv3 Route Codes Information . . . . .	76
Routing Information Protocol . . . . .	77
RIP Routes Information. . . . .	77
RIP Interface Information . . . . .	77
IPv6 Routing Information. . . . .	78
IPv6 Routing Table Information . . . . .	78
IPv6 Neighbor Discovery Cache Information . . . . .	79
IPv6 Neighbor Discovery Cache Information . . . . .	79
IPv6 Neighbor Discovery Prefix Information . . . . .	80
ECMP Static Route Information . . . . .	80
IGMP Multicast Group Information . . . . .	81
IGMP Querier Information. . . . .	83
IGMP Group Information . . . . .	84
IGMP Multicast Router Information . . . . .	84
IPMC Group Information . . . . .	85
MLD information . . . . .	86
VRRP Information . . . . .	88

Interface Information . . . . .	89
IPv6 Interface Information . . . . .	90
IPv6 Path MTU Information . . . . .	91
IP Information . . . . .	92
IKEv2 Information . . . . .	93
IKEv2 Information Dump . . . . .	94
IP Security Information . . . . .	95
IPsec Manual Policy Information . . . . .	96
DHCP Snooping Binding Table Information . . . . .	97
PIM Information . . . . .	98
PIM Component Information . . . . .	99
PIM Interface Information . . . . .	100
PIM Neighbor Information . . . . .	100
PIM Multicast Route Information Commands . . . . .	101
PIM Multicast Route Information . . . . .	102
Quality of Service Information . . . . .	102
802.1p Information . . . . .	103
WRED and ECN Information . . . . .	104
Access Control List Information Commands . . . . .	104
Access Control List Information . . . . .	105
OpenFlow Information . . . . .	107
OpenFlow Global Configuration Information . . . . .	107
OpenFlow Flow Allocation Information . . . . .	108
OpenFlow Configuration Information . . . . .	110
OpenFlow Table Information . . . . .	112
RMON Information Commands . . . . .	114
RMON History Information . . . . .	116
RMON Alarm Information . . . . .	117
RMON Event Information . . . . .	118
Link Status Information . . . . .	119
Port Information . . . . .	119
Port Transceiver Status . . . . .	121
Virtual Machines Information . . . . .	122
VM Information . . . . .	122
VM Check Information . . . . .	123
VMware Information . . . . .	123
VMware Host Information . . . . .	123
vNIC Information . . . . .	125
Virtual NIC (vNIC) Information . . . . .	126
vNIC Group Information . . . . .	127
EVB Information . . . . .	128
Converged Enhanced Ethernet Information . . . . .	129
DCBX Information . . . . .	129
DCBX Control Information . . . . .	130
DCBX Feature Information . . . . .	131
DCBX ETS Information . . . . .	132
DCBX PFC Information . . . . .	133
DCBX Application Protocol Information . . . . .	134
ETS Information . . . . .	136
PFC Information . . . . .	137
FCoE Information . . . . .	138
FIP Snooping Information . . . . .	138
Fibre Channel over Ethernet Forwarder Information . . . . .	140

Information Dump . . . . .	141
Python Scripting Information . . . . .	142
Scheduler Job Information . . . . .	143
<b>Chapter 3. Statistics Commands . . . . .</b>	<b>145</b>
Port Statistics . . . . .	146
802.1X Authenticator Statistics . . . . .	149
802.1X Authenticator Diagnostics . . . . .	150
BootStrap Protocol Relay Statistics . . . . .	152
Bridging Statistics . . . . .	153
Ethernet Statistics . . . . .	154
Interface Statistics . . . . .	157
Interface Protocol Statistics . . . . .	160
Link Statistics . . . . .	160
RMON Statistics . . . . .	161
QoS Queue Counter-Based Statistics . . . . .	164
QoS Queue Rate-Based Statistics . . . . .	165
Trunk Group Statistics . . . . .	166
Layer 2 Statistics . . . . .	167
FDB Statistics . . . . .	168
LACP Statistics . . . . .	168
Hotlinks Statistics . . . . .	169
LLDP Port Statistics . . . . .	170
OAM Statistics . . . . .	171
vLAG Statistics . . . . .	171
vLAG ISL Statistics . . . . .	172
vLAG Statistics . . . . .	172
Layer 3 Statistics . . . . .	174
IPv4 Statistics . . . . .	178
IPv6 Statistics . . . . .	180
IPv4 Route Statistics . . . . .	184
IPv6 Route Statistics . . . . .	185
ARP statistics . . . . .	186
DNS Statistics . . . . .	186
ICMP Statistics . . . . .	187
TCP Statistics . . . . .	189
UDP Statistics . . . . .	190
IGMP Statistics . . . . .	191
MLD Statistics . . . . .	193
OSPF Statistics . . . . .	196
OSPF Global Statistics . . . . .	197
OSPFv3 Statistics . . . . .	200
OSPFv3 Global Statistics . . . . .	201
VRRP Statistics . . . . .	205
PIM Statistics . . . . .	206
Routing Information Protocol Statistics . . . . .	207
DHCP Statistics . . . . .	207
DHCP Snooping Statistics . . . . .	207
OpenFlow Statistics . . . . .	208
Management Processor Statistics . . . . .	221
MP Packet Statistics . . . . .	221
MP Packet Statistics . . . . .	223
Logged Packet Statistics . . . . .	226

TCP Statistics . . . . .	230
UDP Statistics . . . . .	231
CPU Statistics . . . . .	231
CPU Statistics History . . . . .	233
QoS Statistics . . . . .	234
Access Control List Statistics . . . . .	235
ACL Statistics . . . . .	236
VMAP Statistics . . . . .	236
Fiber Channel over Ethernet Statistics . . . . .	237
SNMP Statistics . . . . .	238
NTP Statistics . . . . .	242
PTP Statistics . . . . .	244
Statistics Dump . . . . .	245
<b>Chapter 4. Configuration Commands . . . . .</b>	<b>247</b>
Viewing and Saving Changes . . . . .	249
System Configuration . . . . .	250
System Error Disable and Recovery Configuration . . . . .	253
Link Flap Dampening Configuration . . . . .	254
System Host Log Configuration . . . . .	255
SSH Server Configuration . . . . .	257
RADIUS Server Configuration . . . . .	258
TACACS+ Server Configuration . . . . .	260
LDAP Server Configuration . . . . .	264
NTP Server Configuration . . . . .	266
System SNMP Configuration . . . . .	268
SNMPv3 Configuration . . . . .	270
User Security Model Configuration . . . . .	272
SNMPv3 View Configuration . . . . .	273
View-based Access Control Model Configuration . . . . .	274
SNMPv3 Group Configuration . . . . .	275
SNMPv3 Community Table Configuration . . . . .	276
SNMPv3 Target Address Table Configuration . . . . .	277
SNMPv3 Target Parameters Table Configuration . . . . .	278
SNMPv3 Notify Table Configuration . . . . .	279
System Access Configuration . . . . .	280
Management Network Configuration . . . . .	282
NETCONF Configuration . . . . .	283
NETCONF over SSH Configuration . . . . .	283
User Access Control Configuration . . . . .	284
System User ID Configuration . . . . .	285
Strong Password Configuration . . . . .	286
HTTPS Access Configuration . . . . .	287
Custom Daylight Saving Time Configuration . . . . .	289
sFlow Configuration . . . . .	290
sFlow Port Configuration . . . . .	290
Server Port Configuration . . . . .	291
Port Configuration . . . . .	292
Port Error Disable and Recovery Configuration . . . . .	296
Port Link Flap Dampening Configuration . . . . .	296
Port Link Configuration . . . . .	297
Temporarily Disabling a Port . . . . .	298
UniDirectional Link Detection Configuration . . . . .	298

Port OAM Configuration . . . . .	299
Port ACL Configuration . . . . .	300
Port WRED Configuration . . . . .	301
Port WRED Transmit Queue Configuration . . . . .	301
Stacking Configuration . . . . .	303
Stacking Switch Configuration. . . . .	303
Quality of Service Configuration . . . . .	305
802.1p Configuration . . . . .	305
DSCP Configuration . . . . .	306
Control Plane Protection . . . . .	307
Weighted Random Early Detection Configuration . . . . .	309
WRED Transmit Queue Configuration . . . . .	310
Access Control Configuration . . . . .	311
Access Control List Configuration . . . . .	312
ACL Mirroring Configuration . . . . .	313
Ethernet Filtering Configuration . . . . .	313
IPv4 Filtering Configuration . . . . .	314
TCP/UDP Filtering Configuration . . . . .	315
Packet Format Filtering Configuration . . . . .	316
ACL Metering Configuration . . . . .	317
ACL Re-Mark Configuration . . . . .	318
ACL IPv6 Configuration . . . . .	319
IP version 6 Filtering Configuration . . . . .	320
IPv6 TCP/UDP Filtering Configuration . . . . .	321
IPv6 Re-Mark Configuration . . . . .	322
IPv6 Metering Configuration . . . . .	323
ACL Log Configuration . . . . .	324
ACL Group Configuration . . . . .	324
Management ACL Configuration. . . . .	325
MACL IPv4 Filtering Configuration . . . . .	326
MACL TCP/UDP Filtering Configuration . . . . .	327
VMAP Configuration . . . . .	328
Port Mirroring . . . . .	332
Port-Mirroring Configuration . . . . .	332
Layer 2 Configuration. . . . .	333
802.1X Configuration . . . . .	333
802.1X Global Configuration. . . . .	334
802.1X Guest VLAN Configuration . . . . .	335
802.1X Port Configuration. . . . .	336
Spanning Tree Configuration . . . . .	338
MSTP Configuration . . . . .	340
RSTP/PVRST Configuration. . . . .	343
Forwarding Database Configuration . . . . .	346
Static Multicast MAC Configuration. . . . .	347
Static FDB Configuration. . . . .	348
ECP Configuration . . . . .	348
LLDP Configuration . . . . .	349
LLDP Port Configuration . . . . .	350
LLDP Optional TLV configuration . . . . .	351
Trunk Configuration. . . . .	353
Trunk Hash Configuration . . . . .	354
Layer 2 Trunk Hash . . . . .	354
Layer 3 Trunk Hash . . . . .	355



Virtual Link Aggregation Control Protocol Configuration . . . . .	356
vLAG Health Check Configuration . . . . .	357
vLAG ISL Configuration . . . . .	358
Link Aggregation Control Protocol Configuration . . . . .	358
LACP Port Configuration . . . . .	359
Layer 2 Failover Configuration . . . . .	360
Failover Trigger Configuration . . . . .	361
Failover Manual Monitor Port Configuration . . . . .	361
Failover Manual Monitor Control Configuration . . . . .	362
Hot Links Configuration . . . . .	363
Hot Links Trigger Configuration . . . . .	364
Hot Links Master Configuration . . . . .	365
Hot Links Backup Configuration . . . . .	365
VLAN Configuration . . . . .	366
Protocol-Based VLAN Configuration . . . . .	368
Private VLAN Configuration . . . . .	370
Layer 3 Configuration . . . . .	371
IP Interface Configuration . . . . .	373
IPv6 Neighbor Discovery Configuration . . . . .	375
Default Gateway Configuration . . . . .	377
IPv4 Static Route Configuration . . . . .	378
IP Multicast Route Configuration . . . . .	380
ARP Configuration . . . . .	381
ARP Static Configuration . . . . .	382
ARP Local Proxy Configuration . . . . .	382
IP Forwarding Configuration . . . . .	383
Network Filter Configuration . . . . .	384
Routing Map Configuration . . . . .	385
IP Access List Configuration . . . . .	387
Policy-Based Routing Configuration . . . . .	388
Autonomous System Filter Path Configuration . . . . .	389
Routing Information Protocol Configuration . . . . .	390
Routing Information Protocol Interface Configuration . . . . .	391
RIP Route Redistribution Configuration . . . . .	393
Open Shortest Path First Configuration . . . . .	394
Area Index Configuration . . . . .	396
OSPF Summary Range Configuration . . . . .	398
OSPF Interface Configuration . . . . .	399
OSPF Virtual Link Configuration . . . . .	401
OSPF Host Entry Configuration . . . . .	403
OSPF Route Redistribution Configuration . . . . .	404
OSPF MD5 Key Configuration . . . . .	404
Open Shortest Path First Version 3 Configuration . . . . .	405
OSPFv3 Area Index Configuration . . . . .	407
OSPFv3 Summary Range Configuration . . . . .	409
OSPFv3 AS-External Range Configuration . . . . .	410
OSPFv3 Interface Configuration . . . . .	411
OSPFv3 Virtual Link Configuration . . . . .	415
OSPFv3 Host Entry Configuration . . . . .	416
OSPFv3 Redistribute Entry Configuration . . . . .	417
OSPFv3 Redistribute Configuration . . . . .	418

Border Gateway Protocol Configuration . . . . .	419
BGP Peer Configuration . . . . .	421
BGP Peering Group Configuration . . . . .	424
BGP Aggregation Configuration . . . . .	428
IGMP Configuration . . . . .	431
IGMP Snooping Configuration . . . . .	432
IGMPv3 Configuration . . . . .	433
IGMP Relay Configuration . . . . .	434
IGMP Relay Multicast Router Configuration . . . . .	435
IGMP Static Multicast Router Configuration . . . . .	436
IGMP Filtering Configuration . . . . .	437
IGMP Advanced Configuration . . . . .	439
IGMP Querier Configuration . . . . .	440
IKEv2 Configuration . . . . .	441
IKEv2 Proposal Configuration . . . . .	442
IKEv2 Preshare Key Configuration . . . . .	442
IKEv2 Identification Configuration . . . . .	443
IPsec Configuration . . . . .	443
IPsec Transform Set Configuration . . . . .	444
IPsec Traffic Selector Configuration . . . . .	445
IPsec Dynamic Policy Configuration . . . . .	446
IPsec Manual Policy Configuration . . . . .	447
Domain Name System Configuration . . . . .	449
Bootstrap Protocol Relay Configuration . . . . .	450
BOOTP Relay Broadcast Domain Configuration . . . . .	451
Option 82 Configuration . . . . .	452
VRRP Configuration . . . . .	453
Virtual Router Configuration . . . . .	454
Virtual Router Priority Tracking Configuration . . . . .	456
Virtual Router Group Configuration . . . . .	457
Virtual Router Group Priority Tracking Configuration . . . . .	459
VRRP Interface Configuration . . . . .	460
VRRP Tracking Configuration . . . . .	461
Protocol Independent Multicast Configuration . . . . .	462
PIM Component Configuration . . . . .	462
PIM Interface Configuration . . . . .	464
IPv6 Default Gateway Configuration . . . . .	466
IPv6 Static Route Configuration . . . . .	467
IPv6 Neighbor Discovery Cache Configuration . . . . .	467
IPv6 Path MTU Configuration . . . . .	468
IPv6 Neighbor Discovery Prefix Configuration . . . . .	469
IPv6 Prefix Policy Table Configuration . . . . .	470
IP Loopback Interface Configuration . . . . .	471
Flooding VLAN Configuration Menu . . . . .	472
DHCP Snooping . . . . .	473
Converged Enhanced Ethernet Configuration . . . . .	474
ETS Global Configuration . . . . .	475
ETS Global Priority Group Configuration . . . . .	475
Priority Flow Control Configuration . . . . .	476
802.1p PFC Configuration . . . . .	476
DCBX Port Configuration . . . . .	477
Fibre Channel over Ethernet Configuration . . . . .	478
FIPS Port Configuration . . . . .	479

Remote Monitoring Configuration . . . . .	.480
RMON History Configuration . . . . .	.480
RMON Event Configuration . . . . .	.481
RMON Alarm Configuration . . . . .	.482
Virtualization Configuration . . . . .	.484
VM Policy Bandwidth Management . . . . .	.485
Virtual NIC Configuration . . . . .	.486
vNIC Port Configuration . . . . .	.486
Virtual NIC Group Configuration . . . . .	.487
VM Group Configuration . . . . .	.489
VM Check Configuration . . . . .	.492
VM Profile Configuration . . . . .	.493
VMWare Configuration . . . . .	.494
Miscellaneous VMready Configuration . . . . .	.495
Edge Virtual Bridge VSI Type Database Configuration . . . . .	.496
Edge Virtual Bridge VSI Type Profile Configuration . . . . .	.497
OpenFlow Configuration . . . . .	.499
Static Flows Configuration . . . . .	.507
Precision Time Protocol Configuration . . . . .	.511
Microburst Detection . . . . .	.513
Configuration Dump . . . . .	.514
Saving the Active Switch Configuration . . . . .	.515
Restoring the Active Switch Configuration . . . . .	.516
USB Copy . . . . .	.517
Copy to USB . . . . .	.517
Copy from USB . . . . .	.517
Python Scripting Configuration . . . . .	.518
Python Scripts Management and Execution . . . . .	.518
Scheduler Jobs Management . . . . .	.520
Running Job Monitor . . . . .	.523
<b>Chapter 5. Operations Commands . . . . .</b>	<b>.525</b>
Operations-Level Port Commands . . . . .	.526
Operations-Level FCoE Commands . . . . .	.527
Operations-Level VRRP Commands . . . . .	.528
Operations-Level BGP Commands . . . . .	.529
VMware Operations . . . . .	.530
VMware Distributed Virtual Switch Operations . . . . .	.532
VMware Distributed Port Group Operations . . . . .	.533
<b>Chapter 6. Boot Options . . . . .</b>	<b>.535</b>
Stacking Boot Options . . . . .	.535
Scheduled Reboot of the Switch . . . . .	.538
Netboot Configuration . . . . .	.539
Forwarding Mode Configuration . . . . .	.540
Machine Type Model Configuration . . . . .	.540
QSFP Port Configuration . . . . .	.541
USB Boot Configuration . . . . .	.542
Updating the Switch Software Image . . . . .	.543
Loading New Software to Your Switch . . . . .	.543
Selecting a Software Image to Run . . . . .	.544
Uploading a Software Image from Your Switch . . . . .	.544
Selecting a Configuration Block . . . . .	.546

Setting an Entitlement Serial Number . . . . .	547
Resetting the Switch . . . . .	548
Accessing the IBM N/OS CLI. . . . .	549
Changing the Switch Profile . . . . .	550
Using the Boot Management Menu . . . . .	551
Recovering from a Failed Upgrade . . . . .	551
<b>Chapter 7. Maintenance Commands . . . . .</b>	<b>555</b>
Forwarding Database Maintenance . . . . .	557
Debugging Commands . . . . .	558
IPsec Debugging . . . . .	560
BGP Debugging. . . . .	561
DCBX Maintenance . . . . .	562
LLDP Cache Manipulation . . . . .	563
ARP Cache Maintenance . . . . .	564
BGP Maintenance . . . . .	565
IP Route Manipulation . . . . .	566
IGMP Snooping Maintenance . . . . .	567
IGMP Multicast Routers Maintenance . . . . .	568
MLD Multicast Group Maintenance . . . . .	569
LACP Maintenance . . . . .	570
IPv6 Neighbor Discovery Cache Manipulation . . . . .	571
IPv6 Route Maintenance . . . . .	572
Uuencode Flash Dump . . . . .	573
TFTP, SFTP or FTP System Dump Put. . . . .	574
Clearing Dump Information . . . . .	575
Unscheduled System Dumps. . . . .	576
<b>Appendix A. IBM N/OS System Log Messages. . . . .</b>	<b>577</b>
LOG_ALERT . . . . .	578
LOG_CRIT. . . . .	582
LOG_ERR . . . . .	583
LOG_INFO. . . . .	586
LOG_NOTICE . . . . .	590
LOG_WARNING . . . . .	599
<b>Appendix B. Getting help and technical assistance. . . . .</b>	<b>603</b>
Before you call . . . . .	604
Using the documentation . . . . .	605
Getting help and information on the World Wide Web . . . . .	606
Software service and support . . . . .	607
Hardware service and support . . . . .	608
IBM Taiwan product service . . . . .	609
<b>Index . . . . .</b>	<b>611</b>

---

## Preface

The *IBM System Networking RackSwitch G8264 ISCLI Command Reference* describes how to configure and use the IBM N/OS 7.8 software with your RackSwitch G8264 (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 RackSwitch G8264. For details about configuration and operation of your G8264, see the *IBM N/OS 7.8 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, Spanning Tree Protocol and SNMP configuration parameters.

---

## How This Book Is Organized

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

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

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

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

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

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

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

**Appendix A, “IBM N/OS System Log Messages,”** shows a listing of syslog messages.

**Appendix B, “Getting help and technical assistance,”** lists the resources available from IBM to assist you.

**“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	This type is used for names of commands, files, and directories used within the text. For example:  View the <code>readme.txt</code> file.  It also depicts on-screen computer output and prompts.
bold fixed-width text	This bold type appears in command examples. It shows text that must be typed in exactly as shown. For example:  <code>show sys-info</code>
<b>bold body text</b>	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.
<i>italicized body text</i>	This italicized type indicates book titles, special terms, or words to be emphasized.
angle brackets < >	Indicate a variable to enter based on the description inside the brackets. Do not type the brackets when entering the command.  Example: If the command syntax is <code>ping &lt;IP address&gt;</code>  you enter <code>ping 192.32.10.12</code>
braces { }	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.  Example: If the command syntax is <code>show portchannel {&lt;1-64&gt; hash information}</code>  you enter: <b>show</b> portchannel <1-64>  or  <code>show portchannel hash</code>  or  <code>show portchannel information</code>

Table 1. Typographic Conventions (continued)

Typeface or Symbol	Meaning
brackets [ ]	<p>Indicate optional elements in syntax descriptions. Do not type the brackets when entering the command.</p> <p>Example: If the command syntax is  <code>show interface ip [&lt;1-126&gt;]</code></p> <p>you enter  <code>show interface ip</code></p> <p>or  <code>show interface ip &lt;1-126&gt;</code></p>
vertical line	<p>Separates choices for command keywords and arguments. Enter only one of the choices. Do not type the vertical line when entering the command.</p> <p>Example: If the command syntax is  <code>show portchannel {&lt;1-64&gt; hash information}</code></p> <p>you must enter:  <code><b>show</b> portchannel &lt;1-64&gt;</code></p> <p>or  <code>show portchannel hash</code></p> <p>or  <code>show portchannel information</code></p>

---

## How to Get Help

If you need help, service, or technical assistance, call IBM 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.ibm.com>

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 IBM N/OS CLI. To access the ISCLI, enter the following command and reset the G8264:

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

To access the IBM N/OS CLI, enter the following command from the ISCLI and reload the G8264:

```
Router(config)# boot cli-mode ibmos-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 IBM N/OS CLI. However, the switch retains the CLI boot mode, and will restore your CLI choice.

## ISCLI Command Modes

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

- **User EXEC mode**

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

- **Privileged EXEC mode**

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

- **Global Configuration mode**

This mode allows you to make changes to the running configuration. If you save the configuration, the settings survive a reload of the 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 G8264>	Default mode, entered automatically on console  Exit: <code>exit</code> or <code>logout</code>
Privileged EXEC G8264#	Enter Privileged EXEC mode, from User EXEC mode: <code>enable</code>  Exit to User EXEC mode: <code>disable</code>  Quit ISCLI: <code>exit</code> or <code>logout</code>
Global Configuration G8264 (config)#	Enter Global Configuration mode, from Privileged EXEC mode: <code>configure terminal</code>  Exit to Privileged EXEC: <code>end</code> or <code>exit</code>
Interface IP G8264 (config-ip-if)#	Enter Interface IP Configuration mode, from Global Configuration mode: <code>interface ip &lt;interface number&gt;</code>  Exit to Global Configuration mode: <code>exit</code>  Exit to Privileged EXEC mode: <code>end</code>
Interface loopback G8264 (config-ip-loopback)#	Enter Interface Loopback Configuration mode, from Global Configuration mode: <code>interface loopback &lt;1-5&gt;</code>  Exit to Global Configuration mode: <code>exit</code>  Exit to Privileged EXEC mode: <code>end</code>

Table 2. ISCLI Command Modes (continued)

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
Interface PortChannel Router (config-PortChannel) #	Enter PortChannel (trunk group) Configuration mode, from Global Configuration mode: interface portchannel {<trunk number>   lacp <key>}  Exit to Privileged EXEC mode: exit  Exit to Global Configuration mode: end
VLAN 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 BGP G8264 (config-router-bgp) #	Enter BGP Configuration mode, from Global Configuration mode: router bgp  Exit to Global Configuration mode: exit  Exit to Privileged EXEC mode: end
Router RIP 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

Table 2. ISCLI Command Modes (continued)

Command Mode/Prompt	Command used to enter or exit
Route Map G8264 (config-route-map) #	Enter Route Map Configuration mode, from Global Configuration mode: route-map <1-64>  Exit to Global Configuration mode: exit  Exit to Privileged EXEC mode: end
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
IKEv2 Proposal Router (config-ikev2-prop) #	Enter IKEv2 Proposal Configuration mode, from Global Configuration mode: ikev2 proposal  Exit to Global Configuration mode: exit  Exit to Privileged EXEC mode: end
MLD Configuration Router (config-router-mlD) #	Enter Multicast Listener Discovery Protocol Configuration mode, from Global Configuration mode: ipv6 mld  Exit to Global Configuration mode: exit  Exit to Privileged EXEC mode: end
MST Configuration G8264 (config-mst) #	Enter Multiple Spanning Tree Protocol Configuration mode, from Global Configuration mode: spanning-tree mst configuration  Exit to Global Configuration mode: exit  Exit to Privileged EXEC mode: end
OpenFlow Instance G8264 (config-openflow-instance) #	Enter OpenFlow Instance Configuration mode, from Global Configuration mode: openflow instance  Exit to Global Configuration mode: exit  Exit to Privileged EXEC mode: end

Table 2. ISCLI Command Modes (continued)

Command Mode/Prompt	Command used to enter or exit
VSI Database G8264 (conf-vsldb)#	Enter Virtual Station Interface Database Configuration mode, from Global Configuration mode: virt evb vsldb <VSIDB_number>  Exit to Global Configuration mode: exit  Exit to Privileged EXEC mode: end
EVB Profile G8264 (conf-evbprof)#	Enter Edge Virtual Bridging VSI Type Profile Configuration mode, from Global Configuration mode: virt evb profile <1-16>  Exit to Global Configuration mode: exit  Exit to Privileged EXEC mode: end
Scheduler Job G8264 (config-job)#	Enter Python Scripting Scheduler Job Configuration mode, from Global Configuration mode: scheduler job name <job name>  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
?	Provides more information about a specific command or lists commands available at the current level.
list	Lists the commands available at the current level.
exit	Go up one level in the command mode structure. If already at the top level, exit from the command line interface and log out.
copy running-config startup-config	Write configuration changes to non-volatile flash memory.
logout	Exit from the command line interface and log out.
ping	<p>Use this command to verify station-to-station connectivity across the network. The format is as follows:</p> <pre>ping &lt;host name&gt;   &lt;IP address&gt; [-n &lt;tries (0-4294967295)&gt;] [-w &lt;msec delay (0-4294967295)&gt;] [-l &lt;length (0/32-65500/2080)&gt;] [-s &lt;IP source&gt;] [-v &lt;tos (0-255)&gt;] [-f] [-t] [-m   -mgt   -d   -data]</pre> <p>Where:</p> <ul style="list-style-type: none"> <li>- -n: Sets the number of attempts (optional).</li> <li>- -w: Sets the number of milliseconds between attempts (optional).</li> <li>- -l: Sets the ping request payload size (optional).</li> <li>- -s: Sets the IP source address for the IP packet (optional).</li> <li>- -v: Sets the Type Of Service bits in the IP header.</li> <li>- -f: Sets the <i>don't fragment</i> bit in the IP header (only for IPv4 addresses).</li> <li>- -t: Pings continuously (same as -n 0).</li> </ul> <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>traceroute &lt;hostname&gt;   &lt;IP address&gt; [&lt;max-hops (1-32)&gt; [&lt;msec-delay (1-4294967295)&gt;]] [-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 <i>-m</i> or <i>-mgt</i> option for management port is used. To use data ports, specify the <i>-d</i> or <i>-data</i> option.</p> <p>As with <i>ping</i>, the DNS parameters must be configured if specifying hostnames.</p>
telnet	<p>This command is used to form a Telnet session between the switch and another network device. The format is as follows:</p> <pre>telnet {&lt;hostname&gt;   &lt;IP address&gt;} [&lt;port&gt;] [-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 <i>-m</i> or <i>-mgt</i> option for management port is used. To use data ports, specify the <i>-d</i> or <i>-data</i> option.</p>
show history	This command displays the last ten issued commands.
show who	Displays a list of users who are currently logged in.
show line	Displays a list of users who are currently logged in, in table format.



---

## Command Line Interface Shortcuts

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

### CLI List and Range Inputs

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

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

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

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

Do not use spaces within list and range specifications.

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

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

### Command Abbreviation

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

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

### Tab Completion

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

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, or disabled when set to 0:

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

**Command mode:** Global Configuration



## Chapter 2. Information Commands

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

Table 5. Information Commands

Command Syntax and Usage
<pre>show interface status &lt;port alias or number&gt;</pre> <p>Displays configuration information about the selected port(s), including:</p> <ul style="list-style-type: none"><li>– Port alias and number</li><li>– Port speed</li><li>– Duplex mode (half, full, or auto)</li><li>– Flow control for transmit and receive (no, yes, or both)</li><li>– Link status (up, down, or disabled)</li></ul> <p><b>Command mode:</b> All</p> <p>For details, see <a href="#">page 119</a>.</p>
<pre>show interface trunk &lt;port alias or number&gt;</pre> <p>Displays port status information, including:</p> <ul style="list-style-type: none"><li>– Port alias and number</li><li>– Whether the port uses VLAN Tagging or not</li><li>– Port VLAN ID (PVID)</li><li>– Port name</li><li>– VLAN membership</li><li>– FDB Learning status</li><li>– Flooding status</li></ul> <p>For details, see <a href="#">page 119</a>.</p> <p><b>Command mode:</b> All</p>
<pre>show interface transceiver</pre> <p>Displays the status of the port transceiver module on each port. For details, see <a href="#">page 121</a>.</p> <p><b>Command mode:</b> All</p>
<pre>show information-dump</pre> <p>Dumps all switch information available (10K or more, depending on your configuration).</p> <p>If you want to capture dump data to a file, set your communication software on your workstation to capture session data prior to issuing the dump commands.</p> <p><b>Command mode:</b> All</p>

---

## System Information

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

Table 6. System Information Options

Command Syntax and Usage
<pre>show sys-info</pre> <p>Displays system information, including:</p> <ul style="list-style-type: none"><li>– System date and time</li><li>– Switch model name and number</li><li>– Switch name and location</li><li>– Time of last boot</li><li>– MAC address of the switch management processor</li><li>– IP address of management interface</li><li>– Hardware version and part number</li><li>– Software image file and version number</li><li>– Configuration name</li><li>– Log-in banner, if one is configured</li><li>– Internal temperatures</li><li>– Fan status</li><li>– Power supply status</li></ul> <p>For details, see <a href="#">page 25</a>.</p> <p><b>Command mode:</b> All</p>
<pre>show logging [severity &lt;0-7&gt;] [reverse]</pre> <p>Displays the current syslog configuration, followed by the most recent 2000 syslog messages, as displayed by the <code>show logging messages</code> command. For details, see <a href="#">page 26</a>.</p> <p><b>Command mode:</b> All</p>
<pre>show access user</pre> <p>Displays configured user names and their status.</p> <p><b>Command mode:</b> All</p>

## CLI Display Information

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

Table 7. CLI Display Information Options

Command Syntax and Usage
<pre>show terminal-length</pre> <p>Displays the number of lines per screen displayed in the CLI for the current session. A value of 0 means paging is disabled.</p> <p><b>Command mode:</b> All</p>
<pre>show line console length</pre> <p>Displays the number of lines per screen displayed in the CLI by default for console sessions. A value of 0 means paging is disabled.</p> <p><b>Command mode:</b> All</p>
<pre>show line vty length</pre> <p>Displays the number of lines per screen displayed in the CLI by default for Telnet and SSH sessions. A value of 0 means paging is disabled.</p> <p><b>Command mode:</b> All</p>

## Error Disable and Recovery Information

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

Table 8. Error Disable Information Options

Command Syntax and Usage
<pre>show errdisable recovery</pre> <p>Displays a list ports with their Error Recovery status.</p> <p><b>Command mode:</b> All</p>
<pre>show errdisable timers</pre> <p>Displays a list of active recovery timers, if applicable.</p> <p><b>Command mode:</b> All</p>
<pre>show errdisable information</pre> <p>Displays all Error Disable and Recovery information.</p> <p><b>Command mode:</b> All</p>
<pre>show errdisable link-flap information</pre> <p>Displays ports that have been disabled due to excessive link flaps.</p> <p><b>Command mode:</b> All</p>



## SNMPv3 System Information

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

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

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

Table 9. SNMPv3 Information Options

Command Syntax and Usage
<pre>show snmp-server v3 user</pre> <p>Displays User Security Model (USM) table information. To view the table, see <a href="#">page 18</a>.</p> <p><b>Command mode:</b> All</p>
<pre>show snmp-server v3 view</pre> <p>Displays information about view, subtrees, mask and type of view. To view a sample, see <a href="#">page 19</a>.</p> <p><b>Command mode:</b> All</p>
<pre>show snmp-server v3 access</pre> <p>Displays View-based Access Control information. To view a sample, see <a href="#">page 20</a>.</p> <p><b>Command mode:</b> All</p>
<pre>show snmp-server v3 group</pre> <p>Displays information about the group, including the security model, user name, and group name. To view a sample, see <a href="#">page 21</a>.</p> <p><b>Command mode:</b> All</p>
<pre>show snmp-server v3 community</pre> <p>Displays information about the community table information. To view a sample, see <a href="#">page 21</a>.</p> <p><b>Command mode:</b> All</p>
<pre>show snmp-server v3 target-address</pre> <p>Displays the Target Address table information. To view a sample, see <a href="#">page 22</a>.</p> <p><b>Command mode:</b> All</p>
<pre>show snmp-server v3 target-parameters</pre> <p>Displays the Target parameters table information. To view a sample, see <a href="#">page 23</a>.</p> <p><b>Command mode:</b> All</p>

Table 9. SNMPv3 Information Options (continued)

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

## SNMPv3 USM User Table Information

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

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

**Command mode:** All

The USM user table contains the following information:

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

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

Table 10. USM User Table Information Parameters

Field	Description
User Name	A string representing the user name you can use to access the switch.
Protocol	Whether messages sent from this user are protected from disclosure using a privacy protocol. IBM N/OS supports DES algorithm for privacy and 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 11. SNMPv3 View Table Information Parameters

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

## SNMPv3 Access Table Information

The access control subsystem provides authorization services.

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

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

The following command displays SNMPv3 access information:

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

**Command mode:** All

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

Table 12. 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 13. 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

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

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

**Command mode:** All

Index	Name	User Name	Tag
trap1	public	v1v2only	v1v2trap

Table 14. SNMPv3 Community Table Information Parameters

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

## SNMPv3 Target Address Table Information

The following command displays SNMPv3 target address information stored in the SNMP engine:

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

**Command mode:** All

Name	Transport Addr	Port	Taglist	Params
trap1	47.81.25.66	162	v1v2trap	v1v2param

Table 15. 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 16. 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 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 17. 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

IBM Networking Operating System 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 image1), 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
- Internal temperatures
- Fan status
- Power supply status

## Show Specific System Information

[Table 18](#) lists commands used for displaying specific entries from the general system information screen

*Table 18. Specific System Information Options*

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

## Show Recent Syslog Messages

The following command displays system log messages:

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

## Command mode: All

```
Nov 2 5:49:53 172.25.254.19 INFO console: System log cleared by user admin.
Nov 2 5:51:23 172.25.254.19 CRIT system: Fan Mod 4 Removed
Nov 2 5:54:27 172.25.254.19 CRIT system: **** MAX TEMPERATURE (61) ABOVE FAIL
THRESH ****
Nov 2 5:54:27 172.25.254.19 CRIT system: **** PLATFORM THERMAL SHUTDOWN ****
Nov 2 6:02:06 0.0.0.0 NOTICE system: link up on management port MGT
Nov 2 6:02:06 0.0.0.0 INFO system: booted version 0.0.0 from FLASH image2,
active configuration
Nov 2 6:02:09 0.0.0.0 NOTICE system: SR SFP+ inserted at port 63 is Approved
Nov 2 6:02:12 0.0.0.0 NOTICE system: 1m DAC inserted at port 64 is Accepted
Nov 2 6:02:12 0.0.0.0 NOTICE system: link up on management port MGT
Nov 2 6:03:11 172.25.254.19 NOTICE system: Received DHCP Offer
IP: 172.25.254.19 Mask: 255.255.0.
Broadcast 172.25.255.255 GW: 172.25.1.1
Nov 2 6:03:11 0.0.0.0 NOTICE ip: MGT port default gateway 172.25.1.1 operational
Nov 2 6:22:54 172.25.254.19 NOTICE mgmt: admin(admin) login on Console
Nov 2 6:33:00 172.25.254.19 NOTICE mgmt: admin(admin) idle timeout from Console
```

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

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

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

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

## User Status

The following command displays user status information:

```
show access user
```

**Command mode:** All except User EXEC

```
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.

---

## Stacking Information

Table 19 lists the Stacking information options.

Table 19. Stacking Information Options

Command Syntax and Usage
<pre>show stack switch</pre> <p>Displays information about each switch in the stack, including:</p> <ul style="list-style-type: none"><li>– Configured Switch Number (csnum)</li><li>– Attached Switch Number (asnum)</li><li>– MAC address</li><li>– Stacking state</li></ul> <p><b>Command mode:</b> All</p>
<pre>show stack link</pre> <p>Displays link information for each switch in the stack, listed by assigned switch number.</p> <p><b>Command mode:</b> All</p>
<pre>show stack name</pre> <p>Displays the name of the stack.</p> <p><b>Command mode:</b> All</p>
<pre>show stack backup</pre> <p>Displays the unit number of the backup switch.</p> <p><b>Command mode:</b> All</p>
<pre>show stack version</pre> <p>Displays the firmware version number for the selected switch.</p> <p><b>Command mode:</b> All</p>
<pre>show stack path-map</pre> <p>Displays the Stacking packet path map that shows how the stack switches are connected.</p> <p><b>Command mode:</b> All</p>
<pre>show stack push-status</pre> <p>Displays the status of the most recent firmware and configuration file push from the master to member switches.</p> <p><b>Command mode:</b> All</p>
<pre>show stack dynamic</pre> <p>Displays all stacking information.</p> <p><b>Command mode:</b> All</p>

## Stacking Switch Information

The following command displays Stacking switch information:

```
show stack switch
```

**Command mode:** All

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

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

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

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

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

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

Stack switch information includes the following:

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

---

## Layer 2 Information

Table 20. Layer 2 Information Commands

Command Syntax and Usage
<pre>show vlag information</pre> <p>Displays vLAG Information. For details, see <a href="#">page 46</a>.</p> <p>Command mode: All</p>
<pre>show dot1x information</pre> <p>Displays 802.1X Information. For details, see <a href="#">page 33</a>.</p> <p><b>Command mode:</b> All</p>
<pre>show spanning-tree</pre> <p>Displays Spanning Tree information, including the status (on or off), Spanning Tree mode (RSTP, PVRST, or MSTP), and VLAN membership.</p> <p>In addition to seeing if STG is enabled or disabled, you can view the following STG bridge information:</p> <ul style="list-style-type: none"><li>– Priority</li><li>– Hello interval</li><li>– Maximum age value</li><li>– Forwarding delay</li><li>– Aging time</li></ul> <p>You can also see the following port-specific STG information:</p> <ul style="list-style-type: none"><li>– Port alias and priority</li><li>– Cost</li><li>– State</li></ul> <p><b>Command mode:</b> All</p>
<pre>show spanning-tree root</pre> <p>Displays the Spanning Tree configuration on the root bridge for each STP instance.</p> <p><b>Command mode:</b> All</p> <p>For details, see <a href="#">page 51</a>.</p>
<pre>show spanning-tree blockedports</pre> <p>Lists the ports blocked by each STP instance.</p> <p><b>Command mode:</b> All</p>
<pre>show spanning-tree stp &lt;1-128&gt; information</pre> <p>Displays information about a specific Spanning Tree Group.</p> <p><b>Command mode:</b> All</p> <p>For details, see <a href="#">page 47</a>.</p>

Table 20. Layer 2 Information Commands (continued)

Command Syntax and Usage
<p><code>show spanning-tree mst &lt;0-32&gt; information</code></p> <p>Displays Common Internal Spanning Tree (CIST) information for the specified instance, including the MSTP digest and VLAN membership.</p> <p>CIST bridge information includes:</p> <ul style="list-style-type: none"> <li>– Priority</li> <li>– Hello interval</li> <li>– Maximum age value</li> <li>– Forwarding delay</li> <li>– Root bridge information (priority, MAC address, path cost, root port)</li> </ul> <p>CIST port information includes:</p> <ul style="list-style-type: none"> <li>– Port number and priority</li> <li>– Cost</li> <li>– State</li> </ul> <p>For details, see <a href="#">page 52</a>.</p> <p><b>Command mode:</b> All</p>
<p><code>show spanning-tree mst configuration</code></p> <p>Displays the current MSTP settings.</p> <p><b>Command mode:</b> All</p>
<p><code>show portchannel information</code></p> <p>Displays the state of each port in the various trunk groups. For details, see <a href="#">page 55</a>.</p> <p><b>Command mode:</b> All</p>
<p><code>show vlan</code></p> <p>Displays VLAN configuration information for all configured VLANs, including:</p> <ul style="list-style-type: none"> <li>– VLAN Number</li> <li>– VLAN Name</li> <li>– Status</li> <li>– Port membership of the VLAN</li> </ul> <p>For details, see <a href="#">page 55</a>.</p> <p><b>Command mode:</b> All</p>
<p><code>show failover trigger &lt;trigger number&gt; information</code></p> <p>Displays Layer 2 Failover information. For details, see <a href="#">page 39</a>.</p> <p><b>Command mode:</b> All</p>
<p><code>show hotlinks information</code></p> <p>Displays Hot Links information. For details, see <a href="#">page 41</a>.</p> <p><b>Command mode:</b> All</p>

Table 20. Layer 2 Information Commands (continued)

Command Syntax and Usage
<pre>show lldp information</pre> <p>Displays Link Layer Discovery Protocol (LLDP) information. For details, see <a href="#">page 41</a>.</p> <p><b>Command mode:</b> All</p>
<pre>show layer2 information</pre> <p>Dumps all Layer 2 switch information available (10K or more, depending on your configuration).</p> <p>If you want to capture dump data to a file, set your communication software on your workstation to capture session data prior to issuing the dump commands.</p> <p><b>Command mode:</b> All</p>



## 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 21. 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"> <li>- force-unauth</li> <li>- auto</li> <li>- force-auth</li> </ul>
Auth Status	Displays the current authorization status of the port, either authorized or unauthorized.

Table 21. 802.1X Parameter Descriptions (continued)

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

## 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 22. FDB Information Options

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

Table 22. FDB Information Options (continued)

Command Syntax and Usage
<pre>show mac-address-table counters all</pre> <p>Displays all FDB statistics for all FDB entries.</p> <p><b>Command mode:</b> All</p>
<pre>show mac-address-table counters interface port &lt;port alias or number&gt;</pre> <p>Displays FDB statistics for a particular port.</p> <p><b>Command mode:</b> All</p>
<pre>show mac-address-table counters portchannel &lt;trunk group number&gt;</pre> <p>Displays all FDB statistics for a particular trunk group (portchannel).</p> <p><b>Command mode:</b> All</p>
<pre>show mac-address-table counters state {unknown forward trunk}</pre> <p>Displays all FDB statistics for a particular state.</p> <p><b>Command mode:</b> All</p>
<pre>show mac-address-table counters static</pre> <p>Displays all FDB statistics for all static FDB entries.</p> <p><b>Command mode:</b> All</p>
<pre>show mac-address-table counters unicast</pre> <p>Displays all FDB statistics for all Unicast FDB entries.</p> <p><b>Command mode:</b> All</p>
<pre>show mac-address-table counters vlan &lt;vlan no.&gt;</pre> <p>Displays all FDB statistics on a single VLAN.</p> <p><b>Command mode:</b> All</p>
<pre>show mac-address-table</pre> <p>Displays all entries in the Forwarding Database.</p> <p><b>Command mode:</b> All</p>

## FDB Multicast Information

The following commands display FDB multicast information.

Table 23. Multicast FDB Information Options

Command Syntax and Usage
<pre>show mac-address-table multicast address &lt;MAC address&gt; [&lt;VLAN&gt;]</pre> <p>Displays a single multicast entry by its MAC address. You are prompted to enter the MAC address of the device. Enter the MAC address using the format, xx:xx:xx:xx:xx:xx. For example, 08:00:20:12:34:56</p> <p>You can also enter the MAC address using the format, xxxxxxxxxxxx. For example, 080020123456</p>
<pre>show mac-address-table multicast interface &lt;port number&gt;</pre> <p>Displays all multicast entries for a particular port.</p>
<pre>show mac-address-table multicast vlan &lt;VLAN number&gt;</pre> <p>Displays all multicast entries on a single VLAN.</p>
<pre>show mac-address-table multicast</pre> <p>Displays all Multicast MAC entries in the FDB.</p> <p><b>Command mode:</b> All</p>

## Show All FDB Information

The following command displays Forwarding Database information:

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

**Command mode:** All

MAC address	VLAN	Port	Trnk	State	Permanent
00:04:38:90:54:18	1	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 are listed under "Reference ports."

## Clearing Entries from the Forwarding Database

To clear the entire FDB, refer to ["Forwarding Database Maintenance" on page 557](#).

## Link Aggregation Control Protocol Information

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

Table 24. LACP Information Options

Command Syntax and Usage
<pre>show lacp aggregator &lt;aggregator ID&gt;</pre> <p>Displays detailed information about the LACP aggregator.</p> <p><b>Command mode:</b> All</p>
<pre>show interface port &lt;port alias or number&gt; lacp information</pre> <p>Displays LACP information about the selected port.</p> <p><b>Command mode:</b> All</p>
<pre>show lacp information</pre> <p>Displays a summary of LACP information. For details, see <a href="#">page 38</a>.</p> <p><b>Command mode:</b> All</p>

## Link Aggregation Control Protocol

The following command displays LACP information:

```
show lacp information
```

**Command mode:** All

port	mode	adminkey	operkey	selected	prio	aggr	trunk	status	minlinks
1	off	1	1	no	32768	--	--	--	1
2	off	2	2	no	32768	--	--	--	1
3	off	3	3	no	32768	--	--	--	1
4	off	4	4	no	32768	--	--	--	1
...									

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, down or standby).
- **minlinks** Displays the minimum number of active links in the LACP trunk.

## Layer 2 Failover Information

Table 25. Layer 2 Failover Information Options

Command Syntax and Usage
<pre>show failover trigger &lt;trigger number&gt; information</pre> <p>Displays detailed information about the selected Layer 2 Failover trigger.</p> <p><b>Command mode:</b> All</p>
<pre>show failover trigger information</pre> <p>Displays a summary of Layer 2 Failover information. For details, see <a href="#">page 39</a>.</p> <p><b>Command mode:</b> All</p>

## Layer 2 Failover Information

The following command displays Layer 2 Failover information:

```
show failover trigger information
```

**Command mode:** All

<pre>Failover: On  Trigger 1 Manual Monitor: Enabled Trigger 1 limit: 0 Monitor State: Up Member      Status -----  17         Operational Control State: Auto Controlled Member      Status ----- Physical ports  1         Operational  Trigger 2: Disabled  Trigger 3: Disabled  Trigger 4: Disabled  Trigger 5: Disabled  Trigger 6: Disabled  Trigger 7: Disabled  Trigger 8: Disabled</pre>
---

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

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

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

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

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



## Hot Links Information

The following command displays Hot Links information:

```
show hotlinks information
```

**Command mode:** All

```
Hot Links Info: Trigger

Current global Hot Links setting: ON
bpdudisabled
snrfdbsdisabled

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

The following commands display LLDP information.

*Table 26. LLDP Information Options*

<b>Command Syntax and Usage</b>
<pre>show lldp port</pre> <p>Displays Link Layer Discovery Protocol (LLDP) port information.</p> <p><b>Command mode:</b> All</p>
<pre>show lldp transmit</pre> <p>Displays information about the LLDP transmit state machine.</p> <p><b>Command mode:</b> All</p>
<pre>show lldp receive</pre> <p>Displays information about the LLDP receive state machine.</p> <p><b>Command mode:</b> All</p>
<pre>show lldp remote-device [&lt;1-256&gt; detail]</pre> <p>Displays information received from LLDP-capable devices. For more information, see <a href="#">page 42</a>.</p> <p><b>Command mode:</b> All</p>

Table 26. LLDP Information Options

Command Syntax and Usage
<pre>show lldp remote-device port &lt;port number&gt;</pre> <p>Displays information received from LLDP-capable devices for a specific port. A given list of ports needs to be delimited by ',' and a range of ports delimited by '-'.</p> <p><b>Command mode:</b> All</p>
<pre>show lldp port &lt;1-16&gt; tlv evb</pre> <p>Displays Edge Virtual Bridge (EVB) type-length-value (TLV) information.</p> <p><b>Command mode:</b> All</p>
<pre>show lldp information</pre> <p>Displays all LLDP information.</p> <p><b>Command mode:</b> All</p>

## LLDP Remote Device Information

The following command displays LLDP remote device information:

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

**Command mode:** All

```
LLDP Remote Devices Information
Legend(possible values in DMAC column) :
NB - Nearest Bridge - 01-80-C2-00-00-0E
NnTB - Nearest non-TPMR Bridge - 01-80-C2-00-00-03
NCB - Nearest Customer Bridge - 01-80-C2-00-00-00
Total number of current entries: 9
```

LocalPort	Index	Remote Chassis ID	Remote Port	Remote System Name	DMAC
XGE2	1	34 40 b5 6d ce 00	17		NB
1	2	00 00 00 00 11 00	30		NB
XGE4	3	00 e0 00 01 00 00	62		NB

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

```

Local Port Alias: 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      : IBM Networking Operating System RackSwitch G8264, IBM
Networking OS: version 7.4.0,13 Boot image: version 7.4.0.13
  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 27. UDLD Information Options

Command Syntax and Usage
<pre>show interface port &lt;port alias or number&gt; udld</pre> <p>Displays UDLD information about the selected port.</p> <p><b>Command mode:</b> All</p>
<pre>show udld</pre> <p>Displays all UDLD information.</p> <p><b>Command mode:</b> All</p>

## UDLD Port Information

The following command displays UDLD information for the selected port:

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

**Command mode:** All

```
UDLD information on port 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)

## 802.1x Discovery Information

Table 28. 802.1x Discovery Information Options

Command Syntax and Usage
<pre>show interface port &lt;port alias or number&gt; dot1x</pre> <p>Displays 802.1x information about the selected port.</p> <p><b>Command mode:</b> All</p>
<pre>show dot1x</pre> <p>Displays all 802.1x information.</p> <p><b>Command mode:</b> All</p>

## 802.1x Port Information

The following command displays 802.1x information for the selected port:

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

**Command mode:** All

Port	Auth Mode	Quiet Period	Tx Period	Max Req	Supp Timeout	Server Timeout	ReAuth Status	ReAuth Period	VLAN Assign
G	force-auth	60	30	2	30	30	off	3600	off
1	force-auth	60	30	2	30	30	off	3600	off

-----  
G - Global port configuration

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

## OAM Discovery Information

Table 29. OAM Discovery Information Options

Command Syntax and Usage
<pre>show interface port &lt;port alias or number&gt; oam</pre> <p>Displays OAM information about the selected port.</p> <p><b>Command mode:</b> All</p>
<pre>show oam</pre> <p>Displays all OAM information.</p> <p><b>Command mode:</b> All</p>

## OAM Port Information

The following command displays OAM information for the selected port:

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

**Command mode:** All

<pre>OAM information on port 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</pre>
---

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

## vLAG Information

Table 30. vLAG Information Options

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

## vLAG Trunk Information

The following command displays vLAG information for the trunk group:

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

**Command mode:** All

<pre>vLAG is enabled on trunk 13 Protocol - Static Current settings: enabled   ports: 13 Current L2 trunk hash settings:   smac dmac Current L3 trunk hash settings:   sip dip Current ingress port hash: disabled Current L4 port hash: disabled</pre>
---

## Spanning Tree Information

The following command displays Spanning Tree information:

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

**Command mode:** All

```
Spanning Tree Group 1: On (RSTP)
VLANs: 1 10 4095

Current Root:          Path-Cost  Port Hello MaxAge FwdDel
8000 00:25:03:49:29:00    0      0   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  (pc12) 128   490!+ FWD   DESG 8000-00:25:03:49:29:00  8026 P2P
2  (pc12) 128   490!+ FWD   DESG 8000-00:25:03:49:29:00  8026 P2P
3  (pc12) 128   490!+ FWD   DESG 8000-00:25:03:49:29:00  8026 P2P
4  (pc12) 128   490!+ FWD   DESG 8000-00:25:03:49:29:00  8026 P2P
MGT      0      0    FWD *
* = STP turned off for this port.
! = Automatic path cost.
+ = Portchannel cost, not the individual port cost.
```

The switch software uses the Per VLAN Rapid Spanning Tree Protocol (PVRST) spanning tree mode, with IEEE 802.1w Rapid Spanning Tree Protocol (RSTP) or IEEE 802.1s Multiple Spanning Tree Protocol (MSTP), as alternatives. For details see [“RSTP/PVRST Information” on page 49](#).

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

*Table 31. PVRST/RSTP/MSTP Bridge Parameter Descriptions*

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

Table 31. PVRST/RSTP/MSTP Bridge Parameter Descriptions (continued)

Parameter	Description
Aging	The Aging Time parameter specifies, in seconds, the amount of time the bridge waits without receiving a packet from a station before removing the station from the Forwarding Database.
Topology Change Count	The Topology Change Count shows the number of Topology Changes detected since the last initialization of the Spanning Tree Group (either by reboot or by Spanning Tree mode change).

The following port-specific information is also displayed:

Table 32. PVRST/RSTP/MSTP Port Parameter Descriptions

Parameter	Description
Priority (port)	The Port Priority parameter helps determine which bridge port becomes the designated port. In a network topology that has multiple bridge ports connected to a single segment, the port with the lowest port priority becomes the designated port for the segment.
Cost	The Port Path cost parameter is used to help determine the designated port for a segment. Generally speaking, the faster the port, the lower the path cost. A setting of 0 indicates that the cost will be set to the appropriate default after the link speed has been auto negotiated.
State	The State field shows the current state of the port. The State field can be one of the following: Discarding (DISC), Learning (LRN), or Forwarding (FWD).
Role	The Role field shows the current role of this port in the Spanning Tree. The port role can be one of the following: Designated (DESG), Root (ROOT), Alternate (ALTN), Backup (BKUP).
Designated Bridge	The Designated Bridge shows information about the bridge connected to each port, if applicable. Information includes the priority (in hexadecimal notation) and MAC address of the Designated Bridge.
Designated Port	The Designated Port field shows the port on the Designated Bridge to which this port is connected.
Type	Type of link connected to the port, and whether the port is an edge port. Link type values are AUTO, P2P, or SHARED.



## RSTP/PVRST Information

The following command displays RSTP/PVRST information:

```
show spanning-tree rstp <I-128> information
```

**Command mode:** All I

```

-----
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 33. 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.

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

Parameter	Description
MaxAge	The Maximum Age parameter specifies, in seconds, the maximum time the bridge waits without receiving a configuration bridge protocol data unit before it 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 34. RSTP/MSTP/PVRST Port Parameter Descriptions

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

## Spanning Tree Bridge Information

The following command displays Spanning Tree bridge information:

```
show spanning-tree [vlan <VLAN ID>] bridge
```

**Command mode:** All

Vlan	Priority	Hello	MaxAge	FwdDel	Protocol
-----	-----	-----	-----	-----	-----
1	32768	2	20	15	MSTP

Table 35. Bridge Parameter Descriptions

Parameter	Description
VLAN	VLANs that are part of the Spanning Tree Group
Priority	The bridge priority parameter controls which bridge on the network will become the STP root bridge. The lower the value, the higher the priority.
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 learning state to forwarding state.
Protocol	The STP protocol run by the Spanning Tree Group

## Spanning Tree Root Information

The following command displays information about the root switches in every STP group:

```
show spanning-tree root
```

**Command mode:** All

Instance	Root ID	Path-Cost	Hello	MaxAge	FwdDel	Root Port
-----	-----	-----	-----	-----	-----	-----
1	8001 08:17:f4:32:95:00	0	2	20	15	0
3	8003 08:17:f4:32:95:00	0	2	20	15	0
6	8001 08:17:f4:fb:d8:00	20000	2	20	15	27
17	8011 08:17:f4:32:95:00	0	2	20	15	0

Table 36. Bridge Parameter Descriptions

Parameter	Description
Instance	Spanning Tree instance
Root ID	Indicates the root switch MAC address and port number.
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.
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.
Root Port	Port number allocated to the STP instance on the root switch.

## Multiple Spanning Tree Information

The following command displays Multiple Spanning Tree (MSTP) information:

```
show spanning-tree mst <0-32> 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 37. 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 38. CIST Parameter Descriptions

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

Table 38. CIST Parameter Descriptions (continued)

Parameter	Description
Role	The Role field shows the current role of this port in the Spanning Tree. The port role can be one of the following: Designated (DESIGNATED), Root (ROOT), Alternate (ALTERNATE), Backup (BACKUP), Disabled (DISABLED), Master (MASTER), or Unknown (UNKNOWN).
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 39. VLAN Information Options

Command Syntax and Usage
<pre>show vlan &lt;VLAN number&gt;</pre> <p>Displays general VLAN information.</p> <p><b>Command mode:</b> All</p>
<pre>show protocol-vlan &lt;protocol number (1-8)&gt;</pre> <p>Displays Protocol VLAN information.</p> <p><b>Command mode:</b> All</p>

Table 39. VLAN Information Options (continued)

Command Syntax and Usage	
<pre>show vlan private-vlan [type]</pre> <p>Displays Private VLAN information.</p> <ul style="list-style-type: none"> <li>- type lists only the VLAN type for each private VLAN: community, isolated or primary</li> </ul> <p><b>Command mode:</b> All s</p>	
<pre>show vlan information</pre> <p>Displays information about all VLANs, including:</p> <ul style="list-style-type: none"> <li>- VLAN number and name</li> <li>- Port membership</li> <li>- VLAN status (enabled or disabled)</li> <li>- Protocol VLAN status</li> <li>- Private VLAN status</li> <li>- Spanning Tree membership</li> <li>- VMAP configuration</li> </ul> <p><b>Command mode:</b> All</p>	

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
100	VLAN 100		ena	empty
200	VLAN 200		ena	empty
300	VLAN 300		ena	empty
4095	Mgmt VLAN		ena	MGT
	Primary	Secondary	Type	Ports
	100	200	isolated	14
	100	300	community	12

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 40. Layer 3 Information Commands

Command Syntax and Usage
<pre>show ip route</pre> <p>Displays all routes configured on the switch. For details, see <a href="#">page 61</a>.</p> <p><b>Command mode:</b> All</p>
<pre>show arp</pre> <p>Displays Address Resolution Protocol (ARP) information. For details, see <a href="#">page 62</a>.</p> <p><b>Command mode:</b> All</p>
<pre>show ip bgp information [IPv4 address] [IPv4 mask]</pre> <p>Displays Border Gateway Protocol (BGP) information. For details, see <a href="#">page 67</a>.</p> <p><b>Command mode:</b> All</p>
<pre>show ip ospf information</pre> <p>Displays the OSPF information. For details, see <a href="#">page 68</a>.</p> <p><b>Command mode:</b> All</p>
<pre>show ipv6 ospf information</pre> <p>Displays OSPFv3 information. For more OSPFv3 information options, see <a href="#">page 73</a>.</p> <p><b>Command mode:</b> All</p>
<pre>show ip rip interface</pre> <p>Displays RIP user's configuration. For details, see <a href="#">page 77</a>.</p> <p><b>Command mode:</b> All</p>
<pre>show ipv6 route</pre> <p>Displays IPv6 routing information. For more information options, see <a href="#">page 78</a>.</p> <p><b>Command mode:</b> All</p>
<pre>show ipv6 neighbors</pre> <p>Displays IPv6 Neighbor Discovery cache information. For more information options, see <a href="#">page 79</a>.</p> <p><b>Command mode:</b> All</p>
<pre>show ipv6 prefix</pre> <p>Displays IPv6 Neighbor Discovery prefix information. For details, see <a href="#">page 80</a>.</p> <p><b>Command mode:</b> All</p>
<pre>show ip ecmp</pre> <p>Displays ECMP static route information. For details, see <a href="#">page 80</a>.</p> <p><b>Command mode:</b> All</p>

Table 40. Layer 3 Information Commands (continued)

Command Syntax and Usage
<pre>show ip igmp groups</pre> <p>Displays IGMP Information. For more IGMP information options, see <a href="#">page 81</a>.</p> <p><b>Command mode:</b> All</p>
<pre>show ipv6 mld groups</pre> <p>Displays Multicast Listener Discovery (MLD) information. For more MLD information options, see <a href="#">page 86</a>.</p> <p><b>Command mode:</b> All</p>
<pre>show ip vrrp information</pre> <p>Displays VRRP information. For details, see <a href="#">page 88</a>.</p> <p><b>Command mode:</b> All</p>
<pre>show interface ip</pre> <p>Displays IP interface Information. For details, see <a href="#">page 89</a>.</p> <p><b>Command mode:</b> All</p>
<pre>show ipv6 interface &lt;interface number&gt;</pre> <p>Displays IPv6 interface information. For details, see <a href="#">page 90</a>.</p> <p><b>Command mode:</b> All</p>
<pre>show ipv6 pmtu [&lt;destination IPv6 address&gt;]</pre> <p>Displays IPv6 Path MTU information. For details, see <a href="#">page 91</a>.</p> <p><b>Command mode:</b> All</p>
<pre>show ip interface brief</pre> <p>Displays IP Information. For details, see <a href="#">page 92</a>.</p> <p>IP information, includes:</p> <ul style="list-style-type: none"> <li>– IP interface information: Interface number, IP address, subnet mask, VLAN number, and operational status.</li> <li>– Default gateway information: Metric for selecting which configured gateway to use, gateway number, IP address, and health status</li> <li>– IP forwarding settings, network filter settings, route map settings</li> </ul> <p><b>Command mode:</b> All</p>
<pre>show ikev2</pre> <p>Displays IKEv2 information. For more information options, see <a href="#">page 93</a>.</p> <p><b>Command mode:</b> All</p>
<pre>show ipsec manual-policy</pre> <p>Displays information about manual key management policy for IP security. For more information options, see <a href="#">page 95</a>.</p> <p><b>Command mode:</b> All</p>

Table 40. Layer 3 Information Commands (continued)

Command Syntax and Usage
<pre>show ip dhcp snooping binding</pre> <p>Displays DHCP Snooping information. For details, see <a href="#">page 97</a>.</p> <p><b>Command mode:</b> All</p>
<pre>show ip pim component [&lt;1-2&gt;]</pre> <p>Displays Protocol Independent Multicast (PIM) component information. For more PIM information options, see <a href="#">page 98</a>.</p> <p><b>Command mode:</b> All</p>
<pre>show layer3</pre> <p>Dumps all Layer 3 switch information available (10K or more, depending on your configuration).</p> <p>If you want to capture dump data to a file, set your communication software on your workstation to capture session data before issuing the dump commands.</p> <p><b>Command mode:</b> All</p>

## IP Routing Information

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

Table 41. Route Information Options

Command Syntax and Usage
<pre>show ip route address &lt;IP address&gt;</pre> <p>Displays a single route by destination IP address.</p> <p><b>Command mode:</b> All</p>
<pre>show ip route gateway &lt;IP address&gt;</pre> <p>Displays routes to a single gateway.</p> <p><b>Command mode:</b> All</p>
<pre>show ip route type {indirect direct local broadcast martian multicast}</pre> <p>Displays routes of a single type. For a description of IP routing types, see <a href="#">Table 42 on page 61</a>.</p> <p><b>Command mode:</b> All</p>
<pre>show ip route tag {fixed static addr rip ospf bgp broadcast martian multicast}</pre> <p>Displays routes of a single tag. For a description of IP routing tags, see <a href="#">Table 43 on page 61</a>.</p> <p><b>Command mode:</b> All</p>
<pre>show ip route interface &lt;interface number&gt;</pre> <p>Displays routes on a single interface.</p> <p><b>Command mode:</b> All</p>
<pre>show ip route ecmphash</pre> <p>Displays the current ECMP hashing mechanism.</p> <p><b>Command mode:</b> All</p>
<pre>show ip route static</pre> <p>Displays static routes configured on the switch.</p> <p><b>Command mode:</b> All</p>
<pre>show ip route</pre> <p>Displays all routes configured in the switch.</p> <p><b>Command mode:</b> All</p> <p>For more information, see <a href="#">page 61</a>.</p>

## Show All IP Route Information

The following command displays IP route information:

```
show ip route
```

**Command mode:** All

Status code: * - best						
Destination	Mask	Gateway	Type	Tag	Metr	If
* 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 42. IP Routing Type Parameters*

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

The following table describes the `Tag` parameters.

*Table 43. 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)

Table 43. IP Routing Tag Parameters (continued)

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

## ARP Information

The ARP information includes IP address and MAC address of each entry, address status flags (see [Table 45 on page 63](#)), VLAN and port for the address, and port referencing information.

Table 44. ARP Information Options

Command Syntax and Usage
<pre>show arp find &lt;IP address&gt;</pre> <p>Displays a single ARP entry by IP address.</p> <p><b>Command mode:</b> All</p>
<pre>show arp interface port &lt;port alias or number&gt;</pre> <p>Displays the ARP entries on a single port.</p> <p><b>Command mode:</b> All</p>
<pre>show arp vlan &lt;VLAN number&gt;</pre> <p>Displays the ARP entries on a single VLAN.</p> <p><b>Command mode:</b> All</p>
<pre>show arp</pre> <p>Displays all ARP entries, including:</p> <ul style="list-style-type: none"> <li>– IP address and MAC address of each entry</li> <li>– Address status flag</li> <li>– The VLAN and port to which the address belongs</li> <li>– The ports which have referenced the address (empty if no port has routed traffic to the IP address shown)</li> </ul> <p>For more information, see <a href="#">page 63</a>.</p> <p><b>Command mode:</b> All</p>
<pre>show arp reply</pre> <p>Displays the ARP address list: IP address, IP mask, MAC address, and VLAN flags.</p> <p><b>Command mode:</b> All</p>

## 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 45. 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 46. BGP Peer Information Options

Command Syntax and Usage
<pre>show ip bgp neighbor information</pre> <p>Displays BGP peer information. See <a href="#">page 64</a> for a sample output.</p> <p><b>Command mode:</b> All</p>
<pre>show ip bgp neighbor group</pre> <p>Displays BGP group information. See <a href="#">page 66</a> for a sample output.</p> <p><b>Command mode:</b> All</p>
<pre>show ip bgp neighbor summary</pre> <p>Displays peer summary information such as AS, message received, message sent, up/down, state. See <a href="#">page 67</a> for a sample output.</p> <p><b>Command mode:</b> All</p>
<pre>show ip bgp neighbor &lt;neighbor number&gt; redistribution</pre> <p>Displays BGP neighbor redistribution.</p> <p><b>Command mode:</b> All</p>
<pre>show ip bgp neighbor &lt;neighbor number&gt; routes</pre> <p>Displays BGP peer routes.</p> <p><b>Command mode:</b> All</p>
<pre>show ip bgp information</pre> <p>Displays the BGP routing table. See <a href="#">page 67</a> for a sample output.</p> <p><b>Command mode:</b> All</p>

### BGP Peer information

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

```
show ip bgp neighbor information
```



## Command mode: All

### BGP Peer Information:

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

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

## BGP Group information

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

```
show ip bgp neighbor group
```

**Command mode:** All

```
BGP Group Information:
Local router ID: 1.1.1.2, Local AS: 100
Group 1:
  Name: toG82642007
  Addr: 192.168.128.0   Mask: 255.255.255.248
  Remote AS list: 200
  Dynamic Peers Limit: 8
  Dynamic Peers in established state: 1
Dynamic Peers of this group:
97: 192.168.128.4, Group: 1 (toG82642007), TTL 1
  Remote AS: 200, Local AS: 100, Link type: EBGP
  Remote router ID: 2.2.1.2, Local router ID: 1.1.1.2
  Configured Version: 4
  Negotiated Version: 4
  Total path attribute out: 0
  In Total Messages: 74
  Out Total Messages: 74
  In Updates: 0
  Out Updates: 0
  Established Time: 01:12:36
  MinAdvTime: 00:01:00
  Configured holdtime: 00:03:00
  Negotiated holdtime: 00:03:00
  Configured keepalive 00:01:00
  Negotiated keepalive 00:01:00
  In Update Last Time: 00:00:00
  Out Update Last Time: 00:14:32
  Last Send Time: 01:26:54
  Last Received Time: 01:26:54
  In-rmap list count: 0
  Out-rmap list count: 0
...
```

## 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 [<IPv4 network> <IPv4 mask>]
```

**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 rrmmap; or, a loop detected.

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

## OSPF Information

Table 47. OSPF Information Options

Command Syntax and Usage
<pre>show ip ospf general-information</pre> <p>Displays general OSPF information. See <a href="#">page 69</a> for a sample output.</p> <p><b>Command mode:</b> All</p>
<pre>show ip ospf area information</pre> <p>Displays area information for all areas.</p> <p><b>Command mode:</b> All</p>
<pre>show ip ospf area &lt;area index&gt;</pre> <p>Displays area information for a particular area index.</p> <p><b>Command mode:</b> All</p>
<pre>show interface ip {&lt;interface number&gt;} ospf</pre> <p>Displays interface information for a particular interface. If no parameter is supplied, it displays information for all the interfaces. See <a href="#">page 70</a> for a sample output.</p> <p><b>Command mode:</b> All</p>
<pre>show interface loopback {&lt;interface number&gt;}</pre> <p>Displays loopback information for a particular interface. If no parameter is supplied, it displays loopback information for all the interfaces. See <a href="#">page 70</a> for a sample output.</p> <p><b>Command mode:</b> All</p>
<pre>show ip ospf area-virtual-link information</pre> <p>Displays information about all the configured virtual links.</p> <p><b>Command mode:</b> All</p>
<pre>show ip ospf neighbor</pre> <p>Displays the status of all the current neighbors.</p> <p><b>Command mode:</b> All</p>
<pre>show ip ospf summary-range &lt;area index&gt;</pre> <p>Displays the list of summary ranges belonging to non-NSSA areas.</p> <p><b>Command mode:</b> All</p>
<pre>show ip ospf summary-range-nssa &lt;area index&gt;</pre> <p>Displays the list of summary ranges belonging to NSSA areas.</p> <p><b>Command mode:</b> All</p>

Table 47. OSPF Information Options (continued)

Command Syntax and Usage
<pre>show ip ospf routes</pre> <p>Displays OSPF routing table. See <a href="#">page 72</a> for a sample output.</p> <p><b>Command mode:</b> All</p>
<pre>show ip ospf information</pre> <p>Displays the OSPF information.</p> <p><b>Command mode:</b> All</p>

## OSPF General Information

The following command displays general OSPF information:

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

**Command mode:** All

```
OSPF Version 2
Router ID: 10.10.10.1
Started at 1663 and the process uptime is 4626
Area Border Router: yes, AS Boundary Router: no
LS types supported are 6
External LSA count 0
External LSA checksum sum 0x0
Number of interfaces in this router is 2
Number of virtual links in this router is 1
16 new lsa received and 34 lsa originated from this router
Total number of entries in the LSDB 10
Database checksum sum 0x0
Total neighbors are 1, of which
                2 are >=INIT state,
                2 are >=EXCH state,
                2 are =FULL state
Number of areas is 2, of which 3-transit 0-nssa
  Area Id : 0.0.0.0
  Authentication : none
  Import ASEextern : yes
  Number of times SPF ran : 8
  Area Border Router count : 2
  AS Boundary Router count : 0
  LSA count : 5
  LSA Checksum sum : 0x2237B
  Summary : noSummary
```

## OSPF Interface 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 Loopback Information

The following command displays loopback information for a particular interface. If no parameter is supplied, it displays loopback information for all the interfaces:

```
show ip ospf interface loopback
```

**Command mode:** All

```
Ip Address 123.123.123.1, Area 0.0.0.0, Passive interface, Admin Status UP
Router ID 1.1.1.1, State Loopback, Priority 1
Designated Router (ID) 0.0.0.0, Ip Address 0.0.0.0
Backup Designated Router (ID) 0.0.0.0, Ip Address 0.0.0.0
Timer intervals, Hello 10, Dead 40, Wait 40, Retransmit 5, Transit delay 1
Neighbor count is 0   If Events 1, Authentication type none
```

## OSPF Database Information

Table 48. OSPF Database Information Options

Command Syntax and Usage
<pre>show ip ospf database advertising-router &lt;router ID&gt;</pre> <p>Takes advertising router as a parameter. Displays all the Link State Advertisements (LSAs) in the LS database that have the advertising router with the specified router ID, for example: 20.1.1.1.</p> <p><b>Command mode:</b> All</p>
<pre>show ip ospf database asbr-summary [advertising-router &lt;router ID&gt; link-state-id &lt;A.B.C.D&gt; self]</pre> <p>Displays ASBR summary LSAs. The usage of this command is as follows:</p> <ol style="list-style-type: none"> <li>asbr-summary advertising-router 20.1.1.1 displays ASBR summary LSAs having the advertising router 20.1.1.1.</li> <li>asbr-summary link-state-id 10.1.1.1 displays ASBR summary LSAs having the link state ID 10.1.1.1.</li> <li>asbr-summary self displays the self advertised ASBR summary LSAs.</li> <li>asbr-summary with no parameters displays all the ASBR summary LSAs.</li> </ol> <p><b>Command mode:</b> All</p>
<pre>show ip ospf database database-summary</pre> <p>Displays the following information about the LS database in a table format:</p> <ol style="list-style-type: none"> <li>Number of LSAs of each type in each area.</li> <li>Total number of LSAs for each area.</li> <li>Total number of LSAs for each LSA type for all areas combined.</li> <li>Total number of LSAs for all LSA types for all areas combined.</li> </ol> <p>No parameters are required.</p> <p><b>Command mode:</b> All</p>
<pre>show ip ospf database external [advertising-router &lt;router ID&gt;  link-state-id &lt;A.B.C.D&gt; self]</pre> <p>Displays the AS-external (type 5) LSAs with detailed information of each field of the LSAs.</p> <p><b>Command mode:</b> All</p>
<pre>show ip ospf database network [advertising-router &lt;router ID&gt;  link-state-id &lt;A.B.C.D&gt; self]</pre> <p>Displays the network (type 2) LSAs with detailed information of each field of the LSA.network LS database.</p> <p><b>Command mode:</b> All</p>
<pre>show ip ospf database nssa</pre> <p>Displays the NSSA (type 7) LSAs with detailed information of each field of the LSAs.</p> <p><b>Command mode:</b> All</p>

Table 48. OSPF Database Information Options (continued)

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

## OSPF Information Route Codes

The following command displays OSPF route information:

```
show ip ospf routes
```

**Command mode:** All

<pre>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</pre>
--



## OSPFv3 Information

Table 49. OSPFv3 Information Options

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

Table 49. OSPFv3 Information Options (continued)

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

## OSPFv3 Information Dump

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

## OSPFv3 Interface Information

The following command displays OSPFv3 interface information:

```
show ipv6 ospf interface
```

**Command mode:** All

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

## OSPFv3 Database Information

Table 50. OSPFv3 Database Information Options

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

Table 50. OSPFv3 Database Information Options (continued)

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

## OSPFv3 Route Codes Information

The following command displays OSPFv3 route information:

```
show ipv6 ospf routes
```

**Command mode:** All

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

# Routing Information Protocol

Table 51. Routing Information Protocol Options

Command Syntax and Usage
<pre>show ip rip routes</pre> <p>Displays RIP routes.</p> <p><b>Command mode:</b> All</p> <p>For more information, see <a href="#">page 77</a>.</p>
<pre>show ip rip interface &lt;interface number&gt;</pre> <p>Displays RIP user's configuration.</p> <p><b>Command mode:</b> All</p> <p>For more information, see <a href="#">page 77</a>.</p>

## RIP Routes Information

The following command displays RIP route information:

```
show ip rip routes
```

**Command mode:** All

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

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

## RIP Interface Information

The following command displays RIP user information:

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

**Command mode:** All

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

## IPv6 Routing Information

[Table 52](#) describes the IPv6 Routing information options.

*Table 52. IPv6 Routing Information Options*

Command Syntax and Usage
<pre>show ipv6 route address &lt;IPv6 address&gt;</pre> <p>Displays a single route by destination IP address.</p>
<pre>show ipv6 route gateway &lt;default gateway address&gt;</pre> <p>Displays routes to a single gateway.</p>
<pre>show ipv6 route type {connected static ospf}</pre> <p>Displays routes of a single type. For a description of IP routing types, see <a href="#">Table 42 on page 61</a>.</p>
<pre>show ipv6 route interface &lt;interface number&gt;</pre> <p>Displays routes on a single interface.</p>
<pre>show ipv6 route summary</pre> <p>Displays a summary of IPv6 routing information, including inactive routes.</p>
<pre>show ipv6 route</pre> <p>Displays all IPv6 routing information. For more information, see <a href="#">page 78</a>.</p>

## IPv6 Routing Table Information

The following command displays IPv6 routing information:

```
show ipv6 route
```

**Command mode:** All

<pre>IPv6 Routing Table - 3 entries Codes : C - Connected, S - Static         O - OSPF         M - Management Gateway  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]</pre>
--

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 53. IPv6 Neighbor Discovery Cache Information Options

Command Syntax and Usage
<pre>show ipv6 neighbors find &lt;IPv6 address&gt;</pre> <p>Displays a single IPv6 Neighbor Discovery cache entry by IP address.  <b>Command mode:</b> All</p>
<pre>show ipv6 neighbors interface port &lt;port alias or number&gt;</pre> <p>Displays IPv6 Neighbor Discovery cache entries on a single port.  <b>Command mode:</b> All</p>
<pre>show ipv6 neighbors vlan &lt;VLAN number&gt;</pre> <p>Displays IPv6 Neighbor Discovery cache entries on a single VLAN.  <b>Command mode:</b> All</p>
<pre>show ipv6 neighbors static</pre> <p>Displays static IPv6 Neighbor Discovery cache entries.  <b>Command mode:</b> All</p>
<pre>show ipv6 neighbors</pre> <p>Displays all IPv6 Neighbor Discovery cache entries. For more information, see <a href="#">page 79</a>.  <b>Command mode:</b> All</p>

## IPv6 Neighbor Discovery Cache Information

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

```
show ipv6 neighbors
```

**Command mode:** All

IPv6 Address	Age	Link-layer Addr	State	IF	VLAN	Port
2001:2:3:4::1	10	00:50:bf:b7:76:b0	Reachable	2	1	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 Equal Cost Multi-Path (ECMP) route information:

```
show ip ecmp
```

**Command mode:** All

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

ECMP 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 54. IGMP Multicast Group Information Commands

Command Syntax and Usage
<pre>show ip igmp querier vlan &lt;VLAN number&gt;</pre> <p>Displays IGMP Querier information. For details, see <a href="#">page 83</a>.</p> <p><b>Command mode:</b> All</p>
<pre>show ip igmp snoop</pre> <p>Displays IGMP Snooping information.</p> <p><b>Command mode:</b> All</p>
<pre>show ip igmp relay</pre> <p>Displays IGMP Relay information.</p> <p><b>Command mode:</b> All</p>
<pre>show ip igmp mrouter information</pre> <p>Displays IGMP Multicast Router information. For details, see <a href="#">page 83</a>.</p> <p><b>Command mode:</b> All</p>
<pre>show ip igmp mrouter vlan &lt;VLAN number&gt;</pre> <p>Displays IGMP Multicast Router information for the specified VLAN.</p> <p><b>Command mode:</b> All</p>
<pre>show ip igmp filtering</pre> <p>Displays current IGMP Filtering parameters.</p> <p><b>Command mode:</b> All</p>
<pre>show ip igmp profile &lt;1-16&gt;</pre> <p>Displays information about the current IGMP filter.</p> <p><b>Command mode:</b> All</p>
<pre>show ip igmp groups address &lt;IP address&gt;</pre> <p>Displays a single IGMP multicast group by its IP address.</p> <p><b>Command mode:</b> All</p>
<pre>show ip igmp groups vlan &lt;VLAN number&gt;</pre> <p>Displays all IGMP multicast groups on a single VLAN.</p> <p><b>Command mode:</b> All</p>
<pre>show ip igmp groups interface port &lt;port alias or number&gt;</pre> <p>Displays all IGMP multicast groups on a single port.</p> <p><b>Command mode:</b> All</p>
<pre>show ip igmp groups portchannel &lt;trunk number&gt;</pre> <p>Displays all IGMP multicast groups on a single trunk group.</p> <p><b>Command mode:</b> All</p>

Table 54. IGMP Multicast Group Information Commands (continued)

Command Syntax and Usage	
<pre>show ip igmp groups detail &lt;IP address&gt;</pre>	<p>Displays details about an IGMP multicast group, including source and timer information.</p> <p><b>Command mode:</b> All</p>
<pre>show ip igmp groups</pre>	<p>Displays information for all multicast groups. For details, see <a href="#">page 84</a>.</p> <p><b>Command mode:</b> All</p>
<pre>show ip igmp ipmcgrp</pre>	<p>Displays information for all IPMC groups. For details, see <a href="#">page 85</a>.</p> <p><b>Command mode:</b> All</p>
<pre>show ip igmp counters</pre>	<p>Displays IGMP counters for all VLANs.</p> <p><b>Command mode:</b> All</p>
<pre>show ip igmp vlan &lt;VLAN no.&gt; counter</pre>	<p>Displays IGMP counters for a specific VLAN.</p> <p><b>Command mode:</b> All</p>

## IGMP Querier Information

The following command displays IGMP Querier information:

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

**Command mode:** All

```
Current IGMP Querier information:
IGMP Querier information for vlan 1:
Other IGMP querier - none
Switch-querier enabled, current state: Querier
Switch-querier type: Ipv4, address 1.1.1.1,
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

```
Total entries: 5 Total IGMP groups: 3
Note: The <Total IGMP groups> number is computed as
      the number of unique (Group, Vlan) entries!
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

```
Total entries: 3 Total number of dynamic mroouters: 2
Total number of installed static mroouters: 1
```

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	-	-
*	9	24	V2	static		-	-

IGMP Mrouter information includes:

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

- Querier's Query Interval Code (QQIC)

## IPMC Group Information

The following command displays IGMP IPMC group information:

```
show ip igmp ipmcgrp
```

**Command mode:** All

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

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

IGMP IPMC Group information includes:

- IGMP source address
- IGMP group address
- VLAN and port
- Type of IPMC group
- Expiration timer value

## MLD information

[Table 55](#) describes the commands used to view MLD information.

*Table 55. MLD Information Commands*

Command Syntax and Usage
<pre>show ipv6 mld groups</pre> <p>Displays MLD multicast group information.</p> <p><b>Command mode:</b> All</p>
<pre>show ipv6 mld groups address &lt;IPv6 address&gt;</pre> <p>Displays group information for the specified IPv6 address.</p> <p><b>Command mode:</b> All</p>
<pre>show ipv6 mld groups interface port &lt;port number&gt;</pre> <p>Displays MLD groups on a single interface port.</p> <p><b>Command mode:</b> All</p>
<pre>show ipv6 mld groups portchannel &lt;trunk group number&gt;</pre> <p>Displays groups on a single port channel.</p> <p><b>Command mode:</b> All</p>
<pre>show ipv6 mld groups vlan &lt;vlan number&gt;</pre> <p>Displays groups on a single VLAN.</p> <p><b>Command mode:</b> All</p>
<pre>show ipv6 mld mrouter</pre> <p>Displays all MLD Mrouter ports. See <a href="#">page 87</a> for sample output.</p> <p><b>Command mode:</b> All</p>

## MLD Mrouter Information

The following command displays MLD Mrouter information:

```
show ipv6 mld mrouter
```

**Command mode:** All

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

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

*Table 56. MLD Mrouter*

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

## VRRP Information

Virtual Router Redundancy Protocol (VRRP) support on 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, renter, prio 100, master
 2: vrid 1, 205.178.18.202, if 1, renter, prio 100, backup
 3: vrid 3, 205.178.18.204, if 1, renter, 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.
  - `renter` 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)

**Note:** If routing is enabled using the “no switchport” command in Interface Port mode, this command also displays IP interfaces configured on physical ports as well as LACP and LAGs.

## IPv6 Interface Information

The following command displays IPv6 interface information:

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

**Command mode:** All

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

For each interface, the following information is displayed:

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

## IPv6 Path MTU Information

The following command displays IPv6 Path MTU information:

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

**Command mode:** All

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

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

## IP Information

The following command displays Layer 3 information:

```
show ip interface brief
```

**Command mode:** All

```
IP information:
Flood unregistered IPMC: ena

AS number 0

Interface information:
  1: IP4 192.168.1.253 255.255.255.0 192.168.1.255, vlan 100, up
 99: IP4 192.168.99.100 255.255.255.0 192.168.99.255, vlan 99, DOWN
127: IP4 172.25.101.222 255.255.0.0 172.25.255.255, vlan 4095, up

Loopback interface information:

Default gateway information: metric strict
  3: 172.25.1.1, up active

Default IP6 gateway information:

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

Current BOOTP relay option-82 settings: OFF
Current BOOTP relay option-82 policy: Replace

Current DHCP Snooping settings: Off
DHCP Snooping is configured on the following VLANs:
empty
Insertion of option 82 information is Disable
  Interface  Trusted  Rate limit (pps)
-----
           1      No      none
           2      No      none
...
           MGT     No      none

Current IP forwarding settings: ON, dirbr disabled, ICMPv6 redirect disabled

Current network filter settings:
none

Current route map settings:
RIP is disabled.

OSPF is disabled.

OSPFv3 is disabled.

BGP is disabled.
```

IP information includes:

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

## IKEv2 Information

The following table lists commands that display information about IKEv2.

Table 57. IKEv2 Information Commands

Command Syntax and Usage
<code>show ikev2</code> Displays all IKEv2 information. See <a href="#">page 94</a> for sample output. <b>Command mode:</b> All
<code>show ikev2 ca-cert</code> Displays the CA certificate. <b>Command mode:</b> All
<code>show ikev2 host-cert</code> Displays the host certificate. <b>Command mode:</b> All
<code>show ikev2 identity</code> Displays IKEv2 identity information. <b>Command mode:</b> All
<code>show ikev2 preshare-key</code> Displays the IKEv2 preshare key. <b>Command mode:</b> All
<code>show ikev2 proposal</code> Displays the IKEv2 proposal. <b>Command mode:</b> All
<code>show ikev2 retransmit-interval</code> Displays the IKEv2 retransmit interval. <b>Command mode:</b> All
<code>show ikev2 sa</code> Displays the IKEv2 SA. <b>Command mode:</b> All

## IKEv2 Information Dump

The following command displays IKEv2 information:

```
show ikev2
```

**Command mode:** All

```
IKEv2 retransmit time:      20

IKEv2 cookie notification:  disable

IKEv2 authentication method: Pre-shared key

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

Local preshare key:         ibm123

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

IKEv2 information includes:

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

## IP Security Information

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

Table 58. IPsec Information Commands

Command Syntax and Usage
<pre>show ipsec sa</pre> <p>Displays all security association information.</p> <p><b>Command mode:</b> All</p>
<pre>show ipsec spd</pre> <p>Displays all security policy information.</p> <p><b>Command mode:</b> All</p>
<pre>show ipsec dynamic-policy &lt;1-10&gt;</pre> <p>Displays dynamic policy information.</p> <p><b>Command mode:</b> All</p>
<pre>show ipsec manual-policy &lt;1-10&gt;</pre> <p>Displays manual policy information. See <a href="#">page 96</a> for sample output.</p> <p><b>Command mode:</b> All</p>
<pre>show ipsec transform-set &lt;1-10&gt;</pre> <p>Displays IPsec transform set information.</p> <p><b>Command mode:</b> All</p>
<pre>show ipsec traffic-selector &lt;1-10&gt;</pre> <p>Displays IPsec traffic selector information.</p> <p><b>Command mode:</b> All</p>
<pre>[no] debug sec all</pre> <p>Enables or disables all IP security debug messages.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>[no] debug sec crypto</pre> <p>Enables or disables cryptographic debug messages.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>[no] debug sec ike</pre> <p>Enables or disables IKEv2 debug messages.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>[no] debug sec ipsec</pre> <p>Enables or disables IPsec debug messages.</p> <p><b>Command mode:</b> Global configuration</p>

## IPsec Manual Policy Information

The following command displays IPsec manual key management policy information:

```
show ipsec manual-policy
```

**Command mode:** All

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

IPsec manual policy information includes:

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



## 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 59. PIM Information Options

Command Syntax and Usage
<pre>show ip pim bsr [&lt;component ID&gt;]</pre> <p>Displays information about the PIM bootstrap router (BSR).</p> <p><b>Command mode:</b> All</p>
<pre>show ip pim component [&lt;component ID (1-2)&gt;]</pre> <p>Displays PIM component information. For details, see <a href="#">page 99</a>.</p> <p><b>Command mode:</b> All</p>
<pre>show ip pim counters</pre> <p>Displays PIM statistics for all interfaces.</p> <p><b>Command mode:</b> All</p>
<pre>show ip pim interface [&lt;interface number&gt; detail loopback port &lt;port number&gt;]</pre> <p>Displays PIM interface information. To view sample output, see <a href="#">page 100</a>.</p> <p><b>Command mode:</b> All</p>
<pre>show ip pim neighbor [&lt;interface number&gt; port &lt;port number&gt;]</pre> <p>Displays PIM neighbor information. To view sample output, see <a href="#">page 100</a>.</p> <p><b>Command mode:</b> All</p>
<pre>show ip pim neighbor-filters</pre> <p>Displays information about PIM neighbor filters.</p> <p><b>Command mode:</b> All</p>
<pre>show ip pim mroute [&lt;component ID&gt; count flags  group &lt;multicast group address&gt;  interface {&lt;interface number&gt; port &lt;port number&gt;} source &lt;multicast source address&gt;]</pre> <p>Displays information about PIM multicast routes. For more information about displaying PIM multicast route information, see <a href="#">page 101</a>.</p> <p><b>Command mode:</b> All</p>
<pre>show ip pim rp-candidate [&lt;component ID&gt;]</pre> <p>Displays a list of the candidate Rendezvous Points configured.</p> <p><b>Command mode:</b> All</p>
<pre>show ip pim rp-set [&lt;RP IP address&gt;]</pre> <p>Displays a list of the Rendezvous Points learned.</p> <p><b>Command mode:</b> All</p>

Table 59. PIM Information Options (continued)

Command Syntax and Usage
<pre>show ip pim rp-static [&lt;component ID&gt;]</pre> <p>Displays a list of the static Rendezvous Points configured.</p> <p><b>Command mode:</b> All</p>
<pre>show ip pim elected-rp [group &lt;multicast group address&gt;]</pre> <p>Displays a list of the elected Rendezvous Points.</p> <p><b>Command mode:</b> All</p>

## PIM Component Information

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

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

**Command mode:** All

<pre>PIM Component Information ----- Component-Id: 1   PIM Mode: sparse,   PIM Version: 2   Elected BSR: 0.0.0.0   Candidate RP Holdtime: 0</pre>
---

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	2	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 60. PIM Multicast Route Information Options

Command Syntax and Usage
<pre>show ip pim mroute [&lt;component ID&gt;]</pre> <p>Displays PIM multicast routes for the selected component.</p> <p><b>Command mode:</b> All</p>
<pre>show ip pim mroute flags [s] [r] [w]</pre> <p>Displays PIM multicast routes based on the selected entry flags. Enter flags in any combination:</p> <ul style="list-style-type: none"> <li>– s: Shortest Path Tree (SPT) bit</li> <li>– r: Rendezvous Point Tree (RPT) bit</li> <li>– w: Wildcard bit</li> </ul> <p><b>Command mode:</b> All</p>
<pre>show ip pim mroute group &lt;multicast group IP address&gt;</pre> <p>Displays PIM multicast routes for the selected multicast group.</p> <p><b>Command mode:</b> All</p>
<pre>show ip pim mroute interface {&lt;interface number&gt; port &lt;port number&gt;}</pre> <p>Displays PIM multicast routes for the selected incoming IP interface.</p> <p><b>Command mode:</b> All</p>
<pre>show ip pim mroute source &lt;multicast source IP address&gt;</pre> <p>Displays PIM multicast routes for the selected source IP address.</p> <p><b>Command mode:</b> All</p>
<pre>show ip pim mroute count</pre> <p>Displays a count of PIM multicast routes of each type.</p> <p><b>Command mode:</b> All</p>
<pre>show ip pim mroute</pre> <p>Displays information about all PIM multicast routes.</p> <p><b>Command mode:</b> All</p>

## PIM Multicast Route Information

The following command displays PIM multicast route information:

```
show ip pim mroute
```

**Command mode:** All

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

## Quality of Service Information

Table 61. QoS information Options

Command Syntax and Usage
<pre>show qos transmit-queue</pre> <p>Displays mapping of 802.1p value to Class of Service queue number, and COS queue weight value.</p> <p><b>Command mode:</b> All</p>
<pre>show qos transmit-queue information</pre> <p>Displays all 802.1p information.</p> <p><b>Command mode:</b> All</p> <p>For details, see <a href="#">page 103</a>.</p>
<pre>show qos random-detect</pre> <p>Displays WRED and ECN information.</p> <p><b>Command mode:</b> All</p> <p>For details, see <a href="#">page 104</a>.</p>

## 802.1p Information

The following command displays 802.1p information:

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

**Command mode:** All

```

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

Current port priority information:
Port     Priority  COSq  Weight
-----  -
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 62. 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 63. 802.1p Port Priority Parameter Descriptions*

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

## WRED and ECN Information

The following command displays WRED and ECN information:

```
show qos random-detect
```

**Command mode:** All

Current wred and ecn configuration:							
Global ECN: Disable							
Global WRED: Disable							
--WRED--TcpMinThr--TcpMaxThr--TcpDrate--NonTcpMinThr--NonTcpMaxThr--NonTcpDrate--							
0	TQ0:	Dis	0	0	0	0	0
0	TQ1:	Dis	0	0	0	0	0
0	TQ2:	Dis	0	0	0	0	0
0	TQ3:	Dis	0	0	0	0	0
0	TQ4:	Dis	0	0	0	0	0
0	TQ5:	Dis	0	0	0	0	0
0	TQ6:	Dis	0	0	0	0	0
0	TQ7:	Dis	0	0	0	0	0

## Access Control List Information Commands

Table 64. ACL Information Options

<b>Command Syntax and Usage</b>
<pre>show access-control list &lt;ACL number&gt;</pre> <p>Displays ACL list information. For details, see <a href="#">page 105</a>.</p> <p><b>Command mode:</b> All</p>
<pre>show access-control list6 &lt;ACL number&gt;</pre> <p>Displays IPv6 ACL list information.</p> <p><b>Command mode:</b> All</p>
<pre>show access-control group &lt;ACL group number&gt;</pre> <p>Displays ACL group information.</p> <p><b>Command mode:</b> All</p>
<pre>show access-control vmap &lt;VMAP number&gt;</pre> <p>Displays VMAP information.</p> <p><b>Command mode:</b> All</p>



## Access Control List Information

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

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

**Command mode:** All

```
Current ACL 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
```

If the ACL is being used with Policy-Based Routing (PBR), the output from this command is more like the following:

```
Filter 1 profile: route-map 16
IPv4
  - Protocol   : 17
  Actions      : Permit
               : dscp 22
  Statistics   : enabled
  Installed on Port 16
```

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

*Table 65. 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.

Table 65. ACL List Parameter Descriptions

Parameter	Description
Meter	Displays the ACL meter parameters.
Re-Mark	Displays the ACL re-mark parameters.
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.
Filter x profile	Indicates the ACL number.

---

## OpenFlow Information

The following commands display OpenFlow information.

Table 66. OpenFlow Information Options

Command Syntax and Usage
<pre>show openflow [flow-allocation   information   statistics   table]</pre> <p>Displays the current OpenFlow configuration. For more information, see <a href="#">page 107</a>.</p> <ul style="list-style-type: none"><li>– <code>flow-allocation</code> displays the configured, current and maximum number of flows for each OpenFlow instance. For more information, see <a href="#">page 108</a>.</li><li>– <code>information</code> displays the configuration for each OpenFlow instance. For more information, see <a href="#">page 110</a>.</li><li>– <code>statistics</code> displays traffic statistics for each OpenFlow instance. For more information see <a href="#">page 208</a>.</li><li>– <code>table</code> displays the basic and emergency flow tables for each OpenFlow instance. For more information, see <a href="#">page 112</a></li></ul> <p><b>Command mode:</b> All</p>
<pre>show openflow instance &lt;1-2&gt; [information   statistics   table]</pre> <p>Displays OpenFlow information for the specified instance ID:</p> <ul style="list-style-type: none"><li>– <code>information</code> displays the instance configuration</li><li>– <code>statistics</code> displays traffic statistics</li><li>– <code>table</code> displays the basic and emergency flow tables</li></ul> <p><b>Command mode:</b> All</p>

## OpenFlow Global Configuration Information

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

```
show openflow
```

**Command mode:** All

### In OpenFlow 1.0:

```
Protocol Version: 1.0
Openflow State: Enabled
FDB Table Priority: 1000
FDB Table FDB-timeout: Disabled

Openflow instance 1 is currently disabled

Openflow Instance ID: 2
  state: enabled , buffering: disabled
  retry 4, emergency time-out 30
  echo req interval 30, echo reply time-out 15
  min-flow-timeout : use controller provided values.
  max flows acl      : Maximum Available
  max flows unicast fdb : Maximum Available
  max flows multicast fdb : Maximum Available
  emergency feature: disabled
  dpid: 0x0002749975ab5c00
  ports : 18-19,24,35-38
  Controller Id: 1
    Active Controller
    IP Address: 9.70.31.71, port: 6633, Mgt-Port

Openflow Edge ports : None
```

### In OpenFlow 1.3:

```
Protocol Version: 1.3.1
Openflow State: Enabled
FDB Table Priority: 1000
MPLS Table Priority: 65535
FDB Table FDB-timeout: Disabled

Openflow instance 1 is currently disabled

Openflow Instance ID: 2
  state: enabled , buffering: disabled , table-miss: drop
  echo req interval 30, echo reply time-out 15, retry 4
  min-flow-timeout : use controller provided values.
  max flows acl      : Maximum Available
  max flows unicast fdb : Maximum Available
  max flows multicast fdb : Maximum Available
  max flows mpls push : Maximum Available
  max flows mpls pop : Maximum Available
  dpid: 0x0002749975ab5c00
  table-miss cookie: 0xffffffffffffffff
  mirror-to-controller cookie: 0xffffffffffffffff
  send-to-controller cookie: 0xffffffffffffffff
  ports : 18-19,24,35-38
  portchannel: 10
  Controller Id: 1
    Active Controller
    IP Address: 9.70.31.71, port: 6633, Mgt-Port

Openflow Edge ports : None
```

## OpenFlow Flow Allocation Information

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

```
show openflow flow-allocation
```

**Comand mode:** All

OpenFlow 1.0:

```
Flow Allocation Information

Instance 1

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

Basic Entries

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

Emergency Entries

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

Maximum Current Availability

Maximum Available ACL Count        : 747
Maximum Available Unicast FDB Count : 123904
Maximum Available Multicast FDB Count: 4096

Instance 2
...
```

## In OpenFlow 1.3:

```
Flow Allocation Information

Instance 1

Maximum ACL Count Configured           : Maximum Available
Maximum Unicast FDB Count Configured   : Maximum Available
Maximum Multicast FDB Count Configured : Maximum Available
Maximum MPLS PUSH Count Configured     : Maximum Available
Maximum MPLS POP Count Configured      : Maximum Available

Basic Entries

Current ACL Count                       : 0
Current Unicast FDB Count                : 0
Current Multicast FDB Count              : 0
Current MPLS PUSH Count                  : 0
Current MPLS POP Count                    : 0

Static Entries

Current static ACL Count                  : 0
Current static Unicast FDB Count          : 0
Current static Multicast FDB Count        : 0
Current static MPLS PUSH Count            : 0
Current static MPLS POP Count             : 0

Maximum Current Availability

Maximum Available ACL Count               : 747
Maximum Available Unicast FDB Count       : 123904
Maximum Available Multicast FDB Count     : 4096
Maximum Available MPLS PUSH Count         : 1000
Maximum Available MPLS POP Count          : 1000

Instance 2
...
```

## OpenFlow Configuration Information

The following command displays the OpenFlow configuration for all instances:

```
show openflow information
```

**Command mode:** All

## In OpenFlow 1.0:

```
Openflow feature is Enabled
-----

Openflow instance 1 is currently disabled
-----

Openflow Instance ID: 2
  State : Enabled
  DataPath ID: 0x0002749975ab5c00
  Max Retries per controller: 4
  Echo Request Interval: 30
  Echo Reply Timeout: 15
  Emergency Timeout: 30
  Min-flow-timeout : 0, use controller provided values.
  Max ACL Flows: Maximum Available
  Max Unicast FDB Flows: Maximum Available
  Max Multicast FDB Flows: Maximum Available
  Buffering: Disabled
  Operational Mode: Normal
  Miss Send Len: 65535

Port Alias  Status State      Config   Current   Advertised Supported Peer
18 18      e  0x200    0x2      0xc0     0x0      0x0      0x0
19 19      e  0x200    0x2      0xc0     0x0      0x0      0x0
24 24      d  0x201    0x2      0xc0     0x0      0x0      0x0
35 35      d  0x201    0x2      0x0      0x0      0x0      0x0
36 36      d  0x201    0x2      0x0      0x0      0x0      0x0
37 37      d  0x201    0x2      0x0      0x0      0x0      0x0
38 38      d  0x201    0x2      0x0      0x0      0x0      0x0

Number of Ports: 7
Configured Controllers:
  Openflow Controller 1:
    IP Address: 9.70.31.71
    Port: 6633
    State: Active
    Retry Count: 0
```

## In OpenFlow 1.3:

```
Openflow feature is Enabled
-----

Openflow instance 1 is currently disabled
-----

Openflow Instance ID: 2
  State : Enabled
  DataPathID: 0x0002749975ab5c00
  Table-miss cookie: 0xffffffffffffffff
  Mirror-to-controller cookie: 0xffffffffffffffff
  Send-to-controller cookie: 0xffffffffffffffff
  Max Retries per controller: 4
  Echo Request Interval: 30
  Echo Reply Timeout: 15
  Min-flow-timeout : 0, use controller provided values.
  Max ACL Flows: Maximum Available
  Max Unicast FDB Flows: Maximum Available
  Max Multicast FDB Flows: Maximum Available
  Max MPLS Push Flows: Maximum Available
  Max MPLS Pop Flows: Maximum Available
  Buffering: Disabled
  Table Miss: Drop
  Operational Mode: Normal
  Miss Send Len: 65535

Port  Alias  Status State    Config    Current    Advertised Supported Peer
18    18      e    0x0    0x0      0x840     0x0       0x0       0x0
19    19      e    0x0    0x0      0x840     0x0       0x0       0x0
24    24      d    0x1    0x0      0x840     0x0       0x0       0x0
35    35      d    0x1    0x0      0x0       0x0       0x0       0x0
36    36      d    0x1    0x0      0x0       0x0       0x0       0x0
37    37      d    0x1    0x0      0x0       0x0       0x0       0x0
38    38      d    0x1    0x0      0x0       0x0       0x0       0x0
10010 PCH10   d    0x1    0x0      0x400     0x0       0x0       0x0

Number of Ports: 7
Number of Portchannels: 1

Configured Controllers:
  Openflow Controller 1:
    IP Address: 9.70.31.71
    Port: 6633
    State: Active
```

## OpenFlow Table Information

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

```
show openflow table
```

**Command mode:** All



## OpenFlow 1.0:

```
Openflow instance 1 is currently disabled

Openflow Instance Id: 2

BASIC FLOW TABLE

CONTROLLER ADDED FLOWS

Flow:1
  Filter Based, priority:    0, hard-time-out:    0, idle-time-out:    0
  cookie: 0x0
  QUALIFIERS:
  ACTION: drop
  STATS:  packets=0, bytes=0

Flow:2
  Filter Based, priority:65535, hard-time-out:    0, idle-time-out:    0
  cookie: 0x0
  QUALIFIERS: ether-type:0x88cc
               protocol: 0, tos: 0
               src-ip:0.0.0.0/32, dst-ip:0.0.0.0/32
               src-port: 0, dst-port: 0
  ACTION: output:CONTROLLER [Max Len: 65535 / - bytes (C/S)]
  STATS:  packets=0, bytes=0

Flow:3
  Filter Based, priority:    2, hard-time-out:    0, idle-time-out:    0
  cookie: 0x0
  QUALIFIERS:
  ACTION: output:CONTROLLER [Max Len: 65535 / - bytes (C/S)]
  STATS:  packets=0, bytes=0
```

### In OpenFlow 1.3:

```
Openflow instance 1 is currently disabled

Openflow Instance Id: 2

CONTROLLER added FLOWS

Flow 1, Filter Based, priority:2, hard-time-out:0, idle-time-out:0
  cookie:0x0
  QUALIFIERS:
  Instruction: apply_action
  ACTION: output:CONTROLLER [Max Len: 65535 / - bytes (C/S)]
  STATS: packets=0, bytes=0

Flow 2, Filter Based, priority:65535, hard-time-out:0, idle-time-out:0
  cookie:0x0
  QUALIFIERS: eth-type:0x88cc
  Instruction: apply_action
  ACTION: output:CONTROLLER [Max Len: 65535 / - bytes (C/S)]
  STATS: packets=0, bytes=0

Flow 3, Filter Based, priority:0, hard-time-out:0, idle-time-out:0
  cookie:0x0
  QUALIFIERS:
  Instruction: empty
  ACTION: drop
  STATS: packets=0, bytes=0
```

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

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

---

## RMON Information Commands

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

Table 67. RMON Information Options

Command Syntax and Usage
<pre>show rmon history</pre> <p>Displays RMON History information. For details, see <a href="#">page 116</a>.</p> <p><b>Command mode:</b> All</p>
<pre>show rmon alarm</pre> <p>Displays RMON Alarm information. For details, see <a href="#">page 117</a>.</p> <p><b>Command mode:</b> All</p>

Table 67. RMON Information Options

Command Syntax and Usage
<pre>show rmon event</pre> <p>Displays RMON Event information. For details, see <a href="#">page 118</a>.</p> <p><b>Command mode:</b> All</p>
<pre>show rmon</pre> <p>Displays all RMON information.</p> <p><b>Command mode:</b> All</p>

## 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 68. 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 69. 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"> <li>- <code>abs</code>—absolute value, the value of the selected variable is compared directly with the thresholds at the end of the sampling interval.</li> <li>- <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.</li> </ul>
Type	Displays the type of alarm, as follows: <ul style="list-style-type: none"> <li>- <code>falling</code>—alarm is triggered when a falling threshold is crossed.</li> <li>- <code>rising</code>—alarm is triggered when a rising threshold is crossed.</li> <li>- <code>either</code>—alarm is triggered when either a rising or falling threshold is crossed.</li> </ul>
rLimit	Displays the rising threshold for the sampled statistic.
fLimit	Displays the falling threshold for the sampled statistic.
Last value	Displays the last sampled value.

Table 69. RMON Alarm Parameter Descriptions (continued)

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

## RMON Event Information

The following command displays RMON event 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 70. 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	10000	full	yes	yes	up
2	2	10000	full	yes	yes	up
3	3	10000	full	yes	yes	up
4	4	10000	full	yes	yes	up
5	5	10000	full	yes	yes	down
6	6	10000	full	yes	yes	up
...						
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	DESCRIPTION	VLAN(s)
-----	----	---	-----	---	---	-----	-----	-----
		Trk				NVLAN		
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
...								
MGT	65	n	d	e	e	4095		4095

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

Port information includes:

- Port alias and number
- Whether the port uses VLAN tagging or not (y or n)
- Whether the port has Remote Monitoring (RMON) enabled
- Whether the port has FDB learning enabled (Lrn)
- Whether the port has Port Flooding enabled (Fld)
- Port VLAN ID (PVID)

- Port description
- VLAN membership



## Port Transceiver Status

The following command displays the status of the transceiver module on each 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	Onm	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	Onm	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	Onm	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	Onm	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	Onm	Accepted
Blade-Network			Part:BN-CKM-QP-SR4			Date:101102	S/N:BNNTS10440U			
9 QSFP+ 3	Ena	LINK	no	0.00	1.5	N/A	N/A	SR QSFP	Onm	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	Onm	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	Onm	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	Onm	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	Onm	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 nanometers
- Approval status

## Virtual Machines Information

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

Table 71. Virtual Machines Information Options

Command Syntax and Usage
<pre>show virt port &lt;port alias or number&gt;</pre> <p>Displays Virtual Machine information for the selected port.</p> <p><b>Command mode:</b> All</p>
<pre>show virt vm</pre> <p>Displays all Virtual Machine information.</p> <p><b>Command mode:</b> All</p>

## VM Information

The following command displays VM information:

```
show virt vm
```

**Command mode:** All

IP Address	VMAC Address	Index	Port	VM Group (Profile)
*127.31.46.50	00:50:56:4e:62:f5	4	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)

## VM Check Information

The following command displays VM Check information:

```
show virt vmcheck
```

**Command mode:** All

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

## VMware Information

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

Table 72. VMware Information Options

Command Syntax and Usage
<pre>show virt vmware hosts</pre> <p>Displays a list of VMware hosts.</p> <p><b>Command mode:</b> All</p>
<pre>show virt vmware showhost &lt;host UUID&gt;   &lt;host IP address&gt;   &lt;host name&gt;</pre> <p>Displays detailed information about a specific VMware host.</p> <p><b>Command mode:</b> All</p>
<pre>show virt vmware showvm &lt;VM UUID&gt;   &lt;VM IP address&gt;   &lt;VM name&gt;</pre> <p>Displays detailed information about a specific Virtual Machine (VM).</p> <p><b>Command mode:</b> All</p>
<pre>show virt vmware vms</pre> <p>Displays a the names of all VMware VMs.</p> <p><b>Command mode:</b> All</p>

## VMware Host Information

The following command displays VM host information:

```
show virt vmware hosts
```

**Command mode: All**

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

VM host information includes the following:

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

---

## vNIC Information

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

Table 73. vNIC Information Options

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

## 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)

---

## EVB Information

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

Table 74. EVB Information Options

Command Syntax and Usage
<pre>show virt evb vdp vm</pre> <p>Displays all active Virtual Machines (VMs).</p> <p><b>Command mode:</b> All</p>
<pre>show virt evb vdp tlv</pre> <p>Displays all active Virtual Station Interface (VSI) Discovery and Configuration Protocol (VDP) type-length-values (TLVs).</p> <p><b>Command mode:</b> All</p>
<pre>show virt evb vsidb &lt;VSI_database_number&gt;</pre> <p>Displays Virtual Station Interface database information.</p> <p><b>Command mode:</b> All</p>



---

## Converged Enhanced Ethernet Information

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

*Table 75. CEE Information Options*

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

## DCBX Information

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

*Table 76. DCBX Information Options*

Command Syntax and Usage
<pre>show cee information dcbx port &lt;port alias or number&gt; control</pre> <p>Displays information about the DCBX Control state machine for the specified port or range of ports. For details, see <a href="#">page 130</a>.</p> <p><b>Command mode:</b> All</p>
<pre>show cee information dcbx port &lt;port alias or number&gt; feature</pre> <p>Displays information about the DCBX Feature state machine for the specified port or range of ports. For details, see <a href="#">page 131</a>.</p> <p><b>Command mode:</b> All</p>
<pre>show cee information dcbx port &lt;port alias or number&gt; ets</pre> <p>Displays information about the DCBX ETS state machine for the specified port or range of ports. For details, see <a href="#">page 132</a>.</p> <p><b>Command mode:</b> All</p>
<pre>show cee information dcbx port &lt;port alias or number&gt; pfc</pre> <p>Displays information about the DCBX PFC state machine for the specified port or range of ports. For details, see <a href="#">page 133</a>.</p> <p><b>Command mode:</b> All</p>
<pre>show cee information dcbx port &lt;port alias or number&gt; app_proto</pre> <p>Displays information about the DCBX Application Protocol state machine on the specified port or range of ports. For details, see <a href="#">page 134</a>.</p> <p><b>Command mode:</b> All</p>
<pre>show cee information dcbx port &lt;port alias or number&gt;</pre> <p>Displays all DCBX information for the specified port or range of ports.</p> <p><b>Command mode:</b> All</p>

## DCBX Control Information

The following command displays DCBX Control information:

```
show cee information dcbx port <port range> 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, number, or range> 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 77. DCBX Feature Information Fields*

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

## DCBX ETS Information

The following command displays DCBX ETS information:

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

**Command mode:** All

```

DCBX Port Priority Group - Priority Allocation Table
=====
Alias Port Priority PgIdDes PgIdOper PgIdPeer
-----
  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 78. DCBX Feature Information Fields*

Parameter	Description
<b>DCBX Port Priority Group - Priority Allocation Table</b>	
Alias	Displays each port's alias
Port	Displays each port's number
Priority	Displays each port's priority
PgIdDes	Priority Group ID configured on this switch
PgIdOper	Priority Group negotiated with the peer (operating Priority Group).
PgIdPeer	Priority Group ID configured on the peer

Table 78. DCBX Feature Information Fields (continued)

Parameter	Description
<b>DCBX Port Priority Group - Bandwidth Allocation Table</b>	
Alias	Displays each port's alias
Port	Displays each port's number
PrioGrp	Displays each port's priority group
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 79. DCBX Application Protocol Information Fields

Parameter	Description
Protocol ID	Identifies the supported Application Protocol.
Selector Field	Specifies the Application Protocol type, as follows: <ul style="list-style-type: none"><li>• 0 = Ethernet Type</li><li>• 1 = TCP socket ID</li></ul>
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 80 describes the Enhanced Transmission Selection (ETS) information options

Table 80. ETS Information Options

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

The following command displays ETS information:

```
show cee global ets information
```

**Command mode:** All

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

Enhanced Transmission Selection (ETS) information includes the following:

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



## PFC Information

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

Table 81. PFC Information Options

Command Syntax and Usage
<pre>show cee port &lt;port number or range of ports&gt; pfc</pre> <p>Displays PFC information. <b>Command mode:</b> All</p>
<pre>show cee port &lt;port number or range of ports&gt; pfc priority &lt;0-7&gt;</pre> <p>Displays PFC information. <b>Command mode:</b> All</p>
<pre>show cee port &lt;port number or range of ports&gt; pfc information</pre> <p>Displays PFC information. <b>Command mode:</b> All</p>

The following command displays PFC information:

```
show cee port <port number or range of ports> pfc information
```

**Command mode:** All

PFC information for Port 1:		
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 82](#) describes the Fibre Channel over Ethernet (FCoE) information options.

*Table 82. FCoE Information Options*

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

## FIP Snooping Information

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

*Table 83. FIP Snooping Information Options*

Command Syntax and Usage
<pre>show fcoe fips port &lt;port alias, number, or range&gt; information</pre> <p>Displays FIP Snooping (FIPS) information for the specified port or ports, including a list of current FIPS ACLs.</p> <p><b>Command mode:</b> All</p>
<pre>show fcoe fips fcf</pre> <p>Displays FCF learned (detected).</p> <p><b>Command mode:</b> All</p>
<pre>show fcoe fips fcoe</pre> <p>Displays FCoE connections learned (detected).</p> <p><b>Command mode:</b> All</p>
<pre>show fcoe fips information</pre> <p>Displays FIP Snooping information for all ports.</p> <p><b>Command mode:</b> All</p>
<pre>show fcoe fips vlan</pre> <p>Displays VLAN information.</p> <p><b>Command mode:</b> All</p>

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

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

**Command mode:** All

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

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

```
show fcoe fips port information
```

**Command mode:** All

FCF MAC	Port	Vlan		
00:05:73:ce:96:67	46	1002		
VN_PORT MAC	FCF MAC	Port	Vlan	
0e:fc:00:44:04:03	00:05:73:ce:96:67	18	1002	
0e:fc:00:44:04:02	00:05:73:ce:96:67	19	1002	
0e:fc:00:44:04:04	00:05:73:ce:96:67	21	1002	

```
FIP Snooping on port 1:
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 00:05:73:ce:96:67, action deny.
DMAC 00:05:73:ce:96:67, ethertype 0x8914, action permit.
DMAC 01:10:18:01:00:01, Ethertype 0x8914, action permit.
DMAC 01:10:18:01:00:02, Ethertype 0x8914, action permit.
Ethertype 0x8914, action deny.
Ethertype 0x8906, action deny.
SMAC 0e:fc:00:00:00:00, SMAC mask ff:ff:ff:00:00:00, action deny.
```

FIP Snooping port information includes the following:

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

## Fibre Channel over Ethernet Forwarder Information

The following command shows FCoE forwarder (FCF) information that has been learned (detected) by the switch:

```
show fcoe fips fcf
```

**Command mode:** All

Total number of FCFs detected: 0
----------------------------------

**Command mode:** All

---

## 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.

---

## Python Scripting Information

The following commands display Python Scripting Information.

Table 84. Python Scripting Information Commands

Command Syntax and Usage
<pre>show script</pre> <p>Displays a list of all installed scripts.</p> <p><b>Command mode:</b> All</p>
<pre>show script &lt;script filename&gt;</pre> <p>Displays the content of a specified script.</p> <p><b>Command mode:</b> All</p>
<pre>show script-log</pre> <p>Displays a list of all script log files.</p> <p><b>Command mode:</b> All</p>
<pre>show script-log &lt;script log filename&gt;</pre> <p>Displays the content of a specified script-log.</p> <p><b>Command mode:</b> All</p>
<pre>show scheduler job</pre> <p>Displays detailed information of all currently scheduled jobs. For more information, see <a href="#">page 143</a>.</p> <p><b>Command mode:</b> All</p>
<pre>show scheduler job name &lt;job name&gt;</pre> <p>Displays detailed information of a specified scheduled job.</p> <p><b>Command mode:</b> All</p>
<pre>show scheduler job running</pre> <p>Displays detailed information of all currently running jobs.</p> <p><b>Command mode:</b> All</p>
<pre>show scheduler job cpu-limit</pre> <p>Displays configured CPU usage limit value.</p> <p><b>Command mode:</b> All</p>
<pre>show scheduler job time-limit</pre> <p>Displays configured elapsed time limit value.</p> <p><b>Command mode:</b> All</p>

## Scheduler Job Information

The following command displays detailed information of all current scheduled jobs:

```
show scheduler job
```

**Command mode:** All

```

Job name: "auto_image_upgrade"
  timeevent: absolutestarttime: 2013/11/2014:30:0, interval: 43200
seconds
  action: "auto_image_upgrade.py" "10.20.8.8 group1"
-----
--
-----
--
Job name: "auto_image_upgrade"
State: idle
Previous process id: 0
Next execution time: 14:30:04 Thu Nov 21, 2013
Previous execution time: 02:30:00 Thu Nov 21, 2013
Previous user msec: 255
Previous sys msec: 16
Previous cpu usage: 7.59 (%)
Execution count: 1
-----
--
-----
--
Job name: "monitor"
  syslog event: LINKUP
  action: "exe_ping.py"
-----
--
-----
--
Job name: "monitor"
State: idle
Previous process id: 0
Next execution time: NA
Previous execution time: Yet to be executed or completed
Previous user msec: 0
Previous sys msec: 0
Previous cpu usage: 0.0 (%)
Execution count: 0

```

The following table describes the Scheduler Job information.

*Table 85. Scheduler Job Information Fields*

Parameter	Description
Job name	The name of the displayed scheduler job
State	Current scheduler job state (Idle/Running/Matched)
Matched state	The event was raised but a different job is already running, thus the event is put into the event queue.
Previous process id	The internal process ID of the thread that previously run the job

Table 85. Scheduler Job Information Fields

<b>Parameter</b>	<b>Description</b>
Next execution time	The timestamp when the job is scheduled to run
Previous execution time	The timestamp when the job was last executed
Previous user msec	The CPU time consumed by user owned threads on the previous job execution
Previous sys msec	The CPU time consumed by system owned threads on the previous job execution
Previous cpu usage	The CPU percentage consumed by Python Scripting process on the previous job execution
Execution count	The number of times the job was executed



## 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 86. Statistics Commands

Command Syntax and Usage
<pre>show layer3 counters</pre> <p>Displays Layer 3 statistics.</p> <p><b>Command mode:</b> All</p>
<pre>show snmp-server counters</pre> <p><b>Command mode:</b> All</p> <p>Displays SNMP statistics. See <a href="#">page 238</a> for sample output.</p>
<pre>show ntp counters</pre> <p>Displays Network Time Protocol (NTP) Statistics.</p> <p><b>Command mode:</b> All</p> <p>See <a href="#">page 242</a> for a sample output and a description of NTP Statistics.</p>
<pre>show ptp counters</pre> <p>Displays Precision Time Protocol Statistics.</p> <p><b>Command mode:</b> All</p> <p>See <a href="#">page 244</a> for a sample output and a description of PTP Statistics.</p>
<pre>clear mp-counters</pre> <p>Clears all MP-related statistics.</p> <p><b>Command mode:</b> Privileged EXEC</p>
<pre>clear cpu</pre> <p>Clears all CPU utilization statistics.</p> <p><b>Command mode:</b> Privileged EXEC</p>
<pre>clear interface port &lt;port number&gt; counters</pre> <p>Clears all statistics for the specified port.</p> <p><b>Command mode:</b> All</p>
<pre>show counters</pre> <p>Dumps all switch statistics. Use this command to gather data for tuning and debugging switch performance. If you want to capture dump data to a file, set your communication software on your workstation to capture session data prior to issuing the dump command.</p> <p><b>Command mode:</b> All</p> <p>For details, see <a href="#">page 245</a>.</p>

---

## Port Statistics

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

Table 87. Port Statistics Commands

Command Syntax and Usage
<pre>show interface port &lt;port alias or number&gt; dot1x counters</pre> <p>Displays IEEE 802.1X statistics for the port. See <a href="#">page 149</a> for sample output.</p> <p><b>Command mode:</b> All</p>
<pre>show ip bootp-relay counters interface &lt;port alias or number&gt;</pre> <p>Displays BOOTP relay statistics for the port.</p> <p><b>Command mode:</b> All</p> <p>See <a href="#">page 152</a> for sample output.</p>
<pre>show interface port &lt;port alias or number&gt; bitrate-usage</pre> <p>Displays the traffic rate in kilobits per second.</p> <p><b>Command mode:</b> All</p>
<pre>show interface port &lt;port alias or number&gt; bridging-counters</pre> <p>Displays bridging (“dot1”) statistics for the port.</p> <p><b>Command mode:</b> All</p> <p>See <a href="#">page 153</a> for sample output.</p>
<pre>show interface port &lt;port alias or number&gt; bridging-rate</pre> <p>Displays per-second bridging (“dot1”) statistics for the port.</p> <p><b>Command mode:</b> All</p>
<pre>show interface port &lt;port alias or number&gt; ethernet-counters</pre> <p>Displays Ethernet (“dot3”) statistics for the port.</p> <p><b>Command mode:</b> All</p> <p>See <a href="#">page 154</a> for sample output.</p>
<pre>show interface port &lt;port alias or number&gt; ethernet-rate</pre> <p>Displays per-second Ethernet (“dot3”) statistics for the port.</p> <p><b>Command mode:</b> All</p>
<pre>show interface port &lt;port alias or number&gt; interface-counters</pre> <p>Displays interface statistics for the port. See <a href="#">page 157</a> for sample output.</p> <p><b>Command mode:</b> All</p>
<pre>show interface port &lt;port alias or number&gt; interface-rate</pre> <p>Displays per-second interface statistics for the port.</p> <p><b>Command mode:</b> All</p>

Table 87. Port Statistics Commands (continued)

Command Syntax and Usage
<p>show interface port <i>&lt;port alias or number&gt;</i> ip-counters</p> <p>Displays IP statistics for the port. See <a href="#">page 160</a> for sample output.</p> <p><b>Command mode:</b> All</p>
<p>show interface port <i>&lt;port alias or number&gt;</i> ip-rate</p> <p>Displays per-second IP statistics for the port.</p> <p><b>Command mode:</b> All</p>
<p>show interface port <i>&lt;port alias or number&gt;</i> link-counters</p> <p>Displays link statistics for the port. See <a href="#">page 160</a> for sample output.</p> <p><b>Command mode:</b> All</p>
<p>show interface port <i>&lt;port alias or number&gt;</i> rmon-counters</p> <p>Displays Remote Monitoring (RMON) statistics for the port. See <a href="#">page 161</a> for sample output.</p> <p><b>Command mode:</b> All</p>
<p>show interface port <i>&lt;port alias or number&gt;</i> oam counters</p> <p>Displays Operation, Administrative, and Maintenance (OAM) protocol statistics for the port.</p> <p><b>Command mode:</b> All</p>
<p>show interface port <i>&lt;port aliases or numbers&gt;</i> egress-queue-counters [<i>&lt;queue_no&gt;</i>   drop]</p> <p>Displays the total number of packets and bytes either successfully transmitted or dropped for each queue of the specified ports.</p> <ul style="list-style-type: none"> <li>– <i>queue_no</i> filters the output to the specified queue number</li> <li>– <i>drop</i> lists only the queues with dropped traffic (non-zero counters for dropped packets/bytes counters)</li> </ul> <p>See <a href="#">page 164</a> for sample output.</p> <p><b>Command mode:</b> All</p>
<p>show interface port <i>&lt;port aliases or numbers&gt;</i> egress-queue-rate [<i>&lt;queue_no&gt;</i>   drop]</p> <p>Displays the number of packets and bytes per second either successfully transmitted or dropped for each queue of the specified ports.</p> <ul style="list-style-type: none"> <li>– <i>queue_no</i> filters the output to the specified queue number</li> <li>– <i>drop</i> lists only the queues with dropped traffic (non-zero rates for dropped packets/bytes)</li> </ul> <p>See <a href="#">page 165</a> for sample output.</p> <p><b>Command mode:</b> All</p>
<p>clear interface port <i>&lt;port aliases or numbers&gt;</i> egress-queue-counter</p> <p>Clears all QoS egress counters for the specified ports for all queues.</p> <p><b>Command mode:</b> Privileged EXEC</p>

Table 87. Port Statistics Commands (continued)

Command Syntax and Usage
<pre>show interface port &lt;port alias or number&gt; ptp-counters</pre> <p>Displays Precision Time Protocol statistics for the port. See <a href="#">page 244</a> for a sample output and a description of PTP Statistics.</p> <p><b>Command mode:</b> All</p>
<pre>clear interfaces</pre> <p>Clears counters for all interfaces and queues.</p> <p><b>Command mode:</b> Privileged EXEC</p>
<pre>clear interface port &lt;port alias or number&gt; counters</pre> <p>Clears all statistics for the port.</p> <p><b>Command mode:</b> Privileged EXEC</p>
<pre>clear counters</pre> <p>Clears statistics for all ports.</p> <p><b>Command mode:</b> Privileged EXEC</p>

## 802.1X Authenticator Statistics

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

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

**Command mode:** All

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

*Table 88. 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 89. 802.1X Authenticator Diagnostics of a Port

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

Table 89. 802.1X Authenticator Diagnostics of a Port (continued)

Statistics	Description
authFailWhileAuthenticating	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.
authReauthsWhileAuthenticating	Total number of times that the state machine transitions from AUTHENTICATING to ABORTING, as a result of a re-authentication request
authEapStartsWhileAuthenticating	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.
authEapLogoffWhileAuthenticating	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.
authReauthsWhileAuthenticated	Total number of times that the state machine transitions from AUTHENTICATED to CONNECTING, as a result of a re-authentication request.
authEapStartsWhileAuthenticated	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.
authEapLogoffWhileAuthenticated	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 89. 802.1X Authenticator Diagnostics of a Port (continued)

Statistics	Description
backendOtherRequestsToSupplicant	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.
backendNonNakResponsesFromSupplicant	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.

## BootStrap Protocol Relay Statistics

Use the following command to display the BOOTP Relay statistics of the selected port:

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

**Command mode:** All

```

-----
BOOTP Relay statistics for port 1:

Requests received from client:      0
Requests relayed to server:        0
Requests relayed with option 82:   0
Requests dropped due to ...
  - relay not allowed:              0
  - no server or unreachable server: 0
  - packet or processing errors:    0
Replies received from server:      0
Replies relayed to client:         0
Replies dropped due to ...
  - packet or processing errors:    0

```



## 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 90. Bridging Statistics of a Port*

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

## Ethernet Statistics

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

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

**Command mode:** All

Ethernet statistics for port 1:	
dot3StatsAlignmentErrors:	0
dot3StatsFCSErrors:	0
dot3StatsSingleCollisionFrames:	0
dot3StatsMultipleCollisionFrames:	0
dot3StatsLateCollisions:	0
dot3StatsExcessiveCollisions:	0
dot3StatsInternalMacTransmitErrors:	NA
dot3StatsFrameTooLongs:	0
dot3StatsInternalMacReceiveErrors:	0

*Table 91. 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 91. Ethernet Statistics of a Port (continued)

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

Table 91. Ethernet Statistics of a Port (continued)

Statistics	Description
dot3StatsFrameTooLongs	<p>A count of frames received on a particular interface that exceed the maximum permitted frame size.</p> <p>The count represented by an instance of this object is incremented when the <code>frameTooLong</code> status is returned by the MAC service to the LLC (or other MAC user). Received frames for which multiple error conditions obtained are, according to the conventions of IEEE 802.3 Layer Management, counted exclusively according to the error status presented to the LLC.</p>
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	
PriFlowCtrlPkts:	0	0	
Discards:	0	0	
Errors:	0	21187	
Ingress Discard reasons:		Egress Discard reasons:	
VLAN Discards:	0	HOL-blocking Discards:	0
Filter Discards:	0	MMU Discards:	0
Policy Discards:	0	Cell Error Discards:	0
Non-Forwarding State:	0	MMU Aging Discards:	0
IBP/CBP Discards:	0	Other Discards:	0
Empty Egress Portmap:	3085 *		
* Check for "HOL-blocking" discards on associated egress ports			

Table 92. 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 pause packets received on the interface.
ifInPriFlowControlPkts	The total number of priority flow control pause packets received on the interface.

Table 92. Interface Statistics of a Port (continued)

Statistics	Description
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> .
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.
VLAN Discards	Discarded because the packet was tagged with a VLAN to which this port is not a member.

Table 92. Interface Statistics of a Port (continued)

Statistics	Description
Filter Discards	Dropped by the Content Aware Engine (user-configured filter).
Policy Discards	Dropped due to policy setting. For example, due to a user-configured static entry.
Non-Forwarding State	Discarded because the ingress port is not in the forwarding state.
IBP/CBP Discards	Discarded because of Ingress Back Pressure (flow control), or because the Common Buffer Pool is full (for example, insufficient packet buffering).
HOL-blocking Discards	Discarded because of the Head Of Line (HOL) blocking mechanism. Low-priority packets are placed in a separate queue and can be discarded while applications or the TCP protocol determine whether a retransmission is necessary. HOL blocking forces transmission to stop until the overloaded egress port buffer can receive data again.
MMU Discards	Discarded because of the Memory Management Unit.
Cell Error Discards	
MMU Aging Discards	
Other Discards	Discarded packets not included in any category.

## 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 93. 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 94. 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 95. RMON Statistics of a Port

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

Table 95. RMON Statistics of a Port (continued)

Statistics	Description
etherStatsUndersizePkts	The total number of packets received that were less than 64 octets long (excluding framing bits but including FCS octets) and were otherwise well formed.
etherStatsOversizePkts	The total number of packets received that were longer than 1518 octets (excluding framing bits but including FCS octets) and were otherwise well formed.
etherStatsFragments	The total number of packets received that were less than 64 octets in length (excluding framing bits but including FCS octets) and had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error).
etherStatsJabbers	The total number of packets received that were longer than 1518 octets (excluding framing bits, but including FCS octets), and had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error). Jabber is defined as the condition where any packet exceeds 20 ms. The allowed range to detect jabber is between 20 ms and 150 ms.
etherStatsCollisions	The best estimate of the total number of collisions on this Ethernet segment.
etherStatsPkts64Octets	The total number of packets (including bad packets) received that were less than or equal to 64 octets in length (excluding framing bits but including FCS octets).
etherStatsPkts65to127Octets	The total number of packets (including bad packets) received that were greater than 64 octets in length (excluding framing bits but including FCS octets).
etherStatsPkts128to255Octets	The total number of packets (including bad packets) received that were greater than 127 octets in length (excluding framing bits but including FCS octets).
etherStatsPkts256to511Octets	The total number of packets (including bad packets) received that were greater than 255 octets in length (excluding framing bits but including FCS octets).

Table 95. RMON Statistics of a Port (continued)

Statistics	Description
etherStatsPkts512to1023 Octets	The total number of packets (including bad packets) received that were greater than 511 octets in length (excluding framing bits but including FCS octets).
etherStatsPkts1024to1518 Octets	The total number of packets (including bad packets) received that were greater than 1023 octets in length (excluding framing bits but including FCS octets).

## QoS Queue Counter-Based Statistics

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

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

**Command mode:** All.

```

QoS statistics for port INTA14:
QoS Queue 0:
  Tx Packets:                664872
  Dropped Packets:           0
  Tx Bytes:                  46791050
  Dropped Bytes:             0
QoS Queue 1:
  Tx Packets:                0
  Dropped Packets:           0
  Tx Bytes:                  0
  Dropped Bytes:             0
QoS Queue 2:
  Tx Packets:                0
  Dropped Packets:           0
  Tx Bytes:                  0
  Dropped Bytes:             0
QoS Queue 3:
  Tx Packets:                0
  Dropped Packets:           0
  Tx Bytes:                  0
  Dropped Bytes:             0
QoS Queue 4:
  Tx Packets:                0
  Dropped Packets:           0
  Tx Bytes:                  0
  Dropped Bytes:             0
QoS Queue 5:
  Tx Packets:                0
  Dropped Packets:           0
  Tx Bytes:                  0
  Dropped Bytes:             0
QoS Queue 6:
  Tx Packets:                0
  Dropped Packets:           0
  Tx Bytes:                  0
  Dropped Bytes:             0
QoS Queue 7:
  Tx Packets:                9112
  Dropped Packets:           0
  Tx Bytes:                  1463040
  Dropped Bytes:             0

```

Table 96. QoS Queue Counter-Based Statistics of a Port

Statistics	Description
Tx Packets	Total number of successfully transmitted packets for the QoS queue
Dropped Packets	Total number of dropped packets for the QoS queue

Table 96. QoS Queue Counter-Based Statistics of a Port (continued)

Statistics	Description
Tx Bytes	Total number of successfully transmitted bytes for the QoS queue
Dropped Bytes	Total number of dropped bytes for the QoS queue

## QoS Queue Rate-Based Statistics

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

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

**Command mode:** All.

```

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

```

Table 97. QoS Queue Rate-Based Statistics of a Port

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

---

## Trunk Group Statistics

Table 98. Trunk Group Statistics Commands

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

---

## Layer 2 Statistics

Table 99. Layer 2 Statistics Commands

Command Syntax and Usage
<pre>show mac-address-table counters</pre> <p>Displays FDB statistics. See <a href="#">page 168</a> for sample output.</p> <p><b>Command mode:</b> All</p>
<pre>clear mac-address-table counters</pre> <p>Clears FDB statistics.</p> <p><b>Command mode:</b> Privileged EXEC</p>
<pre>show interface port &lt;port alias or number&gt; lacp counters</pre> <p>Displays Link Aggregation Control Protocol (LACP) statistics. See <a href="#">page 168</a> for sample output.</p> <p><b>Command mode:</b> All</p>
<pre>clear interface port &lt;port alias or number&gt; lacp counters</pre> <p>Clears Link Aggregation Control Protocol (LACP) statistics.</p> <p><b>Command mode:</b> Privileged EXEC</p>
<pre>show hotlinks counters</pre> <p>Displays Hot Links statistics. See <a href="#">page 169</a> for sample output.</p> <p><b>Command mode:</b> All</p>
<pre>clear hotlinks</pre> <p>Clears all Hot Links statistics.</p> <p><b>Command mode:</b> Privileged EXEC</p>
<pre>show interface port &lt;port alias or number&gt; lldp counters</pre> <p>Displays LLDP statistics. See <a href="#">page 170</a> for sample output.</p> <p><b>Command mode:</b> All</p>
<pre>show oam counters</pre> <p>Displays OAM statistics. See <a href="#">page 171</a> for sample output.</p> <p><b>Command mode:</b> All</p>
<pre>show vlag statistics</pre> <p>Displays all vLAG statistics. See <a href="#">page 172</a> for sample output.</p> <p><b>Command mode:</b> All</p>

## 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 100. 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 101. 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.



Table 101. LACP Statistics

Statistic	Description
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 102. 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 103. 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 104. vLAG Statistics Options*

Command Syntax and Usage
<pre>show vlag isl-statistics</pre> <p>Displays vLAG ISL statistics for the selected port. See <a href="#">page 172</a> for sample output.</p> <p><b>Command mode:</b> All</p>
<pre>clear vlag statistics</pre> <p>Clears all vLAG statistics.</p> <p><b>Command mode:</b> Privileged EXEC</p>
<pre>show vlag statistics</pre> <p>Displays all vLAG statistics. See <a href="#">page 172</a> for sample output.</p> <p><b>Command mode:</b> All</p>

## vLAG ISL Statistics

Use the following command to display vLAG statistics:

```
show vlag isl-statistics
```

**Command mode:** All

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

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

## vLAG Statistics

Use the following command to display vLAG statistics:

```
show vlag statistics
```

**Command mode:** All

vLAG PDU sent:			
Role Election:	10	System Info:	7
Peer Instance Enable:	624	Peer Instance Disable:	52
FDB Dynamic Add:	166079	FDB Dynamic Del:	33856
FDB Inactive Add:	0	FDB Inactive Del:	0
Health Check:	4665	ISL Hello:	2126
Other:	0	Unknown:	0
vLAG PDU received:			
Role Election:	11	System Info:	6
Peer Instance Enable:	572	Peer Instance Disable:	52
FDB Dynamic Add:	122523	FDB Dynamic Del:	38991
FDB Inactive Add:	7200	FDB Inactive Del:	0
Health Check:	4656	ISL Hello:	2114
Other:	0	Unknown:	0
vLAG IGMP packets forwarded:			
IGMP Reports:	0		
IGMP Leaves:	0		
Bingo-1#			

The following table describes the vLAG statistics:

*Table 105. VLAG Statistics*

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

Table 105. VLAG Statistics (continued)

Statistic	Description
Peer Instance Disable	Total number of vLAG PDUs sent for disabling peer instance.
FDB Dynamic Add	Total number of vLAG PDUs sent for addition of FDB dynamic entry.
FDB Dynamic Del	Total number of vLAG PDUs sent for deletion of FDB dynamic entry.
FDB Inactive Add	Total number of vLAG PDUs sent for addition of FDB inactive entry.
FDB Inactive Del	Total number of vLAG PDUs sent for deletion of FDB inactive entry.
Health Check	Total number of vLAG PDUs sent for health checks.
ISL Hello	Total number of vLAG PDUs sent for ISL hello.
Other	Total number of vLAG PDUs sent for other reasons.
Unknown	Total number of vLAG PDUs sent for unknown operations.

---

## Layer 3 Statistics

Table 106. Layer 3 Statistics Commands

Command Syntax and Usage
<pre>show ip gea show ip gea bucket &lt;IP address&gt;</pre> <p>Displays Gigabit Ethernet Aggregators (GEA) statistics. GEA statistics are used by service and support personnel.</p> <p><b>Command mode:</b> All</p>
<pre>show ip counters</pre> <p>Displays IP statistics. See <a href="#">page 178</a> for sample output.</p> <p><b>Command mode:</b> All</p>
<pre>clear ip counters</pre> <p>Clears IPv4 statistics. Use this command with caution as it deletes all the IPv4 statistics.</p> <p><b>Command mode:</b> Privileged EXEC</p>
<pre>show ipv6 counters</pre> <p>Displays IPv6 statistics. See <a href="#">page 180</a> for sample output.</p> <p><b>Command mode:</b> All</p>
<pre>clear ipv6 counters</pre> <p>Clears IPv6 statistics. Use this command with caution as it deletes all the IPv6 statistics.</p> <p><b>Command mode:</b> Privileged EXEC</p>
<pre>show ip route counters</pre> <p>Displays route statistics. See <a href="#">page 184</a> for sample output.</p> <p><b>Command mode:</b> All</p>
<pre>show ip arp counters</pre> <p>Displays Address Resolution Protocol (ARP) statistics. See <a href="#">page 186</a> for sample output.</p> <p><b>Command mode:</b> All</p>
<pre>show ip dns counters</pre> <p>Displays Domain Name System (DNS) statistics. See <a href="#">page 186</a> for sample output.</p> <p><b>Command mode:</b> All</p>
<pre>show ip icmp counters</pre> <p>Displays ICMP statistics. See <a href="#">page 187</a> for sample output.</p> <p><b>Command mode:</b> All</p>

Table 106. Layer 3 Statistics Commands (continued)

<b>Command Syntax and Usage</b>
<pre>show ip tcp counters</pre> <p>Displays TCP statistics. See <a href="#">page 189</a> for sample output.</p> <p><b>Command mode:</b> All</p>
<pre>show ip udp counters</pre> <p>Displays UDP statistics. See <a href="#">page 190</a> for sample output.</p> <p><b>Command mode:</b> All</p>
<pre>show ip ospf counters</pre> <p>Displays OSPF statistics. See <a href="#">page 197</a> for sample output.</p> <p><b>Command mode:</b> All</p>
<pre>show ipv6 ospf counters</pre> <p>Displays OSPFv3 statistics. See <a href="#">page 200</a> for sample output.</p> <p><b>Command mode:</b> All</p>
<pre>show ip igmp counters</pre> <p>Displays IGMP statistics. See <a href="#">page 191</a> for sample output.</p> <p><b>Command mode:</b> All</p>
<pre>show ip igmp vlan &lt;vlan number&gt; counter</pre> <p>Displays IGMP statistics for a specific VLAN. See <a href="#">page 191</a> for sample output.</p> <p><b>Command mode:</b> All</p>
<pre>show layer3 igmp-groups</pre> <p>Displays the total number of IGMP groups that are registered on the switch.</p> <p><b>Command mode:</b> All</p>
<pre>show layer3 ipmc-groups</pre> <p>Displays the total number of current IP multicast groups that are registered on the switch.</p> <p><b>Command mode:</b> All</p>
<pre>show ip vrrp counters</pre> <p>When virtual routers are configured, you can display the protocol statistics for VRRP. See <a href="#">page 205</a> for sample output.</p> <p><b>Command mode:</b> All</p>
<pre>show ip pim counters</pre> <p>Displays PIM statistics for all configured PIM interfaces. See <a href="#">page 206</a> for sample output.</p> <p><b>Command mode:</b> All</p>
<pre>show ip pim mroute count</pre> <p>Displays statistics of various multicast entry types.</p> <p><b>Command mode:</b> All</p>

Table 106. Layer 3 Statistics Commands (continued)

Command Syntax and Usage
<pre>show ip pim interface { &lt;interface number&gt;   loopback   port &lt;port number&gt; } counters</pre> <p>Displays PIM statistics for the selected interface.</p> <p><b>Command mode:</b> All</p>
<pre>show ip rip counters</pre> <p>Displays Routing Information Protocol (RIP) statistics. See <a href="#">page 207</a> for sample output.</p> <p><b>Command mode:</b> All</p>
<pre>clear ip arp counters</pre> <p>Clears Address Resolution Protocol (ARP) statistics.</p> <p><b>Command mode:</b> Privileged EXEC</p>
<pre>clear ip dns counters</pre> <p>Clears Domain Name System (DNS) statistics.</p> <p><b>Command mode:</b> Privileged EXEC</p>
<pre>clear ip icmp counters</pre> <p>Clears Internet Control Message Protocol (ICMP) statistics.</p> <p><b>Command mode:</b> Privileged EXEC</p>
<pre>clear ip tcp counters</pre> <p>Clears Transmission Control Protocol (TCP) statistics.</p> <p><b>Command mode:</b> Privileged EXEC</p>
<pre>clear ip udp counters</pre> <p>Clears User Datagram Protocol (UDP) statistics.</p> <p><b>Command mode:</b> Privileged EXEC</p>
<pre>clear ip igmp [&lt;VLAN number&gt;] counters</pre> <p>Clears IGMP statistics.</p> <p><b>Command mode:</b> Privileged EXEC</p>
<pre>clear ip vrrp counters</pre> <p>Clears VRRP statistics.</p> <p><b>Command mode:</b> Privileged EXEC</p>
<pre>clear ip pim counters</pre> <p>Clears PIM statistics for all interfaces.</p> <p><b>Command mode:</b> Privileged EXEC</p>
<pre>clear ip pim interface { &lt;interface number&gt;   loopback   port &lt;port number&gt; } counters</pre> <p>Clears PIM statistics on the selected interface.</p> <p><b>Command mode:</b> Privileged EXEC</p>



Table 106. Layer 3 Statistics Commands (continued)

Command Syntax and Usage
<pre>clear ip counters</pre> <p>Clears IP statistics. Use this command with caution as it will delete all the IP statistics.</p> <p><b>Command mode:</b> Privileged EXEC</p>
<pre>clear ip rip counters</pre> <p>Clears Routing Information Protocol (RIP) statistics.</p> <p><b>Command mode:</b> Privileged EXEC</p>
<pre>clear ip ospf counters</pre> <p>Clears Open Shortest Path First (OSPF) statistics.</p> <p><b>Command mode:</b> Privileged EXEC</p>
<pre>clear ipv6 ospf counters</pre> <p>Clears Open Shortest Path First version 3 (OSPFv3) statistics.</p> <p><b>Command mode:</b> Privileged EXEC</p>
<pre>show layer3 counters</pre> <p>Dumps all Layer 3 statistics. Use this command to gather data for tuning and debugging switch performance. If you want to capture dump data to a file, set your communication software on your workstation to capture session data prior to issuing the dump command.</p> <p><b>Command mode:</b> All</p>

## IPv4 Statistics

The following command displays IPv4 statistics:

```
show ip counters
```

**Command mode:** All

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

Use the following command to clear IPv4 statistics:

```
clear ip counters
```

*Table 107. 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 <code>checksums</code> , version number mismatch, other format errors, time-to-live exceeded, errors discovered in processing their IP options, and so forth.
ipInAddrErrors	The number of input datagrams discarded because the IP address in their IP header's destination field was not a valid address to be received at this entity (the switch). This count includes invalid addresses (for example, 0.0.0.0) and addresses of unsupported Classes (for example, Class E). For entities which are not IP Gateways and therefore do not forward datagrams, this counter includes datagrams discarded because the destination address was not a local address.
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).

Table 107. IPv4 Statistics (continued)

Statistics	Description
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

```

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   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   PktTooBig     10  EchoReq      9   EchoReply
0   RouterSols  0   RouterAdv     11  NeighSols    5   NeighborAdv
0   RedirectMsgs 0   AdminProhibMsgs

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

Sent :
0   UDPDgrams

```

Use the following command to clear IPv6 statistics:

```
clear ipv6 counters
```

[Table 108](#). describes the IPv6 statistics.

*Table 108. 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.

Table 108. IPv6 Statistics (continued)

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

Table 108. IPv6 Statistics (continued)

Statistic	Description
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 <code>Don't Fragment</code> 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 109. ICMP Statistics

Statistic	Description
<b>Received</b>	
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 <code>checksums</code> , 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.

Table 109. ICMP Statistics

Statistic	Description
<b>Sent</b>	
ICMPMsgs	Number of ICMP messages which this entity (the switch) attempted to send.
ICMPErrMsgs	Number of ICMP messages which this entity (the switch) did not send due to problems discovered within ICMP such as a lack of buffer. This value should not include errors discovered outside the ICMP layer such as the inability of IP to route the resultant datagram. In some implementations there may be no types of errors that contribute to this counter's value.
DstUnReach	Number of ICMP Destination Unreachable messages sent.
TimeExcds	Number of ICMP Time Exceeded messages sent.
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 110. describes the UDP statistics.

Table 110. UDP Statistics

Statistic	Description
<b>Received</b>	
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.
<b>Sent</b>	
UDPDgrams	Number of UDP datagrams sent from this entity (the switch).

## IPv4 Route Statistics

The following command displays IPv4 route statistics:

```
show ip route counters
```

**Command mode:** All

```

Route statistics:
-----
Current total outstanding routes      :          1
Highest number ever recorded         :          1
Current static routes                 :           0
Current RIP routes                   :           0
Current OSPF routes                   :           0
Current BGP routes                   :           0
Maximum supported routes              :        16384

ECMP statistics (active in ASIC):
-----
Maximum number of ECMP routes        :        16384
Maximum number of static ECMP routes :         128
Number of routes with ECMP paths     :           0

```

*Table 111. Route Statistics*

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



## IPv6 Route Statistics

The following command displays IPv6 route statistics:

```
show ipv6 route counters
```

**Command mode:** All

IPv6 Route statistics:			
ipv6RoutesCur:	4	ipv6RoutesHighWater:	6
ipv6RoutesMax:	1156		
ECMP statistics:			
-----			
Maximum number of ECMP routes	:	600	
Max ECMP paths allowed for one route	:	5	
Number of routes with ECMP paths	:	0	

Table 112. 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 113. ARP Statistics

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

## DNS Statistics

The following command displays Domain Name System statistics.

```
show ip dns counters
```

**Command mode:** All

DNS statistics:	
dnsInRequests:	0
dnsOutRequests:	0
dnsBadRequests:	0

Table 114. DNS Statistics

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

## ICMP Statistics

The following command displays ICMP statistics:

```
show ip icmp counters
```

**Command mode:** All

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

Table 115. ICMP Statistics

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

Table 115. ICMP Statistics (continued)

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

## TCP Statistics

The following command displays TCP statistics:

```
show ip tcp counters
```

**Command mode:** All

TCP statistics:			
tcpRtoAlgorithm:	4	tcpRtoMin:	0
tcpRtoMax:	240000	tcpMaxConn:	512
tcpActiveOpens:	252214	tcpPassiveOpens:	7
tcpAttemptFails:	528	tcpEstabResets:	4
tcpInSegs:	756401	tcpOutSegs:	756655
tcpRetransSegs:	0	tcpInErrs:	0
tcpCurrEstab:	0	tcpCurConn:	3
tcpOutRsts:	417		

Table 116. 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 SYN-SENT state from the CLOSED state.
tcpPassiveOpens	The number of times TCP connections have made a direct transition to the SYN-RCVD state from the LISTEN state.
tcpAttemptFails	The number of times TCP connections have made a direct transition to the CLOSED state from either the SYN-SENT state or the SYN-RCVD state, plus the number of times TCP connections have made a direct transition to the LISTEN state from the SYN-RCVD state.

Table 116. TCP Statistics (continued)

Statistic	Description
tcpEstabResets	The number of times TCP connections have made a direct transition to the CLOSED state from either the ESTABLISHED state or the CLOSE-WAIT state.
tcpInSegs	The total number of segments received, including those received in error. This count includes segments received on currently established connections.
tcpOutSegs	The total number of segments sent, including those on current connections but excluding those containing only retransmitted octets.
tcpRetransSegs	The total number of segments retransmitted - that is, the number of TCP segments transmitted containing one or more previously transmitted octets.
tcpInErrs	The total number of segments received in error (for example, bad TCP checksums).
tcpCurrEstab	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 117. 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 vlan 2 statistics:			
-----			
rxIgmpValidPkts:	0	rxIgmpInvalidPkts:	0
rxIgmpGenQueries:	0	rxIgmpGrpSpecificQueries:	0
rxIgmpGroupSrcSpecificQueries:	0	rxIgmpDiscardPkts:	0
rxIgmpLeaves:	0	rxIgmpReports:	0
txIgmpReports:	0	txIgmpGrpSpecificQueries:	0
txIgmpLeaves:	0	rxIgmpV3CurrentStateRecords:	0
rxIgmpV3SourceListChangeRecords:	0	rxIgmpV3FilterChangeRecords:	0
txIgmpGenQueries:	18		

The following command displays statistics about the use of the IGMP Multicast Groups for a specific VLAN:

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

**Command mode:** All

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

Table 118. IGMP Statistics

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

Table 118. IGMP Statistics (continued)

<b>Statistic</b>	<b>Description</b>
rxIgmPReports	Total number of Membership Reports received
txIgmPReports	Total number of Membership reports transmitted
txIgmPGrpSpecificQueries	Total number of Membership Query packets transmitted to specific groups
txIgmPLeaves	Total number of Leave messages transmitted
rxIgmPV3CurrentStateRecords	Total number of Current State records received
rxIgmPV3SourceListChangeRecords	Total number of Source List Change records received.
rxIgmPV3FilterChangeRecords	Total number of Filter Change records received.
txIgmPGenQueries	Total number of General Membership Query packets transmitted



## MLD Statistics

Table 119 describes the commands used to view MLD statistics.

Table 119. MLD Statistics Commands

Command Syntax and Usage
<pre>show ipv6 mld counters</pre> <p>Displays MLD statistics. See <a href="#">page 194</a> for sample output.</p> <p><b>Command mode:</b> All</p>
<pre>show ipv6 mld groups counters</pre> <p>Displays total number of MLD entries.</p> <p><b>Command mode:</b> All</p>
<pre>show ipv6 mld interface</pre> <p>Displays information for all MLD interfaces.</p> <p><b>Command mode:</b> All</p>
<pre>show ipv6 mld interface &lt;interface number&gt;</pre> <p>Displays MLD interface statistics for the specified interface.</p> <p><b>Command mode:</b> All</p>
<pre>show ipv6 mld interface &lt;interface number&gt; counters</pre> <p>Displays total number of MLD entries on the interface.</p> <p><b>Command mode:</b> All</p>
<pre>show ipv6 mld interface counters</pre> <p>Displays total number of MLD entries.</p> <p><b>Command mode:</b> All</p>
<pre>clear ipv6 mld counters</pre> <p>Clears MLD counters.</p> <p><b>Command mode:</b> All except User Exec</p>
<pre>clear ipv6 mld dynamic</pre> <p>Clears all dynamic MLD tables.</p> <p><b>Command mode:</b> All except User Exec</p>
<pre>clear ipv6 mld groups</pre> <p>Clears dynamic MLD registered group tables.</p> <p><b>Command mode:</b> All except User Exec</p>
<pre>clear ipv6 mld mrouter</pre> <p>Clears dynamic MLD Mrouter group tables.</p> <p><b>Command mode:</b> All except User Exec</p>

## MLD Global Statistics

The following command displays MLD global statistics for all MLD packets received on all interfaces:

```
show ipv6 mld counters
```

**Command mode:** All

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

MLD packet statistics for interfaces:

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

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

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

Table 120. MLD Global Statistics

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

## OSPF Statistics

Table 121. OSPF Statistics Commands

Command Syntax and Usage
<pre>show ip ospf counters</pre> <p>Displays OSPF statistics. See <a href="#">page 197</a> for sample output.</p> <p><b>Command mode:</b> All</p>
<pre>show ip ospf area counters</pre> <p>Displays OSPF area statistics.</p> <p><b>Command mode:</b> All</p>
<pre>show ip ospf interface [&lt;interface number&gt;] counters</pre> <p>Displays OSPF interface statistics.</p> <p><b>Command mode:</b> All</p>

## OSPF Global Statistics

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

```
show ip ospf counters
```

**Command mode:** All

```

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

Nbr change stats:    Intf change Stats:
hello                2          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 122. OSPF General Statistics

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

Table 122. OSPF General Statistics (continued)

Statistic	Description
Rx Database	The sum total of all Database Description packets received on all OSPF areas and interfaces.
Tx Database	The sum total of all Database Description packets transmitted on all OSPF areas and interfaces.
Rx Is Requests	The sum total of all Link State Request packets received on all OSPF areas and interfaces.
Tx Is Requests	The sum total of all Link State Request packets transmitted on all OSPF areas and interfaces.
Rx Is Acks	The sum total of all Link State Acknowledgement packets received on all OSPF areas and interfaces.
Tx Is Acks	The sum total of all Link State Acknowledgement packets transmitted on all OSPF areas and interfaces.
Rx Is Updates	The sum total of all Link State Update packets received on all OSPF areas and interfaces.
Tx Is Updates	The sum total of all Link State Update packets transmitted on all OSPF areas and interfaces.
<b>Nbr Change Stats:</b>	
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.

Table 122. OSPF General Statistics (continued)

Statistic	Description
bad sequence	The sum total number of Database Description packets which have been received that either: <ol style="list-style-type: none"> <li>Has an unexpected DD sequence number</li> <li>Unexpectedly has the init bit set</li> <li>Has an options field differing from the last Options field received in a Database Description packet.</li> </ol> Any of these conditions indicate that some error has occurred during adjacency establishment for all OSPF areas and interfaces.
loading done	The sum total number of link state updates received for all out-of-date portions of the database across all OSPF areas and interfaces.
n1way	The sum total number of Hello packets received from neighbors, in which this router is not mentioned across all OSPF interfaces and areas.
rst_ad	The sum total number of times the Neighbor adjacency has been reset across all OPSF areas and interfaces.
down	The total number of Neighboring routers down (that is, in the initial state of a neighbor conversation.) across all OSPF areas and interfaces.
<b>Intf Change Stats:</b>	
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 122. OSPF General Statistics (continued)

Statistic	Description
<b>Timers Kickoff:</b>	
hello	The sum total number of times the Hello timer has been fired (which triggers the send of a Hello packet) across all OSPF areas and interfaces.
retransmit	The sum total number of times the Retransmit timer has been fired across all OSPF areas and interfaces.
lsa lock	The sum total number of times the Link State Advertisement (LSA) lock timer has been fired across all OSPF areas and interfaces.
lsa ack	The sum total number of times the LSA 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 123. OSPFv3 Statistics Commands

Command Syntax and Usage
<pre>show ipv6 ospf counters</pre> <p>Displays OSPFv3 statistics.</p> <p><b>Command mode:</b> All</p> <p>See <a href="#">page 197</a> for sample output.</p>
<pre>show ipv6 ospf area counters</pre> <p>Displays OSPFv3 area statistics.</p> <p><b>Command mode:</b> All</p>
<pre>show ipv6 ospf interface [&lt;interface number&gt;] counters</pre> <p>Displays OSPFv3 interface statistics.</p> <p><b>Command mode:</b> All</p>



## OSPFv3 Global Statistics

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

```
show ipv6 ospf counters
```

**Command mode:** All

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

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 124. OSPFv3 General Statistics

Statistics	Description
<b>Rx/Tx Stats:</b>	
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.
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.

Table 124. OSPFv3 General Statistics (continued)

Statistics	Description
<b>Nbr Change Stats:</b>	
down	The total number of Neighboring routers down (in the initial state of a neighbor conversation) across all OSPFv3 interfaces.
attempt	The total number of transitions into attempt state of neighboring routers across all OSPFv3 interfaces.
init	The total number of transitions into init state of neighboring routers across all OSPFv3 interfaces.
n2way	The total number of bidirectional communication establishment between this router and other neighboring routers.
exstart	The total number of transitions into exstart state of neighboring routers across all OSPFv3 interfaces
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.
<b>Inf Change Stats:</b>	
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.

Table 124. OSPFv3 General Statistics (continued)

Statistics	Description
<b>Timers Kickoff:</b>	
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.
<b>Number of LSAs:</b>	
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	vrrpOutGratuitousARPs:	0
vrrpBadVersion:	0	vrrpBadVrid:	0
vrrpBadAddress:	0	vrrpBadData:	0
vrrpBadPassword:	0	vrrpBadInterval:	0

*Table 125. 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.
vrrpOut GratuitousARPs	The total number of VRRP gratuitous ARPs that have been sent.
vrrpBadVrid	The total number of VRRP advertisements received that had a bad virtual router ID.
vrrpBadAddress	The total number of VRRP advertisements received that had a bad address.
vrrpBadData	The total number of VRRP advertisements received that had bad data.
vrrpBadPassword	The total number of VRRP advertisements received that had a bad password.
vrrpBadInterval	The total number of VRRP advertisements received that had a bad interval.

## PIM Statistics

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

```
show ip pim counters
```

**Command mode:** All

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

Table 126. PIM Statistics

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

## Routing Information Protocol Statistics

The following command displays RIP statistics:

```
show ip rip counters
```

**Command mode:** All

```
RIP ALL STATS INFORMATION:
  RIP packets received = 12
  RIP packets sent     = 75
  RIP request received = 0
  RIP response received = 12
  RIP request sent     = 3
  RIP 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 127. DHCP Statistics Options*

Command Syntax and Usage
<pre>show ip dhcp snooping counters</pre> <p>Displays DHCP Snooping statistics.</p> <p><b>Command mode:</b> All</p>
<pre>clear ip dhcp snooping counters</pre> <p>Clears DHCP Snooping statistics.</p> <p><b>Command mode:</b> Privileged EXEC</p>

## 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.

---

## OpenFlow Statistics

Table 128. OpenFlow Statistics Commands

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

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

```
show openflow statistics
```

Command mode: All

In OpenFlow 1.0:

```
Openflow instance 1 is currently disabled
-----
Openflow statistics for instance 2
Flow Count
  Basic Flows:      3      (ACL Based: 3, Unicast FDB Based: 0, Multicast FDB
Based: 0)
  Emergency Flows: 0      (ACL Based: 0, Unicast FDB Based: 0, Multicast FDB
Based: 0)

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

Message Count
Hello-Sent: 1              Hello-Received: 1
Echo-Request-Sent: 31      Echo-Request-Received: 60
Echo-Reply-Sent: 60        Echo-Reply-Received: 31
Vendor: 0
```



```

Vendor Flow-Mod:
  Add: 0
  Modify: 0
  Modify-Strict: 0
  Delete: 0
  Delete-Strict: 0
Feature-Request: 1
Get-Config-Request: 0
Set-Config: 1
Packet-In
  No-Match: 0
  Action: 0
  Action Mirror: 0
Flow-Removed:
  Idle-Timeout: 0
  Hard-Timeout: 0
  Delete: 0
Vendor-Flow-Removed:
  Idle-Timeout: 0
  Hard-Timeout: 0
  Delete: 0
Port-Status:
  Add: 0
  Delete: 0
  Modify: 0
Packet-Out: 1088
Flow-Mod:
  Add: 3
  Modify: 0
  Modify-Strict: 0
  Delete: 0
  Delete-Strict: 1
Port-Mod: 0
Statistics-Request:
  Desc: 1
  Flow: 15
  Aggregate: 0
  Table: 0
  Port: 15
  Vendor: 0
  stats: 0
  stats-strict: 0
Statistics-Reply:
  Desc: 1
  Flow: 15
  Aggregate: 0
  Table: 0
  Port: 15
  Vendor: 0
  stats: 0
  stats-strict: 0
Barrier-Request: 2
Barrier-Reply: 2
Error Messages
Hello Failed Sent:
  Incompatible: 0
Hello Failed Recv:
  Incompatible: 0

```

```
Bad Request:
  Bad-Version: 0
  Bad-Type: 0
  Bad-Stat: 0
  Bad-Vendor: 0
  Bad-Subtype: 0
  Bad-Len: 0
  Buffer-Empty: 0
  Buffer-Unknown: 0
Bad Action:
  Bad-Type: 0
  Bad-Len: 0
  Bad-Out-Port: 0
  Bad-Argument: 0
  Too-many: 0
Flow-Mod-Failed:
  All-Table-Full: 0
  Overlap: 0
  Permission-Error: 0
  Emergency-Timeout: 0
  Bad-Command: 0
  Unsupported: 0
Port-Mod-Failed:
  Bad-Port: 0
  Bad-hw-addr: 0
```

**In Openflow 1.3:**

```
Openflow instance 1 is currently disabled
-----
Openflow statistics for instance 2
Flow Count
  Static Flows: 0
    ACL Based: 0
    Mpls PUSH based: 0
    Mpls POP based: 0
  Dynamic Flows: 3
    ACL Based: 3
    Unicast FDB Based: 0
    Multicast FDB Based: 0
    Mpls PUSH based: 0
    Mpls POP based: 0
Buffering Count:
  Openflow Packets Buffered : 0
  Openflow Packets Timed out : 0
  Openflow Packets Retrieved : 0
  Openflow Packets Retrieve attempts : 0
```

```

Message Count
Hello-Sent: 1
Echo-Request-Sent: 27
Echo-Reply-Sent: 54
Feature-Request: 1
Get-Config-Request: 0
Set-Config: 1
Packet-In
    No-Match: 0
    Action: 0
Flow-Removed:
    Idle-Timeout: 0
    Hard-Timeout: 0
    Delete: 0
Port-Status:
    Add: 1
    Delete: 0
    Modify: 1
Packet-Out: 974
Flow-Mod:
    Add: 3
    Modify: 0
    Modify-Strict: 0
    Delete: 0
    Delete-Strict: 1
Port-Mod: 0
Multipart-Request:
    Switch description: 2
    Individual flow statistics: 13
    Aggregate flow statistics: 0
    Flow table statistics: 0
    Port statistics: 13
    Port description: 1
Multipart-Reply:
    Switch description: 2
    Individual flow statistics: 13
    Aggregate flow statistics: 0
    Flow table statistics: 0
    Port statistics: 13
    Port description: 1
Barrier-Request: 2
Barrier-Reply: 2
Error Messages
Hello Failed Sent:
    Incompatible: 0
Hello Failed Recv:
    Incompatible: 0
Bad Request:
    Bad-Version: 0
    Bad-Type: 0
    Bad-Multipart: 0
    Permission-error: 0
    Bad-Len: 0
    Buffer-Empty: 0
    Buffer-Unknown: 0
    Bad-Table-ID: 0
    Bad-Port: 0
    Bad-Packet: 0
    Multipart-Buffer-Overflow: 0
Hello-Received: 1
Echo-Request-Received: 54
Echo-Reply-Received: 27
Feature-Reply: 1
Get-Config-Reply: 0

```

```

Bad Action:
  Bad-Type: 0
  Bad-Len: 0
  Bad-Out-Port: 0
  Bad-Argument: 0
  Too-many: 0
  Match-Inconsistent: 0
  Unsupported-Order: 0
  Bad-Set-Type: 0
  Bad-Set-Len: 0
  Bad-Set-Argument: 0
Bad Instruction:
  Unknown-Instruction: 0
  Unsupport-Instruction: 0
  Bad-Len: 0
  Permission-Error: 0
Bad Match:
  Bad-Type: 0
  Bad-Len: 0
  Bad-MAC-Addr-Mask: 0
  Bad-IP-Addr-Mask: 0
  Bad-Wildcards: 0
  Bad-Field: 0
  Bad-Value: 0
  Bad-Mask: 0
  Bad-Prerequisites: 0
  Duplicated-Field: 0
Flow-Mod-Failed:
  Unknown: 0
  Table-Full: 0
  Bad-Table-ID: 0
  Overlap: 0
  Permission-Error: 0
  Bad-Timeout: 0
  Bad-Command: 0
  Bad-Flags: 0
Port-Mod-Failed:
  Bad-Port: 0
  Bad-hw-addr: 0
  Bad-Config: 0
  Bad-Advertise: 0
  Permission-Error: 0
Switch-Config-Failed:
  Bad-Flags: 0
  Permission-Error: 0

```

Table 129. OpenFlow Table Statistics

Parameter	Description
<b>Flow Count</b>	
Basic Flows	Count of flows stored in the basic flow table, sorted by type: ACL, unicast FDB and multicast FDB.
Emergency Flows	Count of flows stored in the emergency flow table, sorted by type: ACL, unicast FDB and multicast FDB.

Parameter	Description
Static Flows	Count of flows stored in the static flow table, sorted by type: ACL, unicast FDB, multicast FDB, MPLS push and MPLS pop. Available only in OpenFlow 1.3.
Dynamic Flows	Count of flows stored in the dynamic flow table, sorted by type: ACL, unicast FDB, multicast FDB, MPLS push and MPLS pop. Available only in OpenFlow 1.3.
<b>Buffering Count</b>	
Openflow Packets Buffered	Count of packets buffered.
Openflow Packets Timed out	Count of buffered packets dropped due to time out.
Openflow Packets Retrieved	Count of packets retrieved.
Openflow Packets Retrieve attempts	Count of attempts made to retrieve the buffer.
Message Count	Count of messages exchanged between Controller and switch.
Hello-Sent	Count of Hello messages sent from the switch to Controller.
Hello-Received	Count of Hello messages received in the Controller from the switch.
Echo-Request-Sent	Count of Echo Request messages sent from switch to Controller.
Echo-Request-Received	Count of Echo Request messages received in switch from Controller.
Echo-Reply-Sent	Count of Echo Reply messages received in switch from Controller.
Echo-Reply-Received	Count of Echo Reply messages received in switch from Controller.
Vendor	Count of Vendor messages received in switch from controller. Available only in OpenFlow 1.0.
<b>Vendor Flow-Mod</b>	Available only in OpenFlow 1.0.
Add	Count of vendor-defined add flow_mod messages received in the switch. Available only in OpenFlow 1.0.
Modify	Count of vendor-defined modify flow_mod messages received in the switch. Available only in OpenFlow 1.0.
Modify-Strict	Count of vendor-defined modify_strict flow_mod messages received in the switch. Available only in OpenFlow 1.0.

Parameter	Description
Delete	Count of vendor-defined <code>delete flow_mod</code> messages received in the switch. Available only in OpenFlow 1.0.
Delete-Strict	Count of vendor-defined <code>delete-strict flow_mod</code> messages received in the switch. Available only in OpenFlow 1.0.
Feature-Request	Count of <code>Feature Request</code> messages received from the Controller to the switch.
Feature-Reply	Count of <code>Feature Reply</code> messages sent from the switch to the Controller.
Get-Config-Request	Count of <code>Get Config Request</code> messages received from the Controller to the switch.
Get-Config-Reply	Count of <code>Get Config Reply</code> messages sent from the switch to the Controller.
Set-Config	Count of <code>Set Config</code> messages received from the Controller.
<b>Packet-In</b>	
No-Match	Count of <code>Packet-In</code> messages sent to Controller due to no matching flows.
Action	Count of <code>Packet-In</code> messages sent to Controller due to action explicitly asking to forward to Controller.
Action Mirror	Count of NEC specific <code>Packet-In</code> messages sent to Controller due to action explicitly asking to forward to Controller. Available only in OpenFlow 1.0.
<b>Flow-Removed</b>	
Idle-Timeout	Count of flow entries removed due to idle-timeout expiration.
Hard-Timeout	Count of flow entries removed due to hard-timeout expiration.
Delete	Count of flow entries removed due to explicit deletion.
<b>Vendor-Flow-Removed</b>	Available only in OpenFlow 1.0.
Idle-Timeout	Count of vendor-defined flow entries removed due to idle-timeout expiration. Available only in OpenFlow 1.0.
Hard-Timeout	Count of vendor-defined flow entries removed due to hard-timeout expiration. Available only in OpenFlow 1.0.
Delete	Count of vendor-defined flow entries removed due to explicit deletion. Available only in OpenFlow 1.0.
<b>Port-Status</b>	

Parameter	Description
Add	Count of <code>port-status</code> messages sent triggered by adding a port to OpenFlow.
Delete	Count of <code>port-status</code> messages sent triggered by removing a port from OpenFlow.
Modify	Count of <code>port-status</code> messages sent triggered by a modification of a port belonging to OpenFlow (for example, up/down status).
Packet-Out	Count of <code>packet-out</code> messages received from the Controller.
<b>Flow-Mod</b>	
Add	Count of <code>add flow_mod</code> messages received in the switch.
Modify	Count of <code>modify flow_mod</code> messages received in the switch.
Modify-Strict	Count of <code>modify_strict flow_mod</code> messages received in the switch.
Delete	Count of <code>delete flow_mod</code> messages received in the switch.
Delete-Strict	Count of <code>delete_strict flow_mod</code> messages received in the switch.
<b>Port-Mod</b>	Count of <code>port_mod</code> messages received in the switch from the Controller.
<b>Statistics-Request</b>	Available only in OpenFlow 1.0.
Desc	Count of Description statistics requests received from the Controller. Available only in OpenFlow 1.0.
Flow	Count of Flow statistics requests received from the Controller. Available only in OpenFlow 1.0.
Aggregate	Count of Aggregate statistics requests received from the Controller. Available only in OpenFlow 1.0.
Table	Count of Table statistics requests received from the Controller. Available only in OpenFlow 1.0.
Port	Count of Port statistics requests received from the Controller. Available only in OpenFlow 1.0.
<b>Vendor</b>	Available only in OpenFlow 1.0.
stats	Count of Vendor statistics requests received from the Controller. Available only in OpenFlow 1.0.
stats-strict	Count of Vendor strict statistics requests received from the Controller. Available only in OpenFlow 1.0.
<b>Statistics-Reply</b>	Available only in OpenFlow 1.0.

Parameter	Description
Desc	Count of Description statistics requests sent to the Controller. Available only in OpenFlow 1.0.
Flow	Count of Flow statistics requests sent to the Controller. Available only in OpenFlow 1.0.
Aggregate	Count of Aggregate statistics requests sent to the Controller. Available only in OpenFlow 1.0.
Table	Count of Table statistics requests sent to the Controller. Available only in OpenFlow 1.0.
Port	Count of Port statistics requests sent to the Controller. Available only in OpenFlow 1.0.
<b>Vendor</b>	Available only in OpenFlow 1.0.
stats	Count of Vendor statistics requests sent to the Controller. Available only in OpenFlow 1.0.
stats-strict	Count of Vendor strict statistics requests sent to the Controller. Available only in OpenFlow 1.0.
<b>Multipart-Request</b>	Available only in OpenFlow 1.3
Switch description	Count of Switch Description requests received from the Controller. Available only in OpenFlow 1.3.
Individual flow statistics	Count of Individual Flow statistics requests received from the Controller. Available only in OpenFlow 1.3.
Aggregate flow statistics	Count of Aggregate statistics requests received from the Controller. Available only in OpenFlow 1.3.
Flow table statistics	Count of Table statistics requests received from the Controller. Available only in OpenFlow 1.3.
Port statistics	Count of Port statistics requests received from the Controller. Available only in OpenFlow 1.3.
Port description	Count of Port descriptions requests received from the Controller. Available only in OpenFlow 1.3.
<b>Multipart-Reply</b>	Available only in OpenFlow 1.3
Switch description	Count of Switch Description replies sent to the Controller. Available only in OpenFlow 1.3.
Individual flow statistics	Count of Individual Flow statistics replies sent to the Controller. Available only in OpenFlow 1.3.
Aggregate flow statistics	Count of Aggregate statistics replies sent to the Controller. Available only in OpenFlow 1.3.
Flow table statistics	Count of Table statistics replies sent to the Controller. Available only in OpenFlow 1.3.
Port statistics	Count of Port statistics replies sent to the Controller. Available only in OpenFlow 1.3.



Parameter	Description
Port description	Count of Port description replies sent to the Controller. Available only in OpenFlow 1.3.
Barrier-Request	Count of <code>barrier-request</code> messages received from the Controller.
Barrier-Reply	Count of <code>barrier-reply</code> messages sent to the Controller.
Error Messages	Count of error messages handled - sending/receiving error messages.
<b>Hello Failed Sent</b>	
Incompatible	Count of error messages sent by the switch if the version in the <code>Hello</code> message is incompatible with the version in the Controller.
<b>Hello Failed Recv</b>	
Incompatible	Count of error messages received in the switch if the version in the <code>Hello</code> message is incompatible with the version in the Controller.
<b>Bad Request</b>	
Bad-Version	Count of error messages sent due to <code>bad-version</code> in the request header.
Bad-Type	Count of error messages sent due to <code>bad-type</code> in the request header.
Bad-Stat	Count of error messages sent due to a specific statistics request that is not supported. Available only in OpenFlow 1.0.
Bad-Vendor	Count of error messages sent due to vendor-specific message that is not supported. Available only in OpenFlow 1.0.
Bad-Subtype	Count of error messages sent due to message subtype that is not supported. Available only in OpenFlow 1.0.
Bad-Multipart	Count of error messages sent due to unknown multipart request type specified in the <code>multipart-request</code> message. Available only in OpenFlow 1.3.
Permission-error	Count of error messages sent because the action received in the <code>flow-mod</code> message <code>Port-Mod-Failed</code> is not permitted. Available only in OpenFlow 1.3.
Bad-Len	Count of error messages sent due to wrong request length for type of message received in the request header.
Buffer-Empty	Count of error messages sent when the specified buffer in the request does not exist.
Buffer-Unknown	Count of error messages sent when the specified buffer in the request does not exist.

Parameter	Description
Bad-Table-ID	Count of error messages sent when the specified <code>table-id</code> in the request is invalid or the <code>table-id</code> doesn't exist. Available only in OpenFlow 1.3.
Bad-Port	Count of error messages sent due to invalid port in the <code>port-mod</code> message. Available only in OpenFlow 1.3.
Bad-Packet	Count of error messages sent when the specified packet is invalid in <code>packet-out</code> . Available only in OpenFlow 1.3.
Multipart-Buffer-Overflow	Count of error messages sent when the specified buffer in the <code>multi-part</code> request is overflowed. Available only in OpenFlow 1.3.
<b>Bad Action</b>	
Bad-Type	Count of error messages sent due to unknown action type specified in <code>flow_mod</code> message.
Bad-Len	Count of error messages sent due to wrong action length for type of message received in the <code>flow_mod</code> message.
Bad-Out-Port	Count of error message sent due to invalid port in the action field specified <code>flow_mod</code> message.
Bad-Argument	Count of error message sent due to bad action argument in <code>flow_mod</code> message that is not supported.
Too-Many	Count of error message sent due to too many actions received in the <code>flow_mod</code> message that cannot be handled.
Match-Inconsistent	Count of error messages sent because the action cannot apply for this match or because there is a <code>set-field</code> missing prerequisite. Available only in OpenFlow 1.3.
Unsupported-Order	Count of error messages sent because the action order in an <code>apply-actions</code> instruction is unsupported for the action list. Available only in OpenFlow 1.3.
Bad-Set-Type	Count of error messages sent due to unsupported type in the <code>set-field</code> action. Available only in OpenFlow 1.3.
Bad-Set-Len	Count of error messages sent due to length problem in the <code>set-field</code> action. Available only in OpenFlow 1.3.
Bad-Set-Argument	Count of error messages sent due to bad argument in the <code>set-field</code> action. Available only in OpenFlow 1.3.
<b>Bad Instruction</b>	
Unknown-Instruction	Count of error messages sent due to unknown instruction in the received <code>flow-mod</code> message. Available only in OpenFlow 1.3.
Unsupport-Instruction	Count of error messages sent due to unsupported instruction in the received <code>flow-mod</code> message. Available only in OpenFlow 1.3.

Parameter	Description
Bad-Len	Count of error messages sent due to wrong instruction length. Available only in OpenFlow 1.3.
Permission-Error	Count of error messages sent due to permission error while processing the instruction. Available only in OpenFlow 1.3.
<b>Bad Match</b>	Available only in OpenFlow 1.3
Bad-Type	Count of error messages sent due to unsupported match type in the match. Available only in OpenFlow 1.3.
Bad-Len	Count of error messages sent due to wrong match length. Available only in OpenFlow 1.3.
Bad-MAC-Addr-Mask	Count of error messages sent due to unsupported MAC address mask in the match. Available only in OpenFlow 1.3.
Bad-IP-Addr-Mask	Count of error messages sent due to unsupported IP address mask in the match. Available only in OpenFlow 1.3.
Bad-Wildcards	Count of error messages sent due to unsupported combination of fields masked or omitted in the match. Available only in OpenFlow 1.3.
Bad-Field	Count of error messages sent due to unsupported field type in the match. Available only in OpenFlow 1.3.
Bad-Value	Count of error messages sent due to unsupported value in a match field. Available only in OpenFlow 1.3.
Bad-Mask	Count of error messages sent due to unsupported mask (neither a MAC address nor an IP address mask) in the match. Available only in OpenFlow 1.3.
Bad-Prerequisites	Count of error messages sent due to unfulfilled prerequisite in the match. Available only in OpenFlow 1.3.
Duplicated-Field	Count of error messages sent due to duplicated fields in the match. Available only in OpenFlow 1.3.
<b>Flow-Mod-Failed</b>	
All-Table-Full	Count of error messages due to table full when adding or updating <code>flow_mod</code> message. Available only in OpenFlow 1.0.
Unknown	Count of error messages sent when the error is unspecified. Available only in OpenFlow 1.3.
Table-Full	Count of error messages sent because of full table when adding or updating the <code>flow-mod</code> message. Available only in OpenFlow 1.3.
Bad-Table-ID	Count of error messages sent because the specified <code>table-id</code> in the <code>flow-mod</code> message is invalid or because the <code>table-id</code> doesn't exist. Available only in OpenFlow 1.3.

Parameter	Description
Overlap	Count of error messages sent due to an attempt to add overlapping <code>flow_mod</code> messages.
Permission-Error	Count of error messages due to permissions not available to perform action received in the <code>flow_mod</code> message <code>Port_Mod_Failed</code> .
Emergency-Timeout	Count of error messages sent due to invalid emergency-timeout in the <code>flow-mod</code> message. Available only in OpenFlow 1.0.
Bad-Timeout	Count of error messages sent when the specified idle/hard timeout in the <code>flow_mod</code> message is unsupported. Available only in OpenFlow 1.3.
Bad-Command	Count of error messages sent due to unknown command.
Unsupported	Count of error messages sent due to unsupported action list. Available only in OpenFlow 1.0.
Bad-Flags	Count of error messages sent when the specified flags in the <code>flow_mod</code> message are unsupported. Available only in OpenFlow 1.3.
<b>Port-Mod-Failed</b>	
Bad-Port	Count of error messages sent due to invalid port in <code>port_mod</code> message.
Bad-hw-addr	Count of error messages sent due to wrong hardware address specified in <code>port_mod</code> message.
Bad-Config	Count of error messages sent due to invalid <code>config</code> in the <code>port_mod</code> message. Available only in OpenFlow 1.3.
Bad-Advertise	Count of error messages sent due to invalid <code>advertise</code> in the <code>port_mod</code> message. Available only in OpenFlow 1.3.
Permission-Error	Count of error messages sent due to permission error while processing the <code>port_mod</code> message. Available only in OpenFlow 1.3.
<b>Switch-Config-Failed</b>	Available only in OpenFlow 1.3
Bad-Flags	Count of error messages sent due to invalid flags in the <code>switch-config</code> message. Available only in OpenFlow 1.3.
Permission-Error	Count of error messages sent due to permission error while processing the <code>switch-config</code> message. Available only in OpenFlow 1.3.

---

## Management Processor Statistics

Table 130. Management Processor Statistics Commands

Command Syntax and Usage
<pre>show mp packet counters</pre> <p>Displays packet statistics, to check for leads and load. To view a sample output and a description of the stats, see <a href="#">page 223</a>.</p> <p><b>Command mode:</b> All</p>
<pre>show mp tcp-block</pre> <p>Displays all TCP control blocks that are in use. To view a sample output and a description of the stats, see <a href="#">page 230</a>.</p> <p><b>Command mode:</b> All</p>
<pre>show mp udp-block</pre> <p>Displays all UDP control blocks that are in use. To view a sample output, see <a href="#">page 231</a>.</p> <p><b>Command mode:</b> All</p>
<pre>show processes cpu</pre> <p>Displays CPU utilization for periods of up to 1, 4, and 64 seconds. To view a sample output and a description of the stats, see <a href="#">page 231</a>.</p> <p><b>Command mode:</b> All</p>

## MP Packet Statistics

Table 131. Packet Statistics Commands

Command Syntax and Usage
<pre>show mp packet counters</pre> <p>Displays packet statistics, to check for leads and load. To view a sample output and a description of the stats, see <a href="#">page 223</a>.</p> <p><b>Command mode:</b> All</p>
<pre>show mp packet logs</pre> <p>Displays a log of all packets received by the CPU.</p> <p><b>Command mode:</b> All</p>
<pre>show mp packet last &lt;number of logs&gt;</pre> <p>Displays a list of the most recent packets received by the CPU.</p> <p><b>Command mode:</b> All</p>

Table 131. Packet Statistics Commands (continued)

Command Syntax and Usage
<pre>show mp packet parse rx tx &lt; parsing_option &gt;</pre> <p>Displays a list of received or sent packets that fit the parsing option. For a list of parsing options, see <a href="#">page 226</a>.</p> <p><b>Command mode:</b> All</p>
<pre>show mp packet dump</pre> <p>Displays all packet statistics and logs.</p> <p><b>Command mode:</b> All</p>

## MP Packet Statistics

The following command displays MP packet statistics:

```
show mp packet counters
```

**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

pkt_hdr statistics:
-----
current      :           0
max          :          3072
hi-watermark :           208
```

Table 132. Packet Statistics

Statistics	Description
<b>Packets received by CPU</b>	
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.
<b>Packet Buffer Statistics</b>	
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.
<b>small packet buffers</b>	
current	Total number of packet allocations with size less than 128 bytes from the packet buffer pool by the TCP/IP protocol stack.
max	Maximum number of small packet allocations supported.
threshold	Threshold value for small packet allocations, beyond which only high-priority small packets are allowed.
hi-watermark	The highest number of packet allocation with size less than 128 bytes from the packet buffer pool by the TCP/IP protocol stack.
hi-water time	Time stamp that indicates when the hi-watermark was reached.



Table 132. Packet Statistics (continued)

Statistics	Description
<b>medium packet buffers</b>	
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.
<b>jumbo packet buffers</b>	
current	Total number of packet allocations with more than 1536 bytes from the packet buffer pool by the TCP/IP protocol stack.
max	Maximum number of jumbo packet allocations supported
hi-watermark	The highest number of packet allocation with more than 1536 bytes from the packet buffer pool by the TCP/IP protocol stack.
<b>pkt_hdr statistics</b>	
current	Total number of packet allocations with more than 1536 bytes from the packet buffer pool by the TCP/IP protocol stack.
max	Maximum number of packet allocations with more than 1536 bytes from the packet buffer pool by the TCP/IP protocol stack.
hi-watermark	The highest number of packet allocation with more than 1536 bytes from the packet buffer pool by the TCP/IP protocol stack.

## Logged Packet Statistics

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

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

The filter options are described in [Table 133](#).

Table 133. Packet Log Parsing Options

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

Table 133. Packet Log Parsing Options (continued)

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

Table 133. Packet Log Parsing Options (continued)

Command Syntax and Usage
<pre>show mp packet parse rx tx radius</pre> <p>Displays only RADIUS packets logged.</p> <p><b>Command mode:</b> All</p>
<pre>show mp packet parse rx tx snmp</pre> <p>Displays only SNMP packets logged.</p> <p><b>Command mode:</b> All</p>
<pre>show mp packet parse rx tx tftp</pre> <p>Displays only TFTP packets logged.</p> <p><b>Command mode:</b> All</p>
<pre>show mp packet parse rx tx udpother</pre> <p>Displays only UDP other-port packets logged.</p> <p><b>Command mode:</b> All</p>
<pre>show mp packet parse rx tx ipv6</pre> <p>Displays only IPv6 packets logged.</p> <p><b>Command mode:</b> All</p>
<pre>show mp packet parse rx tx rip</pre> <p>Displays only RIP packets logged.</p> <p><b>Command mode:</b> All</p>
<pre>show mp packet parse rx tx ospf</pre> <p>Displays only OSPF packets logged.</p> <p><b>Command mode:</b> All</p>
<pre>show mp packet parse rx tx bgp</pre> <p>Displays only BGP packets logged.</p> <p><b>Command mode:</b> All</p>
<pre>show mp packet parse rx tx lldp</pre> <p>Displays only LLDP PDUs logged.</p> <p><b>Command mode:</b> All</p>
<pre>show mp packet parse rx tx vlan &lt;VLAN_number&gt;</pre> <p>Displays only logged packets with the specified VLAN.</p> <p><b>Command mode:</b> All</p>
<pre>show mp packet parse rx tx port &lt;port_number&gt;</pre> <p>Displays only logged packets with the specified port.</p> <p><b>Command mode:</b> All</p>

Table 133. Packet Log Parsing Options (continued)

Command Syntax and Usage
<pre>show mp packet parse rx tx mac &lt;MAC_address&gt;</pre> <p>Displays only logged packets with the specified MAC address.</p> <p><b>Command mode:</b> All</p>
<pre>show mp packet parse rx tx ip-addr &lt;IPv4_address&gt;</pre> <p>Displays only logged packets with the specified IPv4 address.</p> <p><b>Command mode:</b> All</p>
<pre>show mp packet parse rx tx other</pre> <p>Displays logs of all packets not explicitly selectable.</p> <p><b>Command mode:</b> All</p>
<pre>show mp packet parse rx tx raw</pre> <p>Displays raw packet buffer in addition to headers.</p> <p><b>Command mode:</b> All</p>
<pre>show mp packet parse rx tx mgmtsock</pre> <p>Displays only packets logged from management ports.</p> <p><b>Command mode:</b> All</p>

## TCP Statistics

The following command displays TCP statistics:

```
show mp tcp-block
```

Command mode: All

```

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

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

```

Table 134. MP Specified TCP Statistics

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

## UDP Statistics

The following command displays UDP statistics:

```
show mp udp-block
```

**Command mode:** All

```

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

Mgmt Ports:
-----
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
udp      0      0 172.31.38.107:snmp      *:*
udp      0      0 172.31.38.107:bootpc    *:*

172.31.35.1             67 <=> 172.31.38.107         68 accept MGT up
172.25.160.114         40391 <=> 172.31.38.107        161 accept MGT up
  
```

## CPU Statistics

The following commands display CPU use statistics:

```
show mp cpu
```

**Command mode:** All

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

*Table 135. CPU Statistics*

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

Table 135. CPU Statistics

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

show processes cpu

**Command mode:** All

```

-----
Total CPU Utilization: For 1 second: 0.66%
                       For 5 second: 3.02%
                       For 1 minute: 3.73%
                       For 5 minute: 3.69%
Highest thread util   : 100% by  58 (I2C ) at 11:31:32 Sat Mar 10, 2012
-----
Thread  Thread          Utilization          Status
  ID    Name             1sec      5sec      1Min      5Min
-----
  1     STEM             0.00%    0.00%    0.00%    0.00%    idle
  2     STP               0.00%    0.00%    0.00%    0.00%    idle
  3     MFDB              0.00%    0.00%    0.00%    0.00%    idle
  4     TND               0.00%    0.00%    0.00%    0.00%    idle
  5     CONS              0.00%    0.01%    0.38%    0.08%    running
  6     TNET              0.00%    0.00%    0.00%    0.00%    idle
...
123    PBR               0.00%    0.00%    0.00%    0.00%    idle
124    HIST              0.00%    0.00%    0.00%    0.00%    idle
126    NORM              0.00%    0.00%    0.00%    0.00%    idle
127    DONE              0.00%    0.00%    0.00%    0.00%    idle
-----

```

Table 136. CPU Statistics

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



## CPU Statistics History

The following command displays a history of CPU use statistics:

```
show processes cpu history
```

**Command mode:** All

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

---

## QoS Statistics

Table 137. QoS Statistics Commands

Command Syntax and Usage
<pre>show qos protocol-packet-control protocol-counters &lt;packet type&gt;</pre> <p>Displays the total packet count of the selected packet type received by hardware.</p> <p><b>Command mode:</b> All</p>
<pre>show qos protocol-packet-control queue-counters</pre> <p>Displays the total number of packets received by each queue.</p> <p><b>Command mode:</b> All</p>
<pre>clear qos protocol-packet-control protocol-counters &lt;packet type&gt;</pre> <p>Clears packet queue statistics for the selected packet type.</p> <p><b>Command mode:</b> All</p>
<pre>clear qos protocol-packet-control queue-counters &lt;queue number&gt;</pre> <p>Clears packet queue statistics for the selected queue.</p> <p><b>Command mode:</b> All</p>
<pre>clear qos protocol-packet-control all</pre> <p>Clears all packet queue statistics.</p> <p><b>Command mode:</b> All</p>

## Access Control List Statistics

Table 138. ACL Statistics Commands

Command Syntax and Usage
<pre>show access-control list &lt;ACL number&gt; counters</pre> <p>Displays the Access Control List statistics for a specific ACL.  <b>Command mode:</b> All</p>
<pre>show access-control list6 &lt;ACL number&gt; counters</pre> <p>Displays the IPv6 ACL statistics for a specific ACL.  <b>Command mode:</b> All</p>
<pre>show access-control macl &lt;MACL number&gt; counters</pre> <p>Displays the ACL statistics for a specific management ACL (MACL).  <b>Command mode:</b> All</p>
<pre>show access-control counters</pre> <p>Displays all ACL statistics.  <b>Command mode:</b> All</p>
<pre>show access-control vmap {&lt;vmap number&gt;} counters</pre> <p>Displays VLAN Map statistics for the selected VMAP. For a sample display, see <a href="#">page 236</a>.  <b>Command mode:</b> All</p>
<pre>clear access-control list {&lt;ACL number&gt; all} counters</pre> <p>Clears ACL statistics.  <b>Command mode:</b> Privileged EXEC</p>
<pre>clear access-control list6 {&lt;ACL number&gt; all} counters</pre> <p>Clears IPv6 ACL statistics.  <b>Command mode:</b> Privileged EXEC</p>
<pre>clear access-control macl {&lt;ACL number&gt; all} counters</pre> <p>Clears Management ACL (MACL) statistics.  <b>Command mode:</b> Privileged EXEC</p>
<pre>clear access-control vmap {&lt;VMAP number&gt;} counters</pre> <p>Clears VLAN Map statistics.  <b>Command mode:</b> Privileged EXEC</p>

Table 138. ACL Statistics Commands (continued)

Command Syntax and Usage
<pre>show access-control meter &lt;meter number&gt; counters</pre> <p>Displays ACL meter statistics.</p> <p><b>Command mode:</b> All</p>
<pre>clear access-control meter &lt;meter number&gt; counters</pre> <p>Clears ACL meter statistics.</p> <p><b>Command mode:</b> Privileged EXEC</p>

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

Table 140. 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 140. SNMP Statistics (continued)

Statistic	Description
snmpInASNParseErrs	<p>The total number of ASN.1 or BER errors encountered by the SNMP protocol entity when decoding SNMP Messages received.</p> <p><b>Note:</b> 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.

Table 140. SNMP Statistics (continued)

Statistic	Description
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 <code>genErr</code> .
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 <code>too big</code> .
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 <code>noSuchName</code> .
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 <code>badValue</code> .
snmpOutReadOnly	Not in use.



Table 140. SNMP Statistics (continued)

Statistic	Description
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 <code>genErr</code> .
snmpOutGetRequests	The total number of SNMP Get-Request Protocol Data Units (PDUs), which have been generated by the SNMP protocol entity.
snmpOutGetNexts	The total number of SNMP Get-Next Protocol Data Units (PDUs), which have been generated by the SNMP protocol entity.
snmpOutSetRequests	The total number of SNMP Set-Request Protocol Data Units (PDUs), which have been generated by the SNMP protocol entity.
snmpOutGetResponses	The total number of SNMP Get-Response Protocol Data Units (PDUs), which have been generated by the SNMP protocol entity.
snmpOutTraps	The total number of SNMP Trap Protocol Data Units (PDUs), which have been generated by the SNMP protocol entity.
snmpSilentDrops	The total number of <code>GetRequest</code> -PDUs, <code>GetNextRequest</code> -PDUs, <code>GetBulkRequest</code> -PDUs, <code>SetRequest</code> -PDUs, and <code>InformRequest</code> -PDUs delivered to the OSPFSNMPv2 entity which were silently dropped because the size of a reply containing an alternate <code>Response</code> -PDU with an empty variable bindings field was greater than either a local constraint or the maximum message size associated with the originator of the request.
snmpProxyDrops	The total number of <code>GetRequest</code> -PDUs, <code>GetNextRequest</code> -PDUs, <code>GetBulkRequest</code> -PDUs, <code>SetRequest</code> -PDUs, and <code>InformRequest</code> -PDUs delivered to the SNMP entity which were silently dropped because the transmission of the message to a proxy target failed in a manner such that no <code>Response</code> -PDU could be returned.

---

## NTP Statistics

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

The following command displays NTP statistics:

```
show ntp counters
```

**Command mode:** All

```
NTP statistics:
  Primary Server:
    Requests Sent:           17
    Responses Received:      17
    Updates:                  1
  Secondary Server:
    Requests Sent:           0
    Responses Received:      0
    Updates:                  0
  Last update based on response from primary server.
  Last update time:         15:22:05 Wed Nov 28, 2012
  Current system time:      8:05:21 Thu Nov 29, 2012
```

Table 141. NTP Statistics

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

Table 141. NTP Statistics

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

The following command displays information about NTP associated peers:

```
show ntp associations
```

**Command mode:** All

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

Table 142. NTP Associations

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

---

## PTP Statistics

Table 143. Precision Time Protocol Statistics Commands

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

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

```
show ptp counters
```

**Command mode:** All

<pre>Precision time protocol counters: +-----+  Received Announce messages:          0   Received Sync messages:              0   Received Follow-Up messages:         0   Received Delay-Request messages:     0   Received Delay-Response messages:    0  +-----+  Sent Announce messages:              0   Sent Sync messages:                  0   Sent Follow-Up messages:             0   Sent Delay-Request messages:         0   Sent Delay-Response messages:        0  +-----+</pre>
--

PTP statistics include the following:

- Total number of Announce messages transmitted and received.
- Total number of Sync transmitted and received.
- Total number of Follow\_Up messages transmitted and received
- Total number of Delay\_Req messages transmitted and received
- Total number of Delay\_Resp messages transmitted and received

---

## 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 144. General Configuration Commands

Command Syntax and Usage
<pre>show running-config</pre> <p>Dumps current configuration to a script file. For details, see <a href="#">page 514</a>.</p> <p><b>Command mode:</b> Privileged EXEC</p>
<pre>show running-config diff</pre> <p>Displays running configuration changes that have been applied but not saved to flash memory.</p> <p><b>Command mode:</b> Privileged EXEC</p>
<pre>copy running-config backup-config</pre> <p>Copy the current (running) configuration from switch memory to the backup-config partition. For details, see <a href="#">page 515</a>.</p> <p><b>Command mode:</b> Privileged EXEC</p>
<pre>copy running-config startup-config</pre> <p>Copy the current (running) configuration from switch memory to the startup-config partition.</p> <p><b>Command mode:</b> Privileged EXEC</p>
<pre>write memory</pre> <p>Copy the current (running) configuration from switch memory to the active-config partition.</p> <p><b>Command mode:</b> Privileged EXEC</p>
<pre>copy running-config {ftp tftp sftp} [data-port mgt-port]</pre> <p>Backs up current configuration to a file on the selected FTP/TFTP/SFTP server.</p> <p><b>Command mode:</b> Privileged EXEC</p>

Table 144. General Configuration Commands

Command Syntax and Usage
<pre>copy {ftp tftp sftp} running-config [data-port mgt-port]</pre> <p>Restores current configuration from a FTP/TFTP/SFTP server.</p> <p><b>Command mode:</b> Privileged EXEC</p> <p>For details, see <a href="#">page 516</a>.</p>
<pre>copy {tftp sftp} {ca-cert host-key host-cert}</pre> <p>Import interface used by NIST certified test laboratories for USGv6 (NIST SP 500-267) certification purposes. Required for RSA digital signature authentication verification during IKEv2 interoperability testing. Uses TFTP or SFTP to import:</p> <ul style="list-style-type: none"><li>– ca-cert: Certificate Authority root certificate</li><li>– host-key: host private key</li><li>– host-cert: host public key</li></ul> <p><b>Command mode:</b> Privileged EXEC</p>



---

## Viewing and Saving Changes

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

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

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

### Saving the Configuration

You must save configuration settings to flash memory, so the 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 546](#).

---

## 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 145. System Configuration Options

Command Syntax and Usage	
<code>system date &lt;yyyy&gt; &lt;mm&gt; &lt;dd&gt;</code>	<p>Prompts the user for the system date. The date retains its value when the switch is reset.</p> <p><b>Command mode:</b> Global configuration</p>
<code>system time &lt;hh&gt;:&lt;mm&gt;:&lt;ss&gt;</code>	<p>Configures the system time using a 24-hour clock format. The time retains its value when the switch is reset.</p> <p><b>Command mode:</b> Global configuration</p>
<code>system timezone</code>	<p>Configures the time zone where the switch resides. You are prompted to select your location (continent, country, region) by the timezone wizard. Once a region is selected, the switch updates the time to reflect local changes to Daylight Savings Time, etc.</p> <p><b>Command mode:</b> Global configuration</p>
<code>[no] system daylight</code>	<p>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.</p> <p><b>Command mode:</b> Global configuration</p>
<code>terminal-length &lt;0-300&gt;</code>	<p>Configures the number of lines per screen displayed in the CLI for the current session. A value of 0 disables paging. By default, it is set to the corresponding <code>line vty length</code> or <code>line console length</code> value in effect at login.</p> <p><b>Command mode:</b> All</p>
<code>line console length &lt;0-300&gt;</code>	<p>Configures the number of lines per screen displayed in the CLI by default for console sessions. Setting it to 0 disables paging. The default value is 28.</p> <p><b>Command mode:</b> Global configuration</p>
<code>no line console</code>	<p>Sets <code>line console length</code> to the default value of 28.</p> <p><b>Command mode:</b> Global configuration</p>
<code>line vty length &lt;0-300&gt;</code>	<p>Sets the default number of lines per screen displayed for Telnet and SSH sessions. A value of 0 disables paging. The default value is 28.</p> <p><b>Command mode:</b> Global configuration</p>

Table 145. System Configuration Options (continued)

Command Syntax and Usage	
no line vty	<p>Sets line vty length to the default value of 28.</p> <p><b>Command mode:</b> Global configuration</p>
system idle <0-60>	<p>Sets the idle timeout for CLI sessions in minutes. The default value is 10 minutes. A value of 0 disables system idle.</p> <p><b>Command mode:</b> Global configuration</p>
system linkscan {normal   fast   slow}	<p>Configures the link scan interval used to poll the status of ports.</p> <p><b>Command mode:</b> Global configuration</p>
system notice <maximum 1024 character multi-line login notice> <'.' to end>	<p>Displays a login notice immediately before the "Enter password:" prompt. This notice can contain up to 1024 characters and new lines.</p> <p><b>Command mode:</b> Global configuration</p>
[no] banner <1-80 characters>	<p>Configures a login banner of up to 80 characters. When a user or administrator logs into the switch, the login banner is displayed. It is also displayed as part of the output from the <code>show sys-info</code> command.</p> <p><b>Command mode:</b> Global configuration</p>
[no] hostname <character string>	<p>Enables or disables displaying of the host name (system administrator's name) in the Command Line Interface (CLI).</p> <p><b>Command mode:</b> Global configuration</p>
[no] system bootp	<p>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.</p> <p><b>Command mode:</b> Global configuration</p>
[no] system default-ip {data mgt}	<p>Enables or disables default IP address on interface 1 and required management interfaces, if any. The default setting is enabled.</p> <p><b>Command mode:</b> Global configuration</p>
[no] system dhcp [hostname syslog]	<p>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.</p> <ul style="list-style-type: none"> <li>– hostname enables or disables hostname option support</li> <li>– syslog enables or disables log server option support</li> </ul> <p><b>Command mode:</b> Global configuration</p>

Table 145. System Configuration Options (continued)

<b>Command Syntax and Usage</b>	
<code>[no] system reset-control</code>	<p>Enables or disables the reset control flag. When enabled, the switch continues to function after a crash of the main processor, using the last known Layer 2/3 information.</p> <p><b>Command mode:</b> Global configuration</p>
<code>[no] system packet-logging</code>	<p>Enables or disables logging of packets that come to the CPU. The default setting is enabled.</p> <p><b>Command mode:</b> Global configuration</p>
<code>system usb-eject</code>	<p>Allows you to safely remove a USB drive from the USB port, without corrupting files on the drive.</p> <p><b>Command mode:</b> Global configuration</p>
<code>[no] boot strict enable</code>	<p>Enables or disables switch operation in security strict mode. When enabled, the authentication and privacy protocols and algorithms of the device are compliant with NIST SP-800-131A, with non-complaint protocols and algorithms disabled.</p> <p>Setting is applied and device is reset to default factory configuration after reboot.</p> <p>By default, this setting is disabled.</p> <p><b>Command mode:</b> Global configuration.</p>
<code>show boot strict</code>	<p>Displays the current security strict mode status.</p> <p><b>Command mode:</b> Global configuration</p>
<code>[no] system service-led</code>	<p>Enables (on) or disables (off) the Service Required LED on the front panel of the switch unit.</p> <p><b>Command mode:</b> Global configuration</p>
<code>show system</code>	<p>Displays the current system parameters.</p> <p><b>Command mode:</b> All</p>

## 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 146. Error Disable Configuration Options

Command Syntax and Usage	
<pre>errdisable timeout &lt;30 - 86400&gt;</pre>	<p>Configures the error-recovery timeout, in seconds. After the timer expires, the switch attempts to re-enable the port. The default value is 300.</p> <p><b>Note:</b> When you change the timeout value, all current error-recovery timers are reset.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>errdisable recovery</pre>	<p>Globally enables automatic error-recovery for error-disabled ports. The default setting is disabled.</p> <p><b>Note:</b> Each port must have error-recovery enabled to participate in automatic error recovery.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>no errdisable recovery</pre>	<p>Globally disables error-recovery for error-disabled ports; <code>errdisable recovery</code> is disabled globally by default.</p> <p><b>Command mode:</b> All</p>
<pre>show errdisable</pre>	<p>Displays the current system Error Disable configuration.</p> <p><b>Command mode:</b> All</p>

## 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 147. Link Flap Dampening Configuration Options

Command Syntax and Usage
<pre>errdisable link-flap max-flaps &lt;1-100&gt;</pre> <p>Configures the maximum number of link flaps allowed in the configured time period. The default value is 5.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>errdisable link-flap time &lt;5-500&gt;</pre> <p>Configures the time period, in seconds. The default value is 30 seconds.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>errdisable link-flap enable</pre> <p>Enables Link Flap Dampening.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>no errdisable link-flap enable</pre> <p>Disables Link Flap Dampening.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>show errdisable link-flap</pre> <p>Displays the current Link Flap Dampening parameters.</p> <p><b>Command mode:</b> All</p>

# System Host Log Configuration

Table 148. Host Log Configuration Options

Command Syntax and Usage	
[no] logging host <1-2> address <IP address>	<p>Sets the IP address of the first or second syslog host.</p> <p><b>Command mode:</b> Global configuration</p>
logging host <1-2> severity <0-7>	<p>This option sets the severity level of the first or second syslog host displayed. The default is 7, which means log all severity levels.</p> <p><b>Command mode:</b> Global configuration</p>
logging host <1-2> facility <0-7>	<p>This option sets the facility level of the first or second syslog host displayed. The default is 0.</p> <p><b>Command mode:</b> Global configuration</p>
logging source-interface <1-5>	<p>Sets the loopback interface number for syslogs.</p> <p><b>Command mode:</b> Global configuration</p>
logging console	<p>Enables delivering syslog messages to the console. It is enabled by default.</p> <p><b>Command mode:</b> Global configuration</p>
no logging console	<p>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.</p> <p><b>Command mode:</b> Global configuration</p>
[no] logging synchronous [level <0-7>   all]	<p>Enables or disables synchronous logging messages. When enabled, logging messages are displayed asynchronously.</p> <p>The level parameter sets the message severity level. Messages with a severity level equal to or higher than this value are displayed asynchronously. Low numbers indicate greater severity. All displays all messages asynchronously, regardless the severity level. The default setting is 2.</p> <p><b>Command mode:</b> Global configuration</p>
logging console severity <0-7>	<p>This option sets the severity level of syslog messages delivered via the console, telnet, and SSH. The system displays only messages with the selected severity level and above. For example, if you set the console severity to 2, only messages with severity level of 1 and 2 are displayed.</p> <p>The default is 7, which means log all severity levels.</p> <p><b>Command mode:</b> Global configuration</p>

Table 148. Host Log Configuration Options (continued)

Command Syntax and Usage	
<code>no logging console severity</code>	<p>Disables delivering syslog messages to the console based on severity.</p> <p><b>Command mode:</b> Global configuration</p>
<code>[no] logging log [&lt;feature&gt;]</code>	<p>Displays a list of features for which syslog messages can be generated. You can choose to enable/disable specific features (such as <code>vlangs</code>, <code>stg</code>, or <code>ssh</code>), or enable/disable syslog on all available features.</p> <p><b>Command mode:</b> Global configuration</p>
<code>logging buffer severity &lt;0-7&gt;</code>	<p>Sets the severity level of the syslog messages saved to flash memory. The default is 7, which means log all severity levels.</p> <p><b>Command mode:</b> Global configuration</p>
<code>show logging [severity &lt;severity level&gt;] [reverse]</code>	<p>Displays the current syslog settings, followed by the most recent 2000 syslog messages, as displayed by the <code>show logging messages</code> command. For details, see <a href="#">page 26</a>.</p> <p><b>Command mode:</b> All</p>



## SSH Server Configuration

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

Table 149. SSH Server Configuration Options

Command Syntax and Usage	
<code>ssh scp-password</code>	Set the administration password for SCP access. <b>Command mode:</b> Global configuration
<code>ssh generate-host-key</code>	Generate the RSA host key. <b>Command mode:</b> Global configuration
<code>ssh port &lt;TCP port number&gt;</code>	Sets the SSH server port number. <b>Command mode:</b> Global configuration
<code>ssh scp-enable</code>	Enables the SCP apply and save. <b>Command mode:</b> Global configuration
<code>no ssh scp-enable</code>	Disables the SCP apply and save. <b>Command mode:</b> Global configuration
<code>ssh enable</code>	Enables the SSH server. <b>Command mode:</b> Global configuration
<code>no ssh enable</code>	Disables the SSH server. <b>Command mode:</b> Global configuration
<code>show ssh</code>	Displays the current SSH server configuration. <b>Command mode:</b> All

# RADIUS Server Configuration

Table 150. RADIUS Server Configuration Options

Command Syntax and Usage	
[no] radius-server primary-host <IP address>	<p>Sets the primary RADIUS server address.</p> <p><b>Command mode:</b> Global configuration</p>
[no] radius-server secondary-host <IP address>	<p>Sets the secondary RADIUS server address.</p> <p><b>Command mode:</b> Global configuration</p>
radius-server primary-host <IP address> key <1-32 characters>	<p>This is the primary shared secret between the switch and the RADIUS server(s).</p> <p><b>Command mode:</b> Global configuration</p>
radius-server secondary-host <IP address> key <1-32 characters>	<p>This is the secondary shared secret between the switch and the RADIUS server(s).</p> <p><b>Command mode:</b> Global configuration</p>
[default] radius-server port <UDP port number>	<p>Enter the number of the UDP port to be configured, between 1500 - 3000. The default is 1645.</p> <p><b>Command mode:</b> Global configuration</p>
radius-server retransmit <1-3>	<p>Sets the number of failed authentication requests before switching to a different RADIUS server. The default is 3 requests.</p> <p><b>Command mode:</b> Global configuration</p>
radius-server timeout <1-10>	<p>Sets the amount of time, in seconds, before a RADIUS server authentication attempt is considered to have failed. The default is 3 seconds.</p> <p><b>Command mode:</b> Global configuration</p>
ip radius source-interface loopback <1-5>	<p>Sets the RADIUS source loopback interface.</p> <p><b>Command mode:</b> Global configuration</p>

Table 150. RADIUS Server Configuration Options (continued)

<b>Command Syntax and Usage</b>	
[no] radius-server backdoor	<p>Enables or disables the RADIUS backdoor for Telnet/SSH/HTTP/HTTPS. The default value is disabled.</p> <p>To obtain the RADIUS backdoor password for your switch, contact your Service and Support line.</p> <p><b>Command mode:</b> Global configuration</p>
[no] radius-server secure-backdoor	<p>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.</p> <p><b>Command mode:</b> Global configuration</p>
radius-server enable	<p>Enables the RADIUS server.</p> <p><b>Command mode:</b> Global configuration</p>
no radius-server enable	<p>Disables the RADIUS server.</p> <p><b>Command mode:</b> Global configuration</p>
show radius-server	<p>Displays the current RADIUS server parameters.</p> <p><b>Command mode:</b> All</p>

## TACACS+ Server Configuration

TACACS (Terminal Access Controller Access Control system) is an authentication protocol that allows a remote access server to forward a user's logon password to an authentication server to determine whether access can be allowed to a given system. TACACS is not an encryption protocol, and therefore less secure than TACACS+ and Remote Authentication Dial-In User Service (RADIUS) protocols. Both TACACS and TACACS+ are described in RFC 1492.

TACACS+ protocol is more reliable than RADIUS, as TACACS+ uses the Transmission Control Protocol (TCP) whereas RADIUS uses the User Datagram Protocol (UDP). Also, RADIUS combines authentication and authorization in a user profile, whereas TACACS+ separates the two operations.

TACACS+ offers the following advantages over RADIUS as the authentication device:

- TACACS+ is TCP-based, so it facilitates connection-oriented traffic.
- It supports full-packet encryption, as opposed to password-only in authentication requests.
- It supports de-coupled authentication, authorization, and accounting.

Table 151. TACACS+ Server Configuration Options

Command Syntax and Usage
<pre>[no] tacacs-server primary-host &lt;IP address&gt;</pre> <p>Defines the primary TACACS+ server address.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>[no] tacacs-server secondary-host &lt;IP address&gt;</pre> <p>Defines the secondary TACACS+ server address.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>[no] tacacs-server primary-host &lt;IP address&gt; key &lt;1-32 characters&gt;</pre> <p>This is the primary shared secret between the switch and the TACACS+ server(s).</p> <p><b>Command mode:</b> Global configuration</p>
<pre>[no] tacacs-server secondary-host &lt;IP address&gt; key &lt;1-32 characters&gt;</pre> <p>This is the secondary shared secret between the switch and the TACACS+ server(s).</p> <p><b>Command mode:</b> Global configuration</p>
<pre>[no] tacacs-server primary-host [data-port mgt-port]</pre> <p>Defines the primary interface port to use to send TACACS+ server requests. Select the port to use for data transfer.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>[no] tacacs-server secondary-host [data-port mgt-port]</pre> <p>Defines the secondary interface port to use to send TACACS+ server requests. Select the port to use for data transfer.</p> <p><b>Command mode:</b> Global configuration</p>

Table 151. TACACS+ Server Configuration Options (continued)

Command Syntax and Usage	
[no] tacacs-server chpassp <1-32 characters>	<p>Defines the password for the primary TACACS+ server.</p> <p><b>Command mode:</b> Global configuration</p>
[no] tacacs-server chpasss <1-32 characters>	<p>Defines the password for the secondary TACACS+ server.</p> <p><b>Command mode:</b> Global configuration</p>
[default] tacacs-server port <TCP port number>	<p>Enter the number of the TCP port to be configured, between 1 and 65000. The default is 49.</p> <p><b>Command mode:</b> Global configuration</p>
tacacs-server retransmit <1-3>	<p>Sets the number of failed authentication requests before switching to a different TACACS+ server. The default is 3 requests.</p> <p><b>Command mode:</b> Global configuration</p>
tacacs-server attempts <1-10>	<p>Sets the number of failed login attempts before disconnecting the user. The default is 2 attempts.</p> <p><b>Command mode:</b> Global configuration</p>
tacacs-server timeout <4-15>	<p>Sets the amount of time, in seconds, before a TACACS+ server authentication attempt is considered to have failed. The default is 5 seconds.</p> <p><b>Command mode:</b> Global configuration</p>
ip tacacs-server source-interface loopback <1-5>	<p>Sets the TACACS+ source loopback interface.</p> <p><b>Command mode:</b> Global configuration</p>
[no] tacacs-server user-mapping {<0-15> user oper admin}	<p>Maps a TACACS+ authorization level to a switch user level. Enter a TACACS+ authorization level (0-15), followed by the corresponding switch user level.</p> <p><b>Command mode:</b> Global configuration</p>

Table 151. TACACS+ Server Configuration Options (continued)

Command Syntax and Usage	
<pre>[no] tacacs-server backdoor</pre>	<p>Enables or disables the TACACS+ back door for Telnet, SSH/SCP, or HTTP/HTTPS.</p> <p>Enabling this feature allows you to bypass the TACACS+ servers. It is recommended that you use Secure Backdoor to ensure the switch is secured, because Secure Backdoor disallows access through the back door when the TACACS+ servers are responding.</p> <p>The default setting is disabled.</p> <p>To obtain the TACACS+ backdoor password for your G8264, contact your Service and Support line.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>[no] tacacs-server secure-backdoor</pre>	<p>Enables or disables TACACS+ secure back door access through Telnet, SSH/SCP, or HTTP/HTTPS only when the TACACS+ servers are not responding.</p> <p>This feature is recommended to permit access to the switch when the TACACS+ servers become unresponsive. If no back door is enabled, the only way to gain access when TACACS+ servers are unresponsive is to use the back door via the console port.</p> <p>The default is disabled.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>[no] tacacs-server privilege-mapping</pre>	<p>Enables or disables TACACS+ privilege-level mapping.</p> <p>The default value is disabled.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>[no] tacacs-server password-change</pre>	<p>Enables or disables TACACS+ password change.</p> <p>The default value is disabled.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>primary-password</pre>	<p>Configures the password for the primary TACACS+ server. The CLI will prompt you for input.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>secondary-password</pre>	<p>Configures the password for the secondary TACACS+ server. The CLI will prompt you for input.</p> <p><b>Command mode:</b> Global configuration</p>

Table 151. TACACS+ Server Configuration Options (continued)

Command Syntax and Usage	
[no] tacacs-server command-authorization	<p>Enables or disables TACACS+ command authorization.</p> <p><b>Command mode:</b> Global configuration</p>
[no] tacacs-server command-logging	<p>Enables or disables TACACS+ command logging.</p> <p><b>Command mode:</b> Global configuration</p>
[no] tacacs-server directed-request	<p>Enables or disables TACACS+ directed request, which uses a specified TACACS+ server for authentication, authorization, accounting. When enabled, When directed-request is enabled, each user must add a configured TACACS+ server hostname to the username (for example, username@hostname) during login.</p> <p>This command allows the following options:</p> <ul style="list-style-type: none"> <li>– Restricted: Only the username is sent to the specified TACACS+ server.</li> <li>– No-truncate: The entire login string is sent to the TACACS+ server.</li> </ul> <p><b>Command mode:</b> Global configuration</p>
[no] tacacs-server accounting-enable	<p>Enables or disables TACACS+ accounting.</p> <p><b>Command mode:</b> Global configuration</p>
[no] tacacs-server enable	<p>Enables or disables the TACACS+ server. By default, the server is disabled.</p> <p><b>Command mode:</b> Global configuration</p>
show tacacs-server	<p>Displays current TACACS+ configuration parameters.</p> <p><b>Command mode:</b> All</p>

## LDAP Server Configuration

LDAP (Lightweight Directory Access Protocol) is an authentication protocol that allows a remote access server to forward a user's logon password to an authentication server to determine whether access can be allowed to a given system.

Table 152. LDAP Server Configuration Options

Command Syntax and Usage	
[no] ldap-server primary-host <IP address> [data-port   mgt-port]	<p>Sets the primary LDAP server address.</p> <p><b>Command mode:</b> Global configuration</p>
[no] ldap-server secondary-host <IP address> [data-port   mgt-port]	<p>Sets the secondary LDAP server address.</p> <p><b>Command mode:</b> Global configuration</p>
[default] ldap-server port <UDP port number>	<p>Enter the number of the UDP port to be configured, between 1 - 65000. The default is 389.</p> <p><b>Command mode:</b> Global configuration</p>
ldap-server retransmit <1-3>	<p>Sets the number of failed authentication requests before switching to a different LDAP server. The default is 3 requests.</p> <p><b>Command mode:</b> Global configuration</p>
ldap-server timeout <4-15>	<p>Sets the amount of time, in seconds, before a LDAP server authentication attempt is considered to have failed. The default is 5 seconds.</p> <p><b>Command mode:</b> Global configuration</p>
ldap-server domain [<1-128 characters>   none]	<p>Sets the domain name for the LDAP server. Enter the full path for your organization. For example:</p> <p>ou=people,dc=mydomain,dc=com</p> <p><b>Command mode:</b> Global configuration</p>
[no] ldap-server backdoor	<p>Enables or disables the LDAP back door for Telnet, SSH/SCP, or HTTP/HTTPS. The default setting is disabled.</p> <p>To obtain the LDAP back door password for your G8264, contact your Service and Support line.</p> <p><b>Command mode:</b> Global configuration</p>



Table 152. LDAP Server Configuration Options (continued)

<b>Command Syntax and Usage</b>	
<code>ldap-server enable</code>	Enables the LDAP server. <b>Command mode:</b> Global configuration
<code>no ldap-server enable</code>	Disables the LDAP server. <b>Command mode:</b> Global configuration
<code>show ldap-server</code>	Displays the current LDAP server parameters. <b>Command mode:</b> All

## NTP Server Configuration

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

Table 153. NTP Server Configuration Options

Command Syntax and Usage	
<pre>[no] ntp primary-server {&lt;host name&gt;   &lt;IP address&gt;}</pre>	<p>Prompts for the hostname or IP addresses of the primary NTP server to which you want to synchronize the switch clock.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>[no] ntp ipv6 primary-server &lt;IPv6 address&gt;</pre>	<p>Prompts for the IPv6 addresses of the primary NTP server to which you want to synchronize the switch clock.</p> <p><b>Note:</b> To delete the IPv6 primary server, use the following command: <code>no ntp primary-server &lt;IP address&gt;</code></p> <p><b>Command mode:</b> Global configuration</p>
<pre>[no] ntp ipv6 secondary-server &lt;IPv6 address&gt;</pre>	<p>Prompts for the IPv6 addresses of the secondary NTP server to which you want to synchronize the switch clock.</p> <p><b>Note:</b> To delete the IPv6 secondary server, use the following command: <code>no ntp secondary-server &lt;IP address&gt;</code></p> <p><b>Command mode:</b> Global configuration</p>
<pre>[no] ntp secondary-server {&lt;host name&gt;   &lt;IP address&gt;}</pre>	<p>Prompts for the hostname or IP addresses of the secondary NTP server to which you want to synchronize the switch clock.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>[no] ntp sync-logs</pre>	<p>Enables or disables informational logs for NTP synchronization failures. Default setting is enabled.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>ntp offset &lt;0-86400&gt;</pre>	<p>Configures the minimum offset in seconds between the switch clock and the NTP server that triggers a system log message.</p> <p>The default value is 300.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>no ntp offset</pre>	<p>Resets the NTP offset to the default 300 seconds value.</p> <p><b>Command mode:</b> Global configuration</p>

Table 153. NTP Server Configuration Options (continued)

<b>Command Syntax and Usage</b>	
ntp interval <5-44640>	<p>Specifies the interval, that is, how often, in minutes, to re-synchronize the switch clock with the NTP server.</p> <p>The default value is 1440.</p> <p><b>Command mode:</b> Global configuration</p>
ntp source loopback <1-5>	<p>Sets the NTP source loopback interface.</p> <p><b>Command mode:</b> Global configuration</p>
ntp enable	<p>Enables the NTP synchronization service.</p> <p><b>Command mode:</b> Global configuration</p>
no ntp enable	<p>Disables the NTP synchronization service.</p> <p><b>Command mode:</b> Global configuration</p>
show ntp	<p>Displays the current NTP service settings.</p> <p><b>Command mode:</b> All</p>

## System SNMP Configuration

IBM N/OS supports SNMP-based network management. In SNMP model of network management, a management station (client/manager) accesses a set of variables known as MIBs (Management Information Base) provided by the managed device (agent). If you are running an SNMP network management station on your network, you can manage the switch using the following standard SNMP MIBs:

- MIB II (RFC 1213)
- Ethernet MIB (RFC 1643)
- Bridge MIB (RFC 1493)

An SNMP agent is a software process on the managed device that listens on UDP port 161 for SNMP messages. Each SNMP message sent to the agent contains a list of management objects to retrieve or to modify.

SNMP parameters that can be modified include:

- System name
- System location
- System contact
- Use of the SNMP system authentication trap function
- Read community string
- Write community string
- Trap community strings

Table 154. System SNMP Options

Command Syntax and Usage
<pre>snmp-server name &lt;1-64 characters&gt;</pre> <p>Configures the name for the system. The name can have a maximum of 64 characters.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>snmp-server location &lt;1-64 characters&gt;</pre> <p>Configures the name of the system location. The location can have a maximum of 64 characters.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>snmp-server contact &lt;1-64 characters&gt;</pre> <p>Configures the name of the system contact. The contact can have a maximum of 64 characters.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>snmp-server read-community &lt;1-32 characters&gt;</pre> <p>Configures the SNMP read community string. The read community string controls SNMP “get” access to the switch. It can have a maximum of 32 characters. The default read community string is <i>public</i>.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>[no] snmp-server read-community-additional &lt;1-32 characters&gt;</pre> <p>Adds or removes an additional SNMP read community string. Up to 7 additional read community strings are supported.</p> <p><b>Command mode:</b> Global configuration</p>

Table 154. System SNMP Options (continued)

Command Syntax and Usage	
[no] snmp-server write-community-additional <1-32 characters>	<p>Adds or removes an additional SNMP write community string. Up to 7 additional write community strings are supported.</p> <p><b>Command mode:</b> Global configuration</p>
snmp-server write-community <1-32 characters>	<p>Configures the SNMP write community string. The write community string controls SNMP “set” and “get” access to the switch. It can have a maximum of 32 characters. The default write community string is <i>private</i>.</p> <p><b>Command mode:</b> Global configuration</p>
snmp-server trap-source {<interface number> loopback <1-5>}	<p>Configures the source interface for SNMP traps.</p> <p>To send traps through the management ports, specify interface 126.</p> <p><b>Command mode:</b> Global configuration</p>
snmp-server host <trap host IP address> <trap host community string>	<p>Adds a trap host server.</p> <p><b>Command mode:</b> Global configuration</p>
no snmp-server host <trap host IP address>	<p>Removes the trap host server.</p> <p><b>Command mode:</b> Global configuration</p>
snmp-server timeout <1-30>	<p>Sets the timeout value for the SNMP state machine, in minutes.</p> <p><b>Command mode:</b> Global configuration</p>
[no] snmp-server authentication-trap	<p>Enables or disables the use of the system authentication trap facility. The default setting is disabled.</p> <p><b>Command mode:</b> Global configuration</p>
[no] snmp-server link-trap	<p>Enables or disables globally the sending of SNMP link up and link down traps. The default setting is enabled.</p> <p><b>Command mode:</b> Global configuration</p>
[no] snmp-server link-trap port <port alias or number>	<p>Enables or disables the sending of SNMP link up and link down traps for a specific system port. The default setting is disabled.</p> <p><b>Command mode:</b> Global configuration</p>
show snmp-server	<p>Displays the current SNMP configuration.</p> <p><b>Command mode:</b> All</p>

## SNMPv3 Configuration

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

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

For more details on the SNMPv3 architecture please refer to RFC3411 to RFC3418.

Table 155. SNMPv3 Configuration Options

Command Syntax and Usage
<pre>snmp-server user &lt;1-16&gt;</pre> <p>This command allows you to create a user security model (USM) entry for an authorized user. You can also configure this entry through SNMP.</p> <p><b>Command mode:</b> Global configuration</p> <p>To view command options, see <a href="#">page 272</a>.</p>
<pre>snmp-server view &lt;1-128&gt;</pre> <p>This command allows you to create different MIB views.</p> <p><b>Command mode:</b> Global configuration</p> <p>To view command options, see <a href="#">page 273</a>.</p>
<pre>snmp-server access &lt;1-32&gt;</pre> <p>This command allows you to specify access rights. The View-based Access Control Model defines a set of services that an application can use for checking access rights of the user. You need access control when you have to process retrieval or modification request from an SNMP entity.</p> <p><b>Command mode:</b> Global configuration</p> <p>To view command options, see <a href="#">page 274</a>.</p>
<pre>snmp-server group &lt;1-16&gt;</pre> <p>A group maps the user name to the access group names and their access rights needed to access SNMP management objects. A group defines the access rights assigned to all names that belong to a particular group.</p> <p><b>Command mode:</b> Global configuration</p> <p>To view command options, see <a href="#">page 275</a>.</p>
<pre>snmp-server community &lt;1-16&gt;</pre> <p>The community table contains objects for mapping community strings and version-independent SNMP message parameters.</p> <p><b>Command mode:</b> Global configuration</p> <p>To view command options, see <a href="#">page 276</a>.</p>

Table 155. SNMPv3 Configuration Options (continued)

<pre>snmp-server target-address &lt;I-16&gt;</pre> <p>This command allows you to configure destination information, consisting of a transport domain and a transport address. This is also termed as transport endpoint. The SNMP MIB provides a mechanism for performing source address validation on incoming requests, and for selecting community strings based on target addresses for outgoing notifications.</p> <p><b>Command mode:</b> Global configuration</p> <p>To view command options, see <a href="#">page 277</a>.</p>
<pre>snmp-server target-parameters &lt;I-16&gt;</pre> <p>This command allows you to configure SNMP parameters, consisting of message processing model, security model, security level, and security name information. There may be multiple transport endpoints associated with a particular set of SNMP parameters, or a particular transport endpoint may be associated with several sets of SNMP parameters.</p> <p><b>Command mode:</b> Global configuration</p> <p>To view command options, see <a href="#">page 278</a>.</p>
<pre>snmp-server notify &lt;I-16&gt;</pre> <p>A notification application typically monitors a system for particular events or conditions, and generates Notification-Class messages based on these events or conditions.</p> <p><b>Command mode:</b> Global configuration</p> <p>To view command options, see <a href="#">page 279</a>.</p>
<pre>snmp-server version {v1v2v3 v3only}</pre> <p>This command allows you to enable or disable the access to SNMP versions 1, 2 or 3. This command is enabled by default.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>show snmp-server v3</pre> <p>Displays the current SNMPv3 configuration.</p> <p><b>Command mode:</b> All</p>

## User Security Model Configuration

You can make use of a defined set of user identities using this Security Model. An SNMP engine must have the knowledge of applicable attributes of a user.

These commands help you create a user security model entry for an authorized user. You need to provide a security name to create the USM entry.

Table 156. User Security Model Configuration Options

Command Syntax and Usage
<pre>snmp-server user &lt;1-16&gt; name &lt;1-32 characters&gt;</pre> <p>This command allows you to configure a string that represents the name of the user. This is the login name that you need in order to access the switch.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>snmp-server user &lt;1-16&gt; authentication-protocol {md5 sha none} authentication-password &lt;password value&gt;</pre> <p>This command allows you to configure the authentication protocol and password.</p> <p>The authentication protocol can be HMAC-MD5-96 or HMAC-SHA-96 for compatibility mode, HMAC-SHA-96 for security strict mode, or none. The default algorithm is none.</p> <p>MD5 authentication protocol is not available in security strict mode if you do not select SNMPv3 account backward compatibility.</p> <p>When you configure an authentication algorithm, you must provide a password, otherwise you will get an error message during validation. This command allows you to create or change your password for authentication.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>snmp-server user &lt;1-16&gt; privacy-protocol {des aes none} privacy-password &lt;password value&gt;</pre> <p>This command allows you to configure the type of privacy protocol and the privacy password.</p> <p>The privacy protocol protects messages from disclosure. The options are <code>des</code> (CBC-DES Symmetric Encryption Protocol), <code>aes</code> (AES-128 Advanced Encryption Standard Protocol) or <code>none</code>. If you specify <code>des</code> as the privacy protocol, then make sure that you have selected one of the authentication protocols (MD5 or HMAC-SHA-96). In security strict mode, if you do not select SNMPv3 account backward compatibility, only <code>des</code> privacy protocol is supported. If you specify <code>aes</code> as the privacy protocol, make sure that you have selected HMAC-SHA-96 authentication protocol. If you select <code>none</code> as the authentication protocol, you will get an error message.</p> <p>You can create or change the privacy password.</p> <p><b>Command mode:</b> Global configuration</p>



Table 156. User Security Model Configuration Options

Command Syntax and Usage
<pre>no snmp-server user &lt;I-16&gt;</pre> <p>Deletes the USM user entries.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>show snmp-server v3 user &lt;I-16&gt;</pre> <p>Displays the USM user entries.</p> <p><b>Command mode:</b> All</p>

## SNMPv3 View Configuration

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

Table 157. SNMPv3 View Configuration Options

Command Syntax and Usage
<pre>snmp-server view &lt;I-128&gt; name &lt;I-32 characters&gt;</pre> <p>This command defines the name for a family of view subtrees.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>snmp-server view &lt;I-128&gt; tree &lt;I-64 characters&gt;</pre> <p>This command defines MIB tree, which when combined with the corresponding mask defines a family of view subtrees.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>[no] snmp-server view &lt;I-128&gt; mask &lt;I-32 characters&gt;</pre> <p>This command defines the bit mask, which in combination with the corresponding tree defines a family of view subtrees.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>snmp-server view &lt;I-128&gt; type {included excluded}</pre> <p>This command indicates whether the corresponding instances of <code>vacmViewTreeFamilySubtree</code> and <code>vacmViewTreeFamilyMask</code> define a family of view subtrees, which is included in or excluded from the MIB view.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>no snmp-server view &lt;I-128&gt;</pre> <p>Deletes the <code>vacmViewTreeFamily</code> group entry.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>show snmp-server v3 view &lt;I-128&gt;</pre> <p>Displays the current <code>vacmViewTreeFamily</code> configuration.</p> <p><b>Command mode:</b> All</p>

## 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 158. View-based Access Control Model Options

Command Syntax and Usage	
<code>snmp-server access &lt;1-32&gt; name &lt;1-32 characters&gt;</code>	<p>Defines the name of the group.</p> <p><b>Command mode:</b> Global configuration</p>
<code>snmp-server access &lt;1-32&gt; security {usm snmpv1 snmpv2}</code>	<p>Allows you to select the security model to be used.</p> <p><b>Command mode:</b> Global configuration</p>
<code>snmp-server access &lt;1-32&gt; level {noAuthNoPriv authNoPriv authPriv}</code>	<p>Defines the minimum level of security required to gain access rights. The level <code>noAuthNoPriv</code> means that the SNMP message will be sent without authentication and without using a privacy protocol. The level <code>authNoPriv</code> means that the SNMP message will be sent with authentication but without using a privacy protocol. The <code>authPriv</code> means that the SNMP message will be sent both with authentication and using a privacy protocol.</p> <p><b>Command mode:</b> Global configuration</p>
<code>snmp-server access &lt;1-32&gt; read-view &lt;1-32 characters&gt;</code>	<p>Defines a read view name that allows you read access to a particular MIB view. If the value is empty or if there is no active MIB view having this value then no access is granted.</p> <p><b>Command mode:</b> Global configuration</p>
<code>snmp-server access &lt;1-32&gt; write-view &lt;1-32 characters&gt;</code>	<p>Defines a write view name that allows you write access to the MIB view. If the value is empty or if there is no active MIB view having this value then no access is granted.</p> <p><b>Command mode:</b> Global configuration</p>
<code>snmp-server access &lt;1-32&gt; notify-view &lt;1-32 characters&gt;</code>	<p>Defines a notify view name that allows you notify access to the MIB view.</p> <p><b>Command mode:</b> Global configuration</p>
<code>no snmp-server access &lt;1-32&gt;</code>	<p>Deletes the View-based Access Control entry.</p> <p><b>Command mode:</b> Global configuration</p>
<code>show snmp-server v3 access &lt;1-32&gt;</code>	<p>Displays the View-based Access Control configuration.</p> <p><b>Command mode:</b> All</p>

## SNMPv3 Group Configuration

Table 159. SNMPv3 Group Configuration Options

Command Syntax and Usage
<pre>snmp-server group &lt;1-16&gt; security {usm snmpv1 snmpv2}</pre> <p>Defines the security model.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>snmp-server group &lt;1-16&gt; user-name &lt;1-32 characters&gt;</pre> <p>Sets the user name as defined in the following command on <a href="#">page 272</a>:</p> <pre>snmp-server user &lt;1-16&gt; name &lt;1-32 characters&gt;</pre> <p><b>Command mode:</b> Global configuration</p>
<pre>snmp-server group &lt;1-16&gt; group-name &lt;1-32 characters&gt;</pre> <p>The name for the access group as defined in the following command:</p> <pre>snmp-server access &lt;1-32&gt; name &lt;1-32 characters&gt;</pre> <p>on <a href="#">page 272</a>.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>no snmp-server group &lt;1-16&gt;</pre> <p>Deletes the vacmSecurityToGroup entry.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>show snmp-server v3 group &lt;1-16&gt;</pre> <p>Displays the current vacmSecurityToGroup configuration.</p> <p><b>Command mode:</b> All</p>

## SNMPv3 Community Table Configuration

These commands are used for configuring the community table entry. The configured entry is stored in the community table list in the SNMP engine. This table is used to configure community strings in the Local Configuration Datastore (LCD) of SNMP engine.

Table 160. SNMPv3 Community Table Configuration Options

Command Syntax and Usage
<pre>snmp-server community &lt;1-16&gt; index &lt;1-32 characters&gt;</pre> <p>Allows you to configure the unique index value of a row in this table.</p> <p><b>Command string:</b> Global configuration</p>
<pre>snmp-server community &lt;1-16&gt; name &lt;1-32 characters&gt;</pre> <p>Defines the user name as defined in the following command on <a href="#">page 272</a>: <pre>snmp-server user &lt;1-16&gt; name &lt;1-32 characters&gt;</pre></p> <p><b>Command string:</b> Global configuration</p>
<pre>snmp-server community &lt;1-16&gt; user-name &lt;1-32 characters&gt;</pre> <p>Defines a readable string that represents the corresponding value of an SNMP community name in a security model.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>snmp-server community &lt;1-16&gt; tag &lt;1-255 characters&gt;</pre> <p>Allows you to configure a tag. This tag specifies a set of transport endpoints to which a command responder application sends an SNMP trap.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>no snmp-server community &lt;1-16&gt;</pre> <p>Deletes the community table entry.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>show snmp-server v3 community &lt;1-16&gt;</pre> <p>Displays the community table configuration.</p> <p><b>Command mode:</b> All</p>

## SNMPv3 Target Address Table Configuration

These commands are used to configure the target transport entry. The configured entry is stored in the target address table list in the SNMP engine. This table of transport addresses is used in the generation of SNMP messages.

Table 161. Target Address Table Configuration Options

Command Syntax and Usage
<pre>snmp-server target-address &lt;1-16&gt; address &lt;IP address&gt; name &lt;1-32 characters&gt;</pre> <p>Allows you to configure the locally arbitrary, but unique identifier, target address name associated with this entry.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>snmp-server target-address &lt;1-16&gt; name &lt;1-32 characters&gt; address &lt;transport IP address&gt;</pre> <p>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.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>snmp-server target-address &lt;1-16&gt; port &lt;port range&gt;</pre> <p>Allows you to configure a transport address port that can be used in the generation of SNMP traps.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>snmp-server target-address &lt;1-16&gt; taglist &lt;1-255 characters&gt;</pre> <p>Allows you to configure a list of tags that are used to select target addresses for a particular operation.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>snmp-server target-address &lt;1-16&gt; parameters-name &lt;1-32 characters&gt;</pre> <p>Defines the name as defined in the following command on <a href="#">page 278</a>:  <pre>snmp-server target-parameters &lt;1-16&gt; name &lt;1-32 characters&gt;</pre></p> <p><b>Command mode:</b> Global configuration</p>
<pre>no snmp-server target-address &lt;1-16&gt;</pre> <p>Deletes the Target Address Table entry.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>show snmp-server v3 target-address &lt;1-16&gt;</pre> <p>Displays the current Target Address Table configuration.</p> <p><b>Command mode:</b> All</p>

## SNMPv3 Target Parameters Table Configuration

You can configure the target parameters entry and store it in the target parameters table in the SNMP engine. This table contains parameters that are used to generate a message. The parameters include the message processing model (for example: SNMPv3, SNMPv2c, SNMPv1), the security model (for example: USM), the security name, and the security level (`noAuthNoPriv`, `authNoPriv`, or `authPriv`).

Table 162. Target Parameters Table Configuration Options

Command Syntax and Usage	
<pre>snmp-server target-parameters &lt;1-16&gt; name &lt;1-32 characters&gt;</pre>	<p>Allows you to configure the locally arbitrary, but unique, identifier that is associated with this entry.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>snmp-server target-parameters &lt;1-16&gt; message {snmpv1   snmpv2c   snmpv3}</pre>	<p>Allows you to configure the message processing model that is used to generate SNMP messages.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>snmp-server target-parameters &lt;1-16&gt; security {usm   snmpv1   snmpv2}</pre>	<p>Allows you to select the security model to be used when generating the SNMP messages.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>snmp-server target-parameters &lt;1-16&gt; user-name &lt;1-32 characters&gt;</pre>	<p>Defines the name that identifies the user in the USM table (<a href="#">page 272</a>) on whose behalf the SNMP messages are generated using this entry.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>snmp-server target-parameters &lt;1-16&gt; level {noAuthNoPriv   authNoPriv   authPriv}</pre>	<p>Allows you to select the level of security to be used when generating the SNMP messages using this entry. The level <code>noAuthNoPriv</code> means that the SNMP message will be sent without authentication and without using a privacy protocol. The level <code>authNoPriv</code> means that the SNMP message will be sent with authentication but without using a privacy protocol. The <code>authPriv</code> means that the SNMP message will be sent both with authentication and using a privacy protocol.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>no snmp-server target-parameters &lt;1-16&gt;</pre>	<p>Deletes the <code>targetParamsTable</code> entry.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>show snmp-server v3 target-parameters &lt;1-16&gt;</pre>	<p>Displays the current <code>targetParamsTable</code> configuration.</p> <p><b>Command mode:</b> All</p>

## SNMPv3 Notify Table Configuration

SNMPv3 uses Notification Originator to send out traps. A notification typically monitors a system for particular events or conditions, and generates Notification-Class messages based on these events or conditions.

Table 163. Notify Table Options

Command Syntax and Usage
<pre>snmp-server notify &lt;1-16&gt; name &lt;1-32 characters&gt;</pre> <p>Defines a locally arbitrary, but unique, identifier associated with this SNMP notify entry.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>snmp-server notify &lt;1-16&gt; tag &lt;1-255 characters&gt;</pre> <p>Allows you to configure a tag that contains a tag value which is used to select entries in the Target Address Table. Any entry in the <code>snmpTargetAddrTable</code>, that matches the value of this tag, is selected.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>no snmp-server notify &lt;1-16&gt;</pre> <p>Deletes the notify table entry.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>show snmp-server v3 notify &lt;1-16&gt;</pre> <p>Displays the current notify table configuration.</p> <p><b>Command mode:</b> All</p>

---

## System Access Configuration

Table 164. System Access Configuration Options

Command Syntax and Usage
<pre>access user user-password</pre> <p>Sets the user (<code>user</code>) password. The user has no direct responsibility for switch management. The user view switch status information and statistics, but cannot make any configuration changes.</p> <p>This command will prompt for required information: current admin password, new password (up to 128 characters) and confirmation of the new password.</p> <p><b>Note:</b> To disable the user account, set the password to null (no password).</p> <p><b>Command Mode:</b> Global configuration</p>
<pre>access user operator-password</pre> <p>Sets the operator (<code>oper</code>) password. The operator manages all functions of the switch. The operator can view all switch information and statistics and can reset ports.</p> <p>This command will prompt for required information: current admin password, new password (up to 128 characters) and confirmation of the new password.</p> <p><b>Note:</b> To disable the operator account, set the password to null (no password). The default setting is disabled (no password).</p> <p><b>Command Mode:</b> Global configuration</p>
<pre>access user administrator-password</pre> <p>Sets the administrator (<code>admin</code>) password. The administrator has complete access to all menus, information, and configuration commands on the G8264, including the ability to change both the user and administrator passwords.</p> <p>This command will prompt for required information: current admin password, new password (up to 128 characters) and confirmation of the new password.</p> <p>Access includes “<code>oper</code>” functions.</p> <p><b>Note:</b> You cannot disable the administrator password.</p> <p><b>Command Mode:</b> Global configuration</p>
<pre>[no] access http enable</pre> <p>Enables or disables HTTP (Web) access to the Browser-Based Interface. It is enabled by default.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>[default] access http port [&lt;port alias or number&gt;]</pre> <p>Sets the switch port used for serving switch Web content. The default is HTTP port 80.</p> <p><b>Command mode:</b> Global configuration</p>



Table 164. System Access Configuration Options (continued)

<b>Command Syntax and Usage</b>	
[no] access snmp {read-only read-write}	Disables or provides read-only/write-read SNMP access. <b>Command mode:</b> Global configuration
[no] access telnet enable	Enables or disables Telnet access. This command is enabled by default. <b>Command mode:</b> 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. <b>Command mode:</b> Global configuration
[default] access tftp-port [<1-65535>]	Sets the TFTP port for the switch. The default is port 69. <b>Command mode:</b> Global configuration
[no] access tsbbi enable	Enables or disables Telnet/SSH configuration through the Browser-Based Interface (BBI). <b>Command mode:</b> Global configuration
[no] access userbbi enable	Enables or disables user configuration access through the Browser-Based Interface (BBI). <b>Command mode:</b> Global configuration
show access	Displays the current system access parameters. <b>Command mode:</b> All

## Management Network Configuration

These commands are used to define IP address ranges which are allowed to access the switch for management purposes.

Table 165. Management Network Configuration Options

Command Syntax and Usage	
<pre>access management-network &lt;mgmt network IPv4 or IPv6 address&gt; &lt;mgmt network mask or prefix length&gt;</pre>	<p>Adds a defined network through which switch access is allowed through Telnet, SNMP, RIP, or the IBM N/OS browser-based interface. A range of IP addresses is produced when used with a network mask address. Specify an IP address and mask address in dotted-decimal notation.</p> <p><b>Note:</b> If you configure the management network without including the switch interfaces, the configuration causes the Firewall Load Balancing health checks to fail and creates a “Network Down” state on the network.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>no access management-network &lt;mgmt network IPv4 or IPv6 address&gt; &lt;mgmt network mask or prefix length&gt;</pre>	<p>Removes a defined network, which consists of a management network address and a management network mask address.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>show access management-network</pre>	<p>Displays the current management network configuration.</p> <p><b>Command mode:</b> All except User EXEC</p>
<pre>clear access management-network</pre>	<p>Removes all defined management networks.</p> <p><b>Command mode:</b> Global configuration</p>

## 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 166. NETCONF Configuration Options

Command Syntax and Usage
<pre>[no] access netconf enable</pre> <p>Enables or disables NETCONF access to the switch.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>access netconf timeout &lt;30-3600&gt;</pre> <p>Configures the timeout value for NETCONF sessions, in seconds. The default value is 300 seconds.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>show access</pre> <p>Displays the current configuration.</p> <p><b>Command mode:</b> All</p>

## 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 167. NETCONF over SSH Configuration Options

Command Syntax and Usage
<pre>[no] access netconf ssh enable</pre> <p>Enables or disables NETCONF access over SSH.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>access netconf ssh port &lt;TCP port number&gt;</pre> <p>Configures the TCP port used for NETCONF. The default port number is 830.</p> <p><b>Command mode:</b> Global configuration</p>

## User Access Control Configuration

The following table describes user-access control commands.

Passwords can be a maximum of 128 characters.

Table 168. User Access Control Configuration Options

<b>Command Syntax and Usage</b>	
access user <1-20>	Configures the User ID. <b>Command mode:</b> Global configuration
access user eject {<user name> <session ID>}	Ejects the specified user from the G8264. <b>Command mode:</b> Global configuration
clear line <1-12>	Ejects the user with the corresponding session ID from the G8264. <b>Command mode:</b> Privileged EXEC
[no] access user administrator-enable	Enables or disables the default administrator account. <b>Command mode:</b> Global configuration
access user user-password	Sets the user ( <code>user</code> ) password. This command will prompt for required information: current admin password, new password (up to 128 characters) and confirmation of the new password. <b>Command mode:</b> Global configuration
access user operator-password	Sets the operator ( <code>oper</code> ) password. This command will prompt for required information: current admin password, new password (up to 128 characters) and confirmation of the new password. <b>Command mode:</b> Global configuration
access user administrator-password	Sets the administrator ( <code>admin</code> ) 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. <b>Command mode:</b> Global configuration
show access user	Displays the current user status. <b>Command mode:</b> All except User EXEC

## System User ID Configuration

Table 169. User ID Configuration Options

Command Syntax and Usage	
access user <1-20> level {user operator administrator}	<p>Sets the Class-of-Service to define the user's authority level. IBM N/OS defines these levels as: User, Operator, and Administrator, with User being the most restricted level.</p> <p><b>Command mode:</b> Global configuration</p>
access user <1-20> name <1-64 characters>	<p>Defines the user name of maximum eight characters.</p> <p><b>Command mode:</b> Global configuration</p>
access user <1-20> password	<p>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.</p> <p><b>Command mode:</b> Global configuration</p>
access user <1-20> enable	<p>Enables the user ID.</p> <p><b>Command mode:</b> Global configuration</p>
no access user <1-20> enable	<p>Disables the user ID.</p> <p><b>Command mode:</b> Global configuration</p>
no access user <1-20>	<p>Deletes the user ID.</p> <p><b>Command mode:</b> Global configuration</p>
show access user	<p>Displays the current user ID configuration.</p> <p><b>Command mode:</b> All except User EXEC</p>

## Strong Password Configuration

Table 170. Strong Password Configuration Options

Command Syntax and Usage
<pre>access user strong-password enable</pre> <p>Enables Strong Password requirement. <b>Command mode:</b> Global configuration</p>
<pre>no access user strong-password enable</pre> <p>Disables Strong Password requirement. <b>Command mode:</b> Global configuration</p>
<pre>access user strong-password expiry &lt;1-365&gt;</pre> <p>Configures the number of days allowed before the password must be changed. The default value is 60 days. <b>Command mode:</b> Global configuration</p>
<pre>access user strong-password warning &lt;1-365&gt;</pre> <p>Configures the number of days before password expiration, that a warning is issued to users. The default value is 15 days. <b>Command mode:</b> Global configuration</p>
<pre>access user strong-password faillog &lt;1-255&gt;</pre> <p>Configures the number of failed login attempts allowed before a security notification is logged. The default value is 3 login attempts. <b>Command mode:</b> Global configuration</p>
<pre>show access user strong-password</pre> <p>Displays the current Strong Password configuration. <b>Command mode:</b> All except User EXEC</p>

## HTTPS Access Configuration

Table 171. HTTPS Access Configuration Options

Command Syntax and Usage	
[no] access https enable	<p>Enables or disables BBI access (Web access) using HTTPS.</p> <p><b>Command mode:</b> Global configuration</p>
[default] access https port [ <i>&lt;TCP port number&gt;</i> ]	<p>Defines the HTTPS Web server port number. The default port is 443.</p> <p><b>Command mode:</b> Global configuration</p>
access https generate-certificate	<p>Allows you to generate a certificate to connect to the SSL to be used during the key exchange. A default certificate is created when HTTPS is enabled for the first time. The user can create a new certificate defining the information that they want to be used in the various fields. For example:</p> <ul style="list-style-type: none"> <li>– Country Name (2 letter code): CA</li> <li>– State or Province Name (full name): Ontario</li> <li>– Locality Name (for example, city): Ottawa</li> <li>– Organization Name (for example, company): Blade</li> <li>– Organizational Unit Name (for example, section): Operations</li> <li>– Common Name (for example, user's name): Mr Smith</li> <li>– Email (for example, email address): info@bladenetwork.net</li> </ul> <p>You will be asked to confirm if you want to generate the certificate. It will take approximately 30 seconds to generate the certificate. Then the switch will restart SSL agent.</p> <p><b>Command mode:</b> Global configuration</p>
access https save-certificate	<p>Allows the client, or the Web browser, to accept the certificate and save the certificate to Flash to be used when the switch is rebooted.</p> <p><b>Command mode:</b> Global configuration</p>
copy tftp ca-cert address <i>&lt;hostname or server-IP-addr&gt;</i> filename <i>&lt;server-filename&gt;</i>	<p>Enables you to import a certificate authority root certificate using TFTP.</p> <p><b>Command mode:</b> Global configuration</p>
copy tftp host-key address <i>&lt;hostname or server-IP-addr&gt;</i> filename <i>&lt;server-filename&gt;</i>	<p>Enables you to import a host private key using TFTP.</p> <p><b>Command mode:</b> Global configuration</p>

Table 171. HTTPS Access Configuration Options (continued)

Command Syntax and Usage
<pre>copy tftp host-cert address &lt;hostname or server-IP-addr&gt; filename &lt;server-filename&gt;</pre> <p>Enables you to import a host certificate using TFTP.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>show access</pre> <p>Displays the current SSL Web Access configuration.</p> <p><b>Command mode:</b> All except User EXEC</p>



## Custom Daylight Saving Time Configuration

Use these commands to configure custom Daylight Saving Time. The DST is defined by two rules, the start rule and end rule. The rules specify the dates when the DST starts and finishes. These dates are represented as specific calendar dates or as relative offsets in a month (for example, 'the second Sunday of September').

Relative offset example:

2070901 = Second Sunday of September, at 1:00 a.m.

Calendar date example:

0070901 = September 7, at 1:00 a.m.

Table 172. Custom DST Options

Command Syntax and Usage
<pre>system custom-dst start-rule &lt;WDDMMhh&gt;</pre> <p>Configures the start date for custom DST, as follows:</p> <p>WDDMMhh</p> <p>W = week (0-5, where 0 means use the calendar date)  D = day of the week (01-07, where 01 is Monday)  MM = month (1-12)  hh = hour (0-23)</p> <p><b>Note:</b> Week 5 is always considered to be the last week of the month.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>system custom-dst end-rule &lt;WDDMMhh&gt;</pre> <p>Configures the end date for custom DST, as follows:</p> <p>WDDMMhh</p> <p>W = week (0-5, where 0 means use the calendar date)  D = day of the week (01-07, where 01 is Monday)  MM = month (1-12)  hh = hour (0-23)</p> <p><b>Note:</b> Week 5 is always considered to be the last week of the month.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>system custom-dst enable</pre> <p>Enables the Custom Daylight Saving Time settings.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>no system custom-dst enable</pre> <p>Disables the Custom Daylight Saving Time settings.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>show custom-dst</pre> <p>Displays the current Custom DST configuration.</p> <p><b>Command mode:</b> All except User EXEC</p>

## sFlow Configuration

IBM N/OS supports sFlow version 5. sFlow is a sampling method used for monitoring high speed switched networks. Use these commands to configure the sFlow agent on the switch.

Table 173. sFlow Configuration Options

Command Syntax and Usage
<pre>sflow enable</pre> <p>Enables the sFlow agent.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>no sflow enable</pre> <p>Disables the sFlow agent.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>sflow server &lt;IP address&gt; [data-port mgt-port]</pre> <p>Defines the sFlow server address and interface port.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>sflow port &lt;1-65535&gt;</pre> <p>Configures the UDP port for the sFlow server. The default value is 6343.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>show sflow</pre> <p>Displays sFlow configuration parameters.</p> <p><b>Command mode:</b> All</p>

## sFlow Port Configuration

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

Table 174. sFlow Port Configuration Options

Command Syntax and Usage
<pre>[no] sflow polling &lt;5-60&gt;</pre> <p>Configures the sFlow polling interval, in seconds. The default setting is disabled.</p> <p><b>Command mode:</b> Interface port</p>
<pre>[no] sflow sampling &lt;256-65536&gt;</pre> <p>Configures the sFlow sampling rate, in packets per sample. The default setting is disabled.</p> <p><b>Command mode:</b> Interface port</p>

## 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 175. Server Port Configuration Options

Command Syntax and Usage
<pre>system server-ports port &lt;port alias or number&gt;</pre> <p>Adds one or more port physical ports to the list of server ports.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>no system server-ports port &lt;port alias or number&gt;</pre> <p>Removes one of more ports from the list of server ports.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>show system server-ports</pre> <p>Displays the current server port configuration.</p> <p><b>Command mode:</b> All</p>

---

## Port Configuration

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

Table 176. Port Configuration Options

Command Syntax and Usage
<pre>interface port &lt;port alias or number&gt;</pre> <p>Enter Interface port mode.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>interface portchannel &lt;trunk number&gt; lacp &lt;1-65535&gt;</pre> <p>Enter Interface portchannel mode. These commands allow you to configure port parameters for all port members in the selected trunk group (portchannel).</p> <p><b>Command mode:</b> Global configuration</p>
<pre>dot1p &lt;0-7&gt;</pre> <p>Configures the port's 802.1p priority level.</p> <p><b>Command mode:</b> Interface port/Interface portchannel</p>
<pre>description &lt;1-64 characters&gt;</pre> <p>Sets a description for the port. The assigned port description appears next to the port number on some information and statistics screens. The default is set to the port number.</p> <p><b>Command mode:</b> Interface port/Interface portchannel</p>
<pre>[no] bpdu-guard</pre> <p>Enables or disables BPDU guard, to avoid Spanning-Tree loops on ports configured as edge ports.</p> <p><b>Command mode:</b> Interface port/Interface portchannel</p>
<pre>[no] dscp-marking</pre> <p>Enables or disables DSCP re-marking on a port.</p> <p><b>Command mode:</b> Interface port/Interface portchannel</p>
<pre>[no] reflective-relay force</pre> <p>Enables or disables constraint to always keep reflective relay active. Default setting is disabled.</p> <p><b>Command mode:</b> Interface port</p>
<pre>[no] switchport</pre> <p>Enables or disables routing on a port.</p> <p><b>Command mode:</b> Interface port/Interface portchannel</p>

Table 176. Port Configuration Options (continued)

Command Syntax and Usage	
<pre>switchport mode {access trunk private-vlan}</pre>	<p>Configures the port's trunking mode:</p> <ul style="list-style-type: none"> <li>– <code>access</code> allows association to a single VLAN</li> <li>– <code>trunk</code> allows association to multiple VLANs</li> <li>– <code>private-vlan</code> allows association to a private VLAN</li> </ul> <p>Default mode is <code>access</code>.</p> <p><b>Note:</b> When switching from <code>access</code> to <code>trunk</code> mode, the port inherits the access VLAN as the trunk Native-VLAN.</p> <p><b>Note:</b> When switching from <code>trunk</code> to <code>access</code> mode, the port inherits the trunk Native-VLAN as the access VLAN.</p> <p><b>Command mode:</b> Interface port/Interface portchannel</p>
<pre>switchport access vlan &lt;1-4094&gt;</pre>	<p>Configures the associated VLAN used in access mode. If the VLAN does not exist, it will be created and enabled automatically. Default value is 1 for data ports and 4095 for the management port.</p> <p><b>Command mode:</b> Interface port/Interface portchannel</p>
<pre>no switchport access vlan</pre>	<p>Resets the access VLAN to its default value.</p> <p><b>Command mode:</b> Interface port/Interface portchannel</p>
<pre>switchport trunk native vlan &lt;1-4094&gt;</pre>	<p>Configures the Port VLAN ID (PVID) or Native-VLAN used to carry untagged traffic in trunk mode. If the VLAN does not exist, it will be created and enabled automatically. Default value is 1 for data ports and 4095 for the management port.</p> <p><b>Command mode:</b> Interface port/Interface portchannel</p>
<pre>switchport trunk allowed vlan [add remove] &lt;VLAN ID range&gt;</pre>	<p>Updates the associated VLANs in trunk mode. If any VLAN in the range does not exist, it will be created and enabled automatically.</p> <ul style="list-style-type: none"> <li>– <code>add</code> enables the VLAN range in addition to the current configuration</li> <li>– <code>remove</code> eliminates the VLAN range from the current configuration</li> </ul> <p><b>Command mode:</b> Interface port/Interface portchannel</p>
<pre>switchport trunk allowed vlan {all none}</pre>	<ul style="list-style-type: none"> <li>– <code>all</code> associates all existing and enabled VLANs to the port. This is an operational command applicable only to VLANs currently configured at the moment of execution. VLANs created afterward will not be associated automatically. Also, as an operational command, it will not be dumped into the configuration file.</li> <li>– <code>none</code> removes the port from all currently associated VLANs except the default VLAN</li> </ul> <p><b>Command mode:</b> Interface port/Interface portchannel</p>

Table 176. Port Configuration Options (continued)

Command Syntax and Usage	
[no] switchport private-vlan mapping <primary VLAN>	<p>Enables or disables private VLAN mapping on a port in promiscuous mode.</p> <p><b>Command mode:</b> Interface port/Interface portchannel</p>
[no] switchport private-vlan host-association <primary VLAN> <secondary VLAN>	<p>Enables or disables the private VLAN association on a secondary port.</p> <p><b>Command mode:</b> Interface port/Interface portchannel</p>
[no] vlan dot1q tag native	<p>Disables or enables VLAN tag persistence. When disabled, the VLAN tag is removed at egress from packets whose VLAN tag matches the port PVID/Native-vlan. The default setting is disabled.</p> <p><b>Note:</b> In global configuration mode, this is an operational command used to set the VLAN tag persistence on all ports currently tagged at the moment of execution. VLAN tag persistence will not be set automatically for ports tagged afterwards. Also, as an operational command, it will not be dumped into the configuration file.</p> <p><b>Command mode:</b> Global configuration/Interface port/Interface portchannel</p>
[no] tagpvid-ingress	<p>Enables or disables tagging the ingress frames with the port's VLAN ID. When enabled, the PVID tag is inserted into untagged and 802.1Q single-tagged ingress frames as outer VLAN ID. The default setting is disabled.</p> <p><b>Command mode:</b> Interface port/Interface portchannel</p>
[no] flood-blocking	<p>Enables or disables port Flood Blocking. When enabled, unicast and multicast packets with unknown destination MAC addresses are blocked from the port.</p> <p><b>Command mode:</b> Interface port/Interface portchannel</p>
[no] mac-address-table mac-notification	<p>Enables or disables MAC Address Notification. With MAC Address Notification enabled, the switch generates a syslog message when a MAC address is added or removed from the MAC address table.</p> <p><b>Command mode:</b> Interface port/Interface portchannel</p>
[no] learning	<p>Enables or disables FDB learning on the port.</p> <p><b>Command mode:</b> Interface port/Interface portchannel</p>
port-channel min-links <1-8>	<p>Set the minimum number of links for this port. If the specified minimum number of ports are not available, the trunk is placed in the down state.</p> <p><b>Command mode:</b> Interface port</p>

Table 176. Port Configuration Options (continued)

Command Syntax and Usage	
storm-control {broadcast multicast unicast} level pps <0-2097151>	Limits the number of broadcast, multicast or unicast packets per second to the specified value. <b>Command mode:</b> Interface port/Interface portchannel
no storm-control {broadcast multicast unicast}	Sets the port to forward all broadcast, multicast or unicast packets. <b>Command mode:</b> Interface port/Interface portchannel
[no] ip dhcp snooping trust	Configures this port as a trusted port for DHCP packets from the server. <b>Command mode:</b> Interface port
ip dhcp snooping limit rate <1-2048>	Configures the maximum number of DHCP packets allowed per second. <b>Command mode:</b> Interface port
[no] openflow edgeport <port numbers>	Enables or disables OpenFlow edge state for the ports. <b>Command mode:</b> Privileged EXEC
[no] openflow mgmtport <port numbers>	Enables or disables OpenFlow management state for the ports. <b>Command mode:</b> Global Configuration
no shutdown	Enables the port. <b>Command mode:</b> Interface port/Interface portchannel
shutdown	Disables the port. (To temporarily disable a port without changing its configuration attributes, refer to <a href="#">“Temporarily Disabling a Port” on page 298.</a> ) <b>Command mode:</b> Interface port/Interface portchannel
show interface port <port alias or number>	Displays current port parameters. <b>Command mode:</b> 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 177. Port Error Disable Options

Command Syntax and Usage
<pre>errdisable recovery</pre> <p>Enables automatic error-recovery for the port. The default setting is enabled.</p> <p><b>Note:</b> Error-recovery must be enabled globally before port-level commands become active.</p> <p><b>Command mode:</b> Interface port</p>
<pre>no errdisable recovery</pre> <p>Enables automatic error-recovery for the port.</p> <p><b>Command mode:</b> Interface port</p>
<pre>show interface port &lt;port alias or number&gt; errdisable</pre> <p>Displays current port Error Disable parameters.</p> <p><b>Command mode:</b> All</p>

## Port Link Flap Dampening Configuration

Table 178. Port Link Flap Dampening Configuration Options

Command Syntax and Usage
<pre>errdisable link-flap enable</pre> <p>Enables Link Flap Dampening on the port. For more information, see <a href="#">“Link Flap Dampening Configuration”</a> on page 254.</p> <p><b>Command mode:</b> Interface port</p>
<pre>no errdisable link-flap enable</pre> <p>Disables Link Flap Dampening on the port.</p> <p><b>Command mode:</b> Interface port</p>
<pre>show interface port errdisable &lt;port alias or number&gt; link-flap</pre> <p>Displays the current Link Flap Dampening parameters for the port.</p> <p><b>Command mode:</b> All</p>



## Port Link Configuration

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

Table 179. Port Link Configuration Options

Command Syntax and Usage
<pre>duplex {full half auto}</pre> <p>Sets the operating mode. The choices include:</p> <ul style="list-style-type: none"> <li>– “Auto negotiation (default)</li> <li>– Half-duplex</li> <li>– Full-duplex</li> </ul> <p><b>Note:</b> Data ports are fixed at full duplex.</p> <p><b>Command mode:</b> Interface port/Interface portchannel</p>
<pre>flowcontrol receive {on off}</pre> <p>Enables or disables flow control receive.</p> <p><b>Command mode:</b> Interface port/Interface portchannel</p>
<pre>flowcontrol send {on off}</pre> <p>Enables or disables flow control transmit.</p> <p><b>Command mode:</b> Interface port/Interface portchannel</p>
<pre>[no] auto</pre> <p>Turns auto-negotiation on or off.</p> <p><b>Note:</b> Data ports are fixed at 10000 Mbps, and cannot be set to auto-negotiate, unless a 1 Gb SFP transceiver is used.</p> <p><b>Command mode:</b> Interface port/Interface portchannel</p>
<pre>show interface port &lt;port alias or number&gt;</pre> <p>Displays current port parameters.</p> <p><b>Command mode:</b> All</p>

## Temporarily Disabling a Port

To temporarily disable a port without changing its stored configuration attributes, enter the following command at any prompt:

```
Router# interface port <port alias or number> shutdown
```

Because this configuration sets a temporary state for the port, you do not need to use a save operation. The port state will revert to its original configuration when the RackSwitch G8264 is reset. See the [“Operations Commands” on page 525](#) for other operations-level commands.

## UniDirectional Link Detection Configuration

UDLD commands are described in the following table.

Table 180. Port UDLD Configuration Options

Command Syntax and Usage
<pre>[no] udld</pre> <p>Enables or disables UDLD on the port.</p> <p><b>Command mode:</b> Interface port</p>
<pre>[no] udld aggressive</pre> <p>Configures the UDLD mode for the selected port, as follows:</p> <ul style="list-style-type: none"><li>– <b>Normal:</b> 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.</li><li>– <b>Aggressive:</b> In addition to the normal mode, the aggressive mode disables the port if the neighbor stops sending UDLD probes for 7 seconds.</li></ul> <p><b>Command mode:</b> Interface port</p>
<pre>show interface port &lt;port number&gt; udld</pre> <p>Displays current port UDLD parameters.</p> <p><b>Command mode:</b> All</p>

## Port OAM Configuration

Operation, Administration, and Maintenance (OAM) protocol allows the switch to detect faults on the physical port links. OAM is described in the IEEE 802.3ah standard. OAM Discovery commands are described in the following table.

Table 181. Port OAM Configuration Options

Command Syntax and Usage
<pre>oam {active passive}</pre> <p>Configures the OAM discovery mode, as follows:</p> <ul style="list-style-type: none"><li>– Active: This port link initiates OAM discovery.</li><li>– Passive: This port allows its peer link to initiate OAM discovery.</li></ul> <p>If OAM determines that the port is in an anomalous condition, the port is disabled.</p> <p><b>Command mode:</b> Interface port/</p>
<pre>no oam {active passive}</pre> <p>Disables OAM discovery on the port.</p> <p><b>Command mode:</b> Interface port</p>
<pre>show interface port &lt;port number&gt; oam</pre> <p>Displays current port OAM parameters.</p> <p><b>Command mode:</b> All</p>

## Port ACL Configuration

Table 182. ACL/QoS Configuration Options

Command Syntax and Usage
<pre>access-control list &lt;ACL number&gt;</pre> <p>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.</p> <p><b>Command mode:</b> Interface port/Interface portchannel</p>
<pre>no access-control list &lt;ACL number&gt;</pre> <p>Removes the specified ACL list from the port.</p> <p><b>Command mode:</b> Interface port/Interface portchannel</p>
<pre>access-control list6 &lt;ACL number&gt;</pre> <p>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.</p> <p><b>Command mode:</b> Interface port/Interface portchannel</p>
<pre>no access-control list6 &lt;ACL number&gt;</pre> <p>Removes the specified IPv6 ACL list from the port.</p> <p><b>Command mode:</b> Interface port/Interface portchannel</p>
<pre>access-control group &lt;ACL group number&gt;</pre> <p>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.</p> <p><b>Command mode:</b> Interface port/Interface portchannel</p>
<pre>no access-control group &lt;ACL group number&gt;</pre> <p>Removes the specified ACL group from the port.</p> <p><b>Command mode:</b> Interface port/Interface portchannel</p>
<pre>show interface port &lt;port alias or number&gt; access-control</pre> <p>Displays current ACL QoS parameters.</p> <p><b>Command mode:</b> All</p>

## Port WRED Configuration

These commands allow you to configure Weighted Random Early Detection (WRED) parameters for a selected port. For global WRED configuration, see [“Weighted Random Early Detection Configuration” on page 309](#).

Table 183. Port WRED Options

Command Syntax and Usage
<pre>[no] random-detect ecn enable</pre> <p>Enables or disables Explicit Congestion Notification (ECN). When ECN is on, the switch marks the ECN bit of the packet (if applicable) instead of dropping the packet. ECN-aware devices are notified of the congestion and those devices can take corrective actions.</p> <p><b>Note:</b> ECN functions only on TCP traffic.</p> <p><b>Command mode:</b> Interface port</p>
<pre>random-detect enable</pre> <p>Turns on Random Detection and avoidance.</p> <p><b>Command mode:</b> Interface port</p>
<pre>no random-detect enable</pre> <p>Turns off Random Detection and avoidance.</p> <p><b>Command mode:</b> Interface port</p>
<pre>show interface port &lt;port alias or number&gt; random-detect</pre> <p>Displays current Random Detection and avoidance parameters.</p> <p><b>Command mode:</b> All</p>

## Port WRED Transmit Queue Configuration

Use this menu to define WRED thresholds for the port’s transmit queues. Set each threshold between 1% and 100%. When the average queue size grows beyond the minimum threshold, packets begin to be dropped. When the average queue size reaches the maximum threshold, all packets are dropped. The probability of packet-drop between the thresholds is defined by the drop rate.

Table 184. Port WRED Transmit Queue Options

Command Syntax and Usage
<pre>[no] random-detect transmit-queue &lt;0-7&gt; tcp &lt;min. threshold (1-100)&gt; &lt;max. threshold (1-100)&gt; &lt;drop rate (1-100)&gt;</pre> <p>Configures the WRED thresholds for TCP traffic. Use the <code>no</code> form to clear the WRED threshold value.</p> <p><b>Command mode:</b> Interface port</p>
<pre>[no] random-detect transmit-queue &lt;0-7&gt; non-tcp &lt;min. threshold (1-100)&gt; &lt;max. threshold (1-100)&gt; &lt;drop rate (1-100)&gt;</pre> <p>Configures the WRED thresholds for non-TCP traffic. Use the <code>no</code> form to clear the WRED threshold value.</p> <p><b>Command mode:</b> Interface port</p>

Table 184. Port WRED Transmit Queue Options

Command Syntax and Usage
<pre>random-detect transmit-queue &lt;0-7&gt; enable</pre> <p>Sets the WRED transmit queue configuration to <code>on</code>.</p> <p><b>Command mode:</b> Interface port</p>
<pre>no random-detect transmit-queue &lt;0-7&gt; enable</pre> <p>Sets the WRED transmit queue configuration to <code>off</code>.</p> <p><b>Command mode:</b> Interface port</p>

---

## Stacking Configuration

A *stack* is a group of switches that work together as a unified system. The network views a stack of switches as a single entity, identified by a single network IP address. The Stacking Configuration commands are used to configure a stack, and to define the Master and Backup interface that represents the stack on the network.

The Stacking Configuration commands are available only after Stacking is enabled and the switch is reset. For more information, see [“Stacking Configuration” on page 303](#).

Table 185. Stacking Configuration Options

Command Syntax and Usage
<pre>[no] stack name &lt;1-63 characters&gt;</pre> <p>Defines a name for the stack.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>[no] stack backup &lt;csnum (1-8)&gt;</pre> <p>Defines the backup switch in the stack, based on its configured switch number (csnum).</p> <p><b>Command mode:</b> Global configuration</p>
<pre>show stack switch-number &lt;csnum (1-8)&gt;</pre> <p>Displays the current stacking parameters.</p> <p><b>Command mode:</b> All</p>

## Stacking Switch Configuration

Table 186. Stacking Switch Options

Command Syntax and Usage
<pre>stack switch-number &lt;csnum (1-8)&gt; bind &lt;asnum (1-8)&gt;</pre> <p>Binds the selected switch to the stack, based on its attached switch number (asnum).</p> <p><b>Note:</b> Binding the switch to a stack resets port numbering.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>stack switch-number &lt;csnum (1-8)&gt; mac &lt;MAC address&gt;</pre> <p>Binds the selected switch to the stack, based on its MAC address.</p> <p><b>Note:</b> Binding the switch to a stack resets port numbering.</p> <p><b>Command mode:</b> Global configuration</p>

Table 186. Stacking Switch Options

Command Syntax and Usage
<pre>no stack switch-number &lt;csnum (1-8)&gt;</pre> <p>Deletes the selected switch from the stack.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>show stack attached-switches</pre> <p>Displays the current stacking switch parameters.</p> <p><b>Command mode:</b> Global configuration</p>



---

## Quality of Service Configuration

Quality of Service (QoS) commands configure the 802.1p priority value and DiffServ Code Point value of incoming packets. This allows you to differentiate between various types of traffic, and provide different priority levels.

### 802.1p Configuration

This feature provides the 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 187. 802.1p Configuration Options

Command Syntax and Usage
<pre>qos transmit-queue mapping &lt;priority (0-7)&gt; &lt;COSq number&gt;</pre> <p>Maps the 802.1p priority of to the Class of Service queue (COSq) priority. Enter the 802.1p priority value (0-7), followed by the Class of Service queue that handles the matching traffic.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>qos transmit-queue weight-cos &lt;COSq number&gt; &lt;weight (0-15)&gt;</pre> <p>Configures the weight of the selected Class of Service queue (COSq). Enter the queue number (0-1), followed by the scheduling weight (0-15).</p> <p><b>Command mode:</b> Global configuration</p>
<pre>show qos transmit-queue</pre> <p>Displays the current 802.1p parameters.</p> <p><b>Command mode:</b> All</p>

## DSCP Configuration

These commands map the DiffServ Code Point (DSCP) value of incoming packets to a new value or to an 802.1p priority value.

Table 188. DSCP Configuration Options

Command Syntax and Usage
<pre>qos dscp dscp-mapping &lt;DSCP (0-63)&gt; &lt;new DSCP (0-63)&gt;</pre> <p>Maps the initial DiffServ Code Point (DSCP) value to a new value. Enter the DSCP value (0-63) of incoming packets, followed by the new value.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>qos dscp dot1p-mapping &lt;DSCP (0-63)&gt; &lt;priority (0-7)&gt;</pre> <p>Maps the DiffServ Code point value to an 802.1p priority value. Enter the DSCP value, followed by the corresponding 802.1p value.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>qos dscp re-marking</pre> <p>Turns on DSCP re-marking globally.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>no qos dscp re-marking</pre> <p>Turns off DSCP re-marking globally.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>show qos dscp</pre> <p>Displays the current DSCP parameters.</p> <p><b>Command mode:</b> All</p>

## 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 189. Control Plane Protection Options

Command Syntax and Usage
<pre>qos protocol-packet-control packet-queue-map &lt;packet queue number (0-40)&gt; &lt;packet type&gt;</pre>
<p>Configures a packet type to associate with each packet queue number. Enter a queue number, followed by the packet type. You may map multiple packet types to a single queue. The following packet types are allowed:</p>
<ul style="list-style-type: none"><li>– <b>802.1x</b> (IEEE 802.1x packets)</li><li>– <b>application-cri-packets</b> (critical packets of various applications, such as telnet,ssh)</li><li>– <b>arp-bcast</b> (ARP broadcast packets)</li><li>– <b>arp-ucast</b> (ARP unicast reply packets)</li><li>– <b>bgp</b> (BGP packets)</li><li>– <b>bpdu</b> (Spanning Tree Protocol packets)</li><li>– <b>cisco-bpdu</b> (Cisco STP packets)</li><li>– <b>dest-unknown</b> (packets with destination not yet learned)</li><li>– <b>dhcp</b> (DHCP packets)</li><li>– <b>icmp</b> (ICMP packets)</li><li>– <b>igmp</b> (IGMP packets)</li><li>– <b>ipv4-miscellaneous</b> (IPv4 packets with IP options and TTL exception)</li><li>– <b>ipv6-nd</b> (IPv6 Neighbor Discovery packets)</li><li>– <b>lACP</b> (LACP/Link Aggregation protocol packets)</li><li>– <b>lldp</b> (LLDP packets)</li><li>– <b>ospf</b> (OSPF packets)</li><li>– <b>ospf3</b> (OSPF3 Packets)</li><li>– <b>pim</b> (PIM packets)</li><li>– <b>rip</b> (RIP packets)</li><li>– <b>system</b> (system protocols, such as tftp, ftp, telnet, ssh)</li><li>– <b>udld</b> (UDLD packets)</li><li>– <b>vlag</b> (VLAG packets)</li><li>– <b>vrrp</b> (VRRP packets)</li></ul>
<p><b>Command mode:</b> Global configuration</p>

Table 189. Control Plane Protection Options (continued)

Command Syntax and Usage
<pre>qos protocol-packet-control rate-limit-packet-queue &lt;packet queue number (0-40)&gt; &lt;1-10000&gt;</pre> <p>Configures the number of packets per second allowed for each packet queue.  <b>Command mode:</b> Global configuration</p>
<pre>no qos protocol-packet-control packet-queue-map &lt;packet type&gt;</pre> <p>Clears the selected packet type from its associated packet queue.  <b>Command mode:</b> Global configuration</p>
<pre>no qos protocol-packet-control rate-limit-packet-queue &lt;packet queue number (0-40)&gt;</pre> <p>Clears the packet rate configured for the selected packet queue.  <b>Command mode:</b> Global configuration</p>
<pre>show qos protocol-packet-control information protocol</pre> <p>Displays of mapping of protocol packet types to each packet queue number. The status indicates whether the protocol is running or not running.  <b>Command mode:</b> All</p>
<pre>show qos protocol-packet-control information queue</pre> <p>Displays the packet rate configured for each packet queue.  <b>Command mode:</b> All</p>

## Weighted Random Early Detection Configuration

Weighted Random Early Detection (WRED) provides congestion avoidance by pre-emptively dropping packets before a queue becomes full. 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 301](#).

Table 190. WRED Configuration Options

Command Syntax and Usage	
<code>qos random-detect ecn</code>	<p>Enables or disables Explicit Congestion Notification (ECN). When ECN is on, the switch marks the ECN bit of the packet (if applicable) instead of dropping the packet. ECN-aware devices are notified of the congestion and those devices can take corrective actions.</p> <p><b>Note:</b> ECN functions only on TCP traffic.</p> <p><b>Command mode:</b> Global configuration</p>
<code>qos random-detect enable</code>	<p>Turns on Random Detection and avoidance.</p> <p><b>Command mode:</b> Global configuration</p>
<code>no qos random-detect enable</code>	<p>Turns off Random Detection and avoidance.</p> <p><b>Command mode:</b> Global configuration</p>
<code>show qos random-detect</code>	<p>Displays current Random Detection and avoidance parameters.</p> <p><b>Command mode:</b> All</p>

## WRED Transmit Queue Configuration

Table 191. WRED Transmit Queue Options

Command Syntax and Usage
<pre>[no] qos random-detect transmit-queue &lt;0-7&gt;     tcp &lt;min. threshold (1-100)&gt; &lt;max. threshold (1-100)&gt; &lt;drop rate (1-100)&gt;</pre> <p>Configures the WRED thresholds for TCP traffic. Use the <code>no</code> form to clear the WRED threshold value.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>[no] qos random-detect transmit-queue &lt;0-7&gt;     non-tcp &lt;min. threshold (1-100)&gt; &lt;max. threshold (1-100)&gt; &lt;drop rate (1-100)&gt;</pre> <p>Configures the WRED thresholds for non-TCP traffic. Use the <code>no</code> form to clear the WRED threshold value.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>qos random-detect transmit-queue &lt;0-7&gt; enable</pre> <p>Sets the WRED transmit queue configuration to <code>on</code>.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>no qos random-detect transmit-queue &lt;0-7&gt; enable</pre> <p>Sets the WRED transmit queue configuration to <code>off</code>.</p> <p><b>Command mode:</b> Global configuration</p>

---

## 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 300](#).

Table 192. General ACL Configuration Options

Command Syntax and Usage	
[no] access-control list <1-256>	Configures an Access Control List. To view command options, see <a href="#">page 312</a> . <b>Command mode:</b> Global configuration
[no] access-control list6 <1-128>	Configures an Access Control List. To view command options, see <a href="#">page 319</a> . <b>Command mode:</b> Global configuration
[no] access-control macl <1-256>	Configures an Access Control List. To view command options, see <a href="#">page 312</a> . <b>Command mode:</b> Global configuration
[no] access-control group <1-256>	Configures an ACL Group. To view command options, see <a href="#">page 324</a> . <b>Command mode:</b> Global configuration
[no] access-control vmap <1-256>	Configures an ACL VLAN map. To view command options, see <a href="#">page 328</a> . <b>Command mode:</b> Global configuration
show access-control	Displays the current ACL parameters. <b>Command mode:</b> All

## Access Control List Configuration

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

Table 193. ACL Configuration Options

Command Syntax and Usage
<pre>access-control list &lt;1-256&gt; action {permit deny set-priority &lt;0-7&gt;}</pre> <p>Configures a filter action for packets that match the ACL definitions. You can choose to permit (pass) or deny (drop) packets, or set the 802.1p priority level (0-7).</p> <p><b>Command mode:</b> Global configuration</p>
<pre>[no] access-control list &lt;1-256&gt; egress-port port &lt;port alias or number&gt;</pre> <p>Configures the ACL to function on egress packets.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>[no] access-control list &lt;1-256&gt; statistics</pre> <p>Enables or disables the statistics collection for the Access Control List.</p> <p><b>Command mode:</b> All except User EXEC</p>
<pre>[no] access-control list &lt;1-256&gt; log</pre> <p>Enables or disables logging for the Access Control List.</p> <p><b>Note:</b> Enabling the LOG feature neutralizes ACL deny filter actions for Telnet and SSH traffic that is addressed to the switch's Layer 3 interfaces.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>default access-control list &lt;1-256&gt;</pre> <p>Resets the ACL parameters to their default values.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>show access-control list &lt;1-256&gt;</pre> <p>Displays the current ACL parameters.</p> <p><b>Command mode:</b> All</p>



## 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 194. ACL Port Mirroring Options

Command Syntax and Usage
<pre>[no] access-control list &lt;I-256&gt; mirror port &lt;port alias or number&gt; none</pre> <p>Configures the destination to which packets that match this ACL are mirrored. <b>Command mode:</b> Global configuration</p>
<pre>show access-control list &lt;I-256&gt; mirror</pre> <p>Displays the current port mirroring parameters for the ACL. <b>Command mode:</b> All</p>

## Ethernet Filtering Configuration

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

Table 195. Ethernet Filtering Configuration Options

Command Syntax and Usage
<pre>[no] access-control list &lt;I-256&gt; ethernet source-mac-address &lt;MAC address&gt; &lt;MAC mask&gt;</pre> <p>Defines the source MAC address for this ACL. <b>Command mode:</b> Global configuration</p>
<pre>[no] access-control list &lt;I-256&gt; ethernet destination-mac-address &lt;MAC address&gt; &lt;MAC mask&gt;</pre> <p>Defines the destination MAC address for this ACL. <b>Command mode:</b> Global configuration</p>
<pre>[no] access-control list &lt;I-256&gt; ethernet vlan &lt;VLAN ID&gt; &lt;VLAN mask&gt;</pre> <p>Defines a VLAN number and mask for this ACL. <b>Command mode:</b> Global configuration</p>
<pre>[no] access-control list &lt;I-256&gt; ethernet ethernet-type {arp ip ipv6 mpls rarp any &lt;other (0x600-0xFFFF)&gt;}</pre> <p>Defines the Ethernet type for this ACL. <b>Command mode:</b> Global configuration</p>
<pre>[no] access-control list &lt;I-256&gt; ethernet priority &lt;0-7&gt;</pre> <p>Defines the Ethernet priority value for the ACL. <b>Command mode:</b> Global configuration</p>
<pre>default access-control list &lt;I-256&gt; ethernet</pre> <p>Resets Ethernet parameters for the ACL to their default values. <b>Command mode:</b> Global configuration</p>

Table 195. Ethernet Filtering Configuration Options

Command Syntax and Usage
<pre>no access-control list &lt;I-256&gt; ethernet</pre> <p>Removes Ethernet parameters for the ACL.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>show access-control list &lt;I-256&gt; ethernet</pre> <p>Displays the current Ethernet parameters for the ACL.</p> <p><b>Command mode:</b> All</p>

## IPv4 Filtering Configuration

These commands allow you to define IPv4 matching criteria for an ACL.

Table 196. IP version 4 Filtering Configuration Options

Command Syntax and Usage														
<pre>[no] access-control list &lt;I-256&gt; ipv4 source-ip-address &lt;IP address&gt; &lt;IP mask&gt;</pre> <p>Defines a source IP address for the ACL. If defined, traffic with this source IP address will match this ACL. Specify an IP address in dotted decimal notation.</p> <p><b>Command mode:</b> Global configuration</p>														
<pre>[no] access-control list &lt;I-256&gt; ipv4 destination-ip-address &lt;IP address&gt; &lt;IP mask&gt;</pre> <p>Defines a destination IP address for the ACL. If defined, traffic with this destination IP address will match this ACL.</p> <p><b>Command mode:</b> Global configuration</p>														
<pre>[no] access-control list &lt;I-256&gt; ipv4 protocol &lt;0-255&gt;</pre> <p>Defines an IP protocol for the ACL. If defined, traffic from the specified protocol matches this filter. Specify the protocol number. Listed below are some of the well-known protocols.</p> <table border="1"> <thead> <tr> <th>Number</th> <th>Name</th> </tr> </thead> <tbody> <tr> <td>1</td> <td>icmp</td> </tr> <tr> <td>2</td> <td>igmp</td> </tr> <tr> <td>6</td> <td>tcp</td> </tr> <tr> <td>17</td> <td>udp</td> </tr> <tr> <td>89</td> <td>ospf</td> </tr> <tr> <td>112</td> <td>vrrp</td> </tr> </tbody> </table> <p><b>Command mode:</b> Global configuration</p>	Number	Name	1	icmp	2	igmp	6	tcp	17	udp	89	ospf	112	vrrp
Number	Name													
1	icmp													
2	igmp													
6	tcp													
17	udp													
89	ospf													
112	vrrp													
<pre>[no] access-control list &lt;I-256&gt; ipv4 type-of-service &lt;0-255&gt;</pre> <p>Defines a Type of Service (ToS) value for the ACL. For more information on ToS, refer to RFC 1340 and 1349.</p> <p><b>Command mode:</b> Global configuration</p>														

Table 196. IP version 4 Filtering Configuration Options

Command Syntax and Usage
<pre>default access-control list &lt;I-256&gt; ipv4</pre> <p>Resets the IPv4 parameters for the ACL to their default values.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>show access-control list &lt;I-256&gt; ipv4</pre> <p>Displays the current IPv4 parameters.</p> <p><b>Command mode:</b> All</p>

## TCP/UDP Filtering Configuration

These commands allow you to define TCP/UDP matching criteria for an ACL.

Table 197. TCP/UDP Filtering Configuration Options

Command Syntax and Usage																												
<pre>[no] access-control list &lt;I-256&gt; tcp-udp source-port &lt;I-65535&gt; &lt;mask (0xFFFF)&gt;</pre> <p>Defines a source port for the ACL. If defined, traffic with the specified TCP or UDP source port will match this ACL. Specify the port number. Listed here are some of the well-known ports:</p> <table border="1"> <thead> <tr> <th>Number</th> <th>Name</th> </tr> </thead> <tbody> <tr><td>20</td><td>ftp-data</td></tr> <tr><td>21</td><td>ftp</td></tr> <tr><td>22</td><td>ssh</td></tr> <tr><td>23</td><td>telnet</td></tr> <tr><td>25</td><td>smtp</td></tr> <tr><td>37</td><td>time</td></tr> <tr><td>42</td><td>name</td></tr> <tr><td>43</td><td>whois</td></tr> <tr><td>53</td><td>domain</td></tr> <tr><td>69</td><td>tftp</td></tr> <tr><td>70</td><td>gopher</td></tr> <tr><td>79</td><td>finger</td></tr> <tr><td>80</td><td>http</td></tr> </tbody> </table> <p><b>Command mode:</b> Global configuration</p>	Number	Name	20	ftp-data	21	ftp	22	ssh	23	telnet	25	smtp	37	time	42	name	43	whois	53	domain	69	tftp	70	gopher	79	finger	80	http
Number	Name																											
20	ftp-data																											
21	ftp																											
22	ssh																											
23	telnet																											
25	smtp																											
37	time																											
42	name																											
43	whois																											
53	domain																											
69	tftp																											
70	gopher																											
79	finger																											
80	http																											
<pre>[no] access-control list &lt;I-256&gt; tcp-udp destination-port &lt;I-65535&gt; &lt;mask (0xFFFF)&gt;</pre> <p>Defines a destination port for the ACL. If defined, traffic with the specified TCP or UDP destination port will match this ACL. Specify the port number, just as with source-port.</p> <p><b>Command mode:</b> Global configuration</p>																												
<pre>[no] access-control list &lt;I-256&gt; tcp-udp flags &lt;value (0x0-0x3f)&gt; &lt;mask (0x0-0x3f)&gt;</pre> <p>Defines a TCP/UDP flag for the ACL.</p> <p><b>Command mode:</b> Global configuration</p>																												

Table 197. TCP/UDP Filtering Configuration Options

Command Syntax and Usage
<pre>default access-control list &lt;1-256&gt; tcp-udp</pre> <p>Resets the TCP/UDP parameters for the ACL to their default values.  <b>Command mode:</b> Global configuration</p>
<pre>show access-control list &lt;1-256&gt; tcp-udp</pre> <p>Displays the current TCP/UDP Filtering parameters.  <b>Command mode:</b> All</p>

## Packet Format Filtering Configuration

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

Table 198. Packet Format Filtering Configuration Options

Command Syntax and Usage
<pre>[no] access-control list &lt;1-256&gt; packet-format ethernet {ethertype2 snap llc}</pre> <p>Defines the Ethernet format for the ACL.  <b>Command mode:</b> Global configuration</p>
<pre>[no] access-control list &lt;1-256&gt; packet-format tagging {any none tagged}</pre> <p>Defines the tagging format for the ACL.  <b>Command mode:</b> Global configuration</p>
<pre>[no] access-control list &lt;1-256&gt; packet-format ip {ipv4 ipv6}</pre> <p>Defines the IP format for the ACL.  <b>Command mode:</b> Global configuration</p>
<pre>default access-control list &lt;1-256&gt; packet-format</pre> <p>Resets Packet Format parameters for the ACL to their default values.  <b>Command mode:</b> Global configuration</p>
<pre>show access-control list &lt;1-256&gt; packet-format</pre> <p>Displays the current Packet Format parameters for the ACL.  <b>Command mode:</b> All</p>

## ACL Metering Configuration

These commands define the Access Control profile for the selected ACL.

Table 199. ACL Metering Configuration Options

Command Syntax and Usage
<pre>access-control list &lt;1-256&gt; meter committed-rate &lt;64-10000000&gt;</pre> <p>Configures the committed rate, in kilobits per second. The committed rate must be a multiple of 64.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>access-control list &lt;1-256&gt; meter maximum-burst-size &lt;32-4096&gt;</pre> <p>Configures the maximum burst size, in kilobits. Enter one of the following values for <code>mbsize</code>: 32, 64, 128, 256, 512, 1024, 2048, 4096</p> <p><b>Command mode:</b> Global configuration</p>
<pre>[no] access-control list &lt;1-256&gt; meter enable</pre> <p>Enables or disables ACL Metering.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>access-control list &lt;1-256&gt; meter action {drop pass}</pre> <p>Configures the ACL Meter to either drop or pass out-of-profile traffic.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>default access-control list &lt;1-256&gt; meter</pre> <p>Sets the ACL meter configuration to its default values.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>no access-control list &lt;1-256&gt; meter</pre> <p>Deletes the selected ACL meter.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>show access-control list &lt;1-256&gt; meter</pre> <p>Displays current ACL Metering parameters.</p> <p><b>Command mode:</b> All</p>

## 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 200. ACL Re-Marking In-Profile Options

Command Syntax and Usage
<pre>[no] access-control list &lt;1-256&gt; re-mark in-profile dot1p &lt;0-7&gt;</pre> <p>Re-marks the 802.1p value. The value is the priority bits information in the packet structure.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>[no] no access-control list &lt;1-256&gt; re-mark in-profile dscp &lt;0-63&gt;</pre> <p>Remarks the DSCP value for in-profile traffic.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>[no] no access-control list &lt;1-256&gt; re-mark use-tos-precedence</pre> <p>Enables or disables mapping of TOS (Type of Service) priority to 802.1p priority for in-profile packets. When enabled, the TOS value is used to set the 802.1p value.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>default access-control list &lt;1-256&gt; re-mark</pre> <p>Sets the ACL re-mark parameters to their default values.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>show access-control list &lt;1-256&gt; re-markS</pre> <p>Displays current re-mark parameters.</p> <p><b>Command mode:</b> All</p>

### Re-Marking Out-of-Profile Configuration

Table 201. ACL Re-Marking Out-of-Profile Options

Command Syntax and Usage
<pre>access-control list &lt;1-256&gt; re-mark out-profile dscp &lt;1-63&gt;</pre> <p>Re-marks the DSCP value on out-of-profile packets for the ACL.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>no access-control list &lt;1-256&gt; re-mark out-profile</pre> <p>Disables re-marking on out-of-profile traffic.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>show access-control list &lt;1-256&gt; re-mark</pre> <p>Displays current re-mark parameters.</p> <p><b>Command mode:</b> All</p>

## ACL IPv6 Configuration

These commands allow you to define filtering criteria for each IPv6 Access Control List (ACL).

Table 202. IPv6 ACL Options

Command Syntax and Usage
<pre>[no] access-control list6 &lt;I-128&gt; egress-port port &lt;port alias or number&gt;</pre> <p>Configures the ACL to function on egress packets.  <b>Command mode:</b> Global configuration</p>
<pre>access-control list6 &lt;I-128&gt; action {permit deny set-priority &lt;0-7&gt;}</pre> <p>Configures a filter action for packets that match the ACL definitions. You can choose to permit (pass) or deny (drop) packets, or set the 802.1p priority level (0-7).  <b>Command mode:</b> Global configuration</p>
<pre>[no] access-control list6 &lt;I-128&gt; statistics</pre> <p>Enables or disables the statistics collection for the Access Control List.  <b>Command mode:</b> Global configuration</p>
<pre>[no] access-control list6 &lt;I-128&gt; log</pre> <p>Enables or disables Access Control List logging.</p>
<pre>default access-control list6 &lt;I-128&gt;</pre> <p>Resets the ACL parameters to their default values.  <b>Command mode:</b> Global configuration</p>
<pre>show access-control list6 &lt;I-128&gt;</pre> <p>Displays the current ACL parameters.  <b>Command mode:</b> All</p>

## IP version 6 Filtering Configuration

These commands allow you to define IPv6 matching criteria for an ACL.

Table 203. IP version 6 Filtering Options

Command Syntax and Usage	
[no] access-control list6 <1-128> ipv6 source-address <IPv6 address> <prefix length (1-128)>	<p>Defines a source IPv6 address for the ACL. If defined, traffic with this source address will match this ACL.</p> <p><b>Command mode:</b> Global configuration</p>
[no] access-control list6 <1-128> ipv6 destination-address <IPv6 address> <prefix length (1-128)>	<p>Defines a destination IPv6 address for the ACL. If defined, traffic with this destination address will match this ACL.</p> <p><b>Command mode:</b> Global configuration</p>
[no] access-control list6 <1-128> ipv6 next-header <0-255>	<p>Defines the next header value for the ACL. If defined, traffic with this next header value will match this ACL.</p> <p><b>Command mode:</b> Global configuration</p>
[no] access-control list6 <1-128> ipv6 flow-label <0-1048575>	<p>Defines the flow label for the ACL. If defined, traffic with this flow label will match this ACL.</p> <p><b>Command mode:</b> Global configuration</p>
[no] access-control list6 <1-128> ipv6 traffic-class <0-255>	<p>Defines the traffic class for the ACL. If defined, traffic with this traffic class will match this ACL.</p> <p><b>Command mode:</b> Global configuration</p>
default access-control list6 <1-128> ipv6	<p>Resets the IPv6 parameters for the ACL to their default values.</p> <p><b>Command mode:</b> Global configuration</p>
show access-control list6 <1-128> ipv6	<p>Displays the current IPv6 parameters.</p> <p><b>Command mode:</b> All</p>



## IPv6 TCP/UDP Filtering Configuration

These commands allow you to define TCP/UDP matching criteria for an ACL.

Table 204. IPv6 ACL TCP/UDP Filtering Options

Command Syntax and Usage																													
<pre>[no] access-control list6 &lt;I-128&gt; tcp-udp source-port &lt;I-65535&gt; &lt;mask (0xFFFF)&gt;</pre>	<p>Defines a source port for the ACL. If defined, traffic with the specified TCP or UDP source port will match this ACL. Specify the port number. Listed here are some of the well-known ports:</p> <table border="1"> <thead> <tr> <th>Number</th> <th>Name</th> </tr> </thead> <tbody> <tr><td>20</td><td>ftp-data</td></tr> <tr><td>21</td><td>ftp</td></tr> <tr><td>22</td><td>ssh</td></tr> <tr><td>23</td><td>telnet</td></tr> <tr><td>25</td><td>smtp</td></tr> <tr><td>37</td><td>time</td></tr> <tr><td>42</td><td>name</td></tr> <tr><td>43</td><td>whois</td></tr> <tr><td>53</td><td>domain</td></tr> <tr><td>69</td><td>tftp</td></tr> <tr><td>70</td><td>gopher</td></tr> <tr><td>79</td><td>finger</td></tr> <tr><td>80</td><td>http</td></tr> </tbody> </table> <p><b>Command mode:</b> Global configuration</p>	Number	Name	20	ftp-data	21	ftp	22	ssh	23	telnet	25	smtp	37	time	42	name	43	whois	53	domain	69	tftp	70	gopher	79	finger	80	http
Number	Name																												
20	ftp-data																												
21	ftp																												
22	ssh																												
23	telnet																												
25	smtp																												
37	time																												
42	name																												
43	whois																												
53	domain																												
69	tftp																												
70	gopher																												
79	finger																												
80	http																												
<pre>[no] access-control list6 &lt;I-128&gt; tcp-udp destination-port &lt;I-65535&gt; &lt;mask (0xFFFF)&gt;</pre>	<p>Defines a destination port for the ACL. If defined, traffic with the specified TCP or UDP destination port will match this ACL. Specify the port number, just as with <code>sport</code> above.</p> <p><b>Command mode:</b> Global configuration</p>																												
<pre>[no] access-control list6 &lt;I-128&gt; tcp-udp flags &lt;value (0x0-0x3f)&gt; &lt;mask (0x0-0x3f)&gt;</pre>	<p>Defines a TCP/UDP flag for the ACL.</p> <p><b>Command mode:</b> Global configuration</p>																												
<pre>default access-control list6 &lt;I-128&gt; tcp-udp</pre>	<p>Resets the TCP/UDP parameters for the ACL to their default values.</p> <p><b>Command mode:</b> Global configuration</p>																												
<pre>show access-control list6 &lt;I-128&gt; tcp-udp</pre>	<p>Displays the current TCP/UDP Filtering parameters.</p> <p><b>Command mode:</b> All</p>																												

## IPv6 Re-Mark Configuration

You can choose to re-mark IP header data for the selected ACL. You can configure different re-mark values, based on whether packets fall within the ACL metering profile, or out of the ACL metering profile.

### IPv6 Re-Marking In-Profile Configuration

Table 205. IPv6 Re-Marking In-Profile Options

Command Syntax and Usage
<pre>[no] access-control list6 &lt;1-128&gt; re-mark dot1p &lt;0-7&gt;</pre> <p>Re-marks the 802.1p value. The value is the priority bits information in the packet structure.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>[no] access-control list6 &lt;1-128&gt; re-mark in-profile dscp &lt;0-63&gt;</pre> <p>Re-marks the DSCP value for in-profile traffic.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>[no] access-control list6 &lt;1-128&gt; re-mark use-tos-precedence</pre> <p>Enables or disables mapping of TOS (Type of Service) priority to 802.1p priority for in-profile packets. When enabled, the TOS value is used to set the 802.1p value.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>default access-control list6 &lt;1-128&gt; re-mark</pre> <p>Sets the ACL re-mark parameters to their default values.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>show access-control list6 &lt;1-128&gt; re-mark</pre> <p>Displays current re-mark parameters.</p> <p><b>Command mode:</b> All</p>

## IPv6 Metering Configuration

These commands define the Access Control profile for the selected ACL.

### IPv6 Metering Configuration

Table 206. IPv6 Metering Options

Command Syntax and Usage	
<pre>access-control list6 &lt;1-256&gt; meter committed-rate &lt;64-10000000&gt;</pre>	<p>Configures the committed rate, in kilobits per second. The committed rate must be a multiple of 64.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>access-control list6 &lt;1-256&gt; meter maximum-burst-size &lt;32-4096&gt;</pre>	<p>Configures the maximum burst size, in kilobits. Enter one of the following values for mbsize: 32, 64, 128, 256, 512, 1024, 2048, 4096</p> <p><b>Command mode:</b> Global configuration</p>
<pre>[no] access-control list6 &lt;1-256&gt; meter enable</pre>	<p>Enables or disables ACL Metering.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>access-control list6 &lt;1-256&gt; meter action {drop pass}</pre>	<p>Configures the ACL Meter to either drop or pass out-of-profile traffic.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>default access-control list6 &lt;1-256&gt; meter</pre>	<p>Sets the ACL meter configuration to its default values.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>no access-control list6 &lt;1-256&gt; meter</pre>	<p>Deletes the selected ACL meter.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>show access-control list6 &lt;1-256&gt; meter</pre>	<p>Displays current ACL Metering parameters.</p> <p><b>Command mode:</b> All</p>

## ACL Log Configuration

These commands allow you to define filtering criteria for each IPv6 Access Control List (ACL) log.

Table 207. ACL Log Configuration Options

Command Syntax and Usage
<pre>access-control list &lt;I-128&gt; log</pre> <p>Enables access control list logging. <b>Command mode:</b> Global configuration</p>
<pre>access-control log interval &lt;seconds&gt;</pre> <p>Sets the filter log displaying interval in seconds. <b>Command mode:</b> Global configuration</p>
<pre>access-control log rate-limit &lt;seconds&gt;</pre> <p>Sets the filter log queue rate limit in seconds. <b>Command mode:</b> Global configuration</p>
<pre>default access-control log [interval   rate-lmt]</pre> <p>Resets the specified filter log parameters to their default values. <b>Command mode:</b> Global configuration</p>
<pre>show access-control log</pre> <p>Displays the current ACL log parameters. <b>Command mode:</b> All</p>

## ACL Group Configuration

These commands allow you to compile one or more ACLs into an ACL group. Once you create an ACL group, you can assign the ACL group to one or more ports.

Table 208. ACL Group Configuration Commands

Command Syntax and Usage
<pre>access-control group &lt;I-256&gt; list &lt;I-256&gt;</pre> <p>Adds the selected IPv4 ACL to the ACL group. <b>Command mode:</b> Global configuration</p>
<pre>no access-control group &lt;I-256&gt; list &lt;I-256&gt;</pre> <p>Removes the selected IPv4 ACL from the ACL group. <b>Command mode:</b> Global configuration</p>
<pre>access-control group &lt;I-256&gt; list6 &lt;I-128&gt;</pre> <p>Adds the selected IPv6 ACL to the ACL group. <b>Command mode:</b> Global configuration</p>

Table 208. ACL Group Configuration Commands

Command Syntax and Usage
<pre>no access-control group &lt;I-256&gt; list6 &lt;I-128&gt;</pre> <p>Removes the selected IPv6 ACL from the ACL group.  <b>Command mode:</b> Global configuration</p>
<pre>show access-control group &lt;I-256&gt;</pre> <p>Displays the current ACL group parameters.  <b>Command mode:</b> All</p>

## Management ACL Configuration

These commands allow you to define filtering criteria for each management ACL (MACL).

Table 209. MACL Configuration Options

Command Syntax and Usage
<pre>access-control macl &lt;I-256&gt; action {permit deny set-priority &lt;0-7&gt;}</pre> <p>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).  <b>Command mode:</b> Global configuration</p>
<pre>[no] access-control macl &lt;I-256&gt; statistics</pre> <p>Enables or disables the statistics collection for the MACL.  <b>Command mode:</b> All except User EXEC</p>
<pre>[no] access-control macl &lt;I-256&gt; enable</pre> <p>Enables or disables the management ACL.  <b>Command mode:</b> Global configuration</p>
<pre>show access-control macl &lt;I-256&gt;</pre> <p>Displays the current MACL parameters.  <b>Command mode:</b> All</p>

## MACL IPv4 Filtering Configuration

These commands allow you to define IPv4 matching criteria for an MACL.

Table 210. IP version 4 Filtering Configuration Options

Command Syntax and Usage															
<pre>[no] access-control macl &lt;1-256&gt; ipv4 source-ip-address &lt;IP address&gt; &lt;IP mask&gt;</pre>	<p>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.</p> <p><b>Command mode:</b> Global configuration</p>														
<pre>[no] access-control macl &lt;1-256&gt; ipv4 destination-ip-address &lt;IP address&gt; &lt;IP mask&gt;</pre>	<p>Defines a destination IP address for the MACL. If defined, traffic with this destination IP address will match this MACL.</p> <p><b>Command mode:</b> Global configuration</p>														
<pre>[no] access-control macl &lt;1-256&gt; ipv4 protocol &lt;0-255&gt;</pre>	<p>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.</p> <table border="1"> <thead> <tr> <th>Number</th> <th>Name</th> </tr> </thead> <tbody> <tr> <td>1</td> <td>icmp</td> </tr> <tr> <td>2</td> <td>igmp</td> </tr> <tr> <td>6</td> <td>tcp</td> </tr> <tr> <td>17</td> <td>udp</td> </tr> <tr> <td>89</td> <td>ospf</td> </tr> <tr> <td>112</td> <td>vrrp</td> </tr> </tbody> </table> <p><b>Command mode:</b> Global configuration</p>	Number	Name	1	icmp	2	igmp	6	tcp	17	udp	89	ospf	112	vrrp
Number	Name														
1	icmp														
2	igmp														
6	tcp														
17	udp														
89	ospf														
112	vrrp														
<pre>default access-control macl &lt;1-256&gt; ipv4</pre>	<p>Resets the IPv4 parameters for the MACL to their default values.</p> <p><b>Command mode:</b> Global configuration</p>														
<pre>show access-control macl &lt;1-256&gt; ipv4</pre>	<p>Displays the current IPv4 parameters.</p> <p><b>Command mode:</b> All</p>														

## MACL TCP/UDP Filtering Configuration

These commands allow you to define TCP/UDP matching criteria for an MACL.

Table 211. TCP/UDP Filtering Configuration Options

Command Syntax and Usage																													
<pre>[no] access-control macl &lt;I-256&gt; tcp-udp source-port &lt;I-65535&gt; &lt;mask (0xFFFF)&gt;</pre>	<p>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:</p> <table border="1"> <thead> <tr> <th>Number</th> <th>Name</th> </tr> </thead> <tbody> <tr><td>20</td><td>ftp-data</td></tr> <tr><td>21</td><td>ftp</td></tr> <tr><td>22</td><td>ssh</td></tr> <tr><td>23</td><td>telnet</td></tr> <tr><td>25</td><td>smtp</td></tr> <tr><td>37</td><td>time</td></tr> <tr><td>42</td><td>name</td></tr> <tr><td>43</td><td>whois</td></tr> <tr><td>53</td><td>domain</td></tr> <tr><td>69</td><td>tftp</td></tr> <tr><td>70</td><td>gopher</td></tr> <tr><td>79</td><td>finger</td></tr> <tr><td>80</td><td>http</td></tr> </tbody> </table> <p><b>Command mode:</b> Global configuration</p>	Number	Name	20	ftp-data	21	ftp	22	ssh	23	telnet	25	smtp	37	time	42	name	43	whois	53	domain	69	tftp	70	gopher	79	finger	80	http
Number	Name																												
20	ftp-data																												
21	ftp																												
22	ssh																												
23	telnet																												
25	smtp																												
37	time																												
42	name																												
43	whois																												
53	domain																												
69	tftp																												
70	gopher																												
79	finger																												
80	http																												
<pre>[no] access-control macl &lt;I-256&gt; tcp-udp destination-port &lt;I-65535&gt; &lt;mask (0xFFFF)&gt;</pre>	<p>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 <code>sport</code> above.</p> <p><b>Command mode:</b> Global configuration</p>																												
<pre>[no] access-control macl &lt;I-256&gt; tcp-udp flags &lt;value (0x0-0x3f)&gt; &lt;mask (0x0-0x3f)&gt;</pre>	<p>Defines a TCP/UDP flag for the MACL.</p> <p><b>Command mode:</b> Global configuration</p>																												
<pre>default access-control macl &lt;I-256&gt; tcp-udp</pre>	<p>Resets the TCP/UDP parameters for the MACL to their default values.</p> <p><b>Command mode:</b> Global configuration</p>																												
<pre>show access-control macl &lt;I-256&gt; tcp-udp</pre>	<p>Displays the current TCP/UDP Filtering parameters.</p> <p><b>Command mode:</b> All</p>																												

## VMAP Configuration

A VLAN Map is an Access Control List (ACL) that can be assigned to a VLAN or a VM group instead of a port. In a virtualized environment where Virtual Machines move between physical servers, VLAN Maps allow you to create traffic filtering and metering policies associated with a VM's VLAN.

For more information about VLAN Map configuration commands, see [“Access Control List Configuration” on page 312](#).

For more information about assigning VLAN Maps to a VLAN, see [“VLAN Configuration” on page 366](#).

For more information about assigning VLAN Maps to a VM group, see [“VM Group Configuration” on page 489](#).

**Table 212.** lists the general VMAP configuration commands.

*Table 212. VMAP Configuration Options*

<b>Command Syntax and Usage</b>
<pre>[no] access-control vmap &lt;1-128&gt; egress-port &lt;port alias or number&gt;</pre> <p>Configures the VMAP to function on egress packets.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>access-control vmap &lt;1-256&gt; action {permit deny set-priority &lt;0-7&gt;}</pre> <p>Configures a filter action for packets that match the VMAP definitions. You can choose to permit (pass) or deny (drop) packets, or set the 802.1p priority level (0-7).</p> <p><b>Command mode:</b> Global configuration</p>
<pre>[no] access-control vmap &lt;1-256&gt; ipv4 source-ip-address &lt;IPv4 address&gt; &lt;IPv4 mask&gt;</pre> <p>Enables or disables filtering of VMAP statistics collection based on source IP address.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>[no] access-control vmap &lt;1-256&gt; ipv4 destination-ip-address &lt;IPv4 address&gt; &lt;IPv4 mask&gt;</pre> <p>Enables or disables filtering of VMAP statistics collection based on destination IP address.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>[no] access-control vmap &lt;1-256&gt; ipv4 protocol &lt;0-255&gt;</pre> <p>Enables or disables filtering of VMAP statistics collection based on protocol.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>[no] access-control vmap &lt;1-256&gt; ipv4 type-of-service &lt;0-255&gt;</pre> <p>Enables or disables filtering of VMAP statistics collection based on type of service.</p> <p><b>Command mode:</b> Global configuration</p>



Table 212. VMAP Configuration Options

Command Syntax and Usage
<pre>access-control vmap &lt;1-256&gt; meter enable</pre> <p>Enables ACL port metering.</p> <p><b>Command mode:</b> All except User EXEC</p>
<pre>access-control vmap &lt;1-256&gt; meter action drop pass</pre> <p>Sets ACL port metering to drop or pass out-of-profile traffic.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>access-control vmap &lt;1-256&gt; meter committed-rate &lt;64-10000000&gt;</pre> <p>Sets the ACL port metering control rate in kilobits per second.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>access-control vmap &lt;1-256&gt; meter maximum-burst-size &lt;32-4096&gt;</pre> <p>Sets the ACL port metering maximum burst size in kilobytes. The following eight values are allowed:</p> <ul style="list-style-type: none"> <li>– 32</li> <li>– 64</li> <li>– 128</li> <li>– 256</li> <li>– 512</li> <li>– 1024</li> <li>– 2048</li> <li>– 4096</li> </ul> <p><b>Command mode:</b> Global configuration</p>
<pre>no access-control vmap &lt;1-256&gt; meter enable</pre> <p>Disables ACL port metering.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>access-control vmap &lt;1-256&gt; mirror port &lt;port&gt;</pre> <p>Sets the specified port as the mirror target.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>no access-control vmap &lt;1-256&gt; mirror</pre> <p>Turns off ACL mirroring.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>access-control vmap &lt;1-256&gt; packet-format ethernet ethernet-type2 llc snap</pre> <p>Sets to filter the specified ethernet packet format type.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>access-control vmap &lt;1-256&gt; packet-format ip ipv4 ipv6</pre> <p>Sets to filter the specified IP packet format type.</p> <p><b>Command mode:</b> Global configuration</p>

Table 212. VMAP Configuration Options

Command Syntax and Usage
<pre>access-control vmap &lt;1-256&gt; packet-format tagging any none tagged</pre> <p>Sets to filter the based on packet tagging. The options are:</p> <ul style="list-style-type: none"> <li>– any: Filter tagged &amp; untagged packets</li> <li>– none: Filter only untagged packets</li> <li>– tagged: Filter only tagged packets</li> </ul> <p><b>Command mode:</b> Global configuration</p>
<pre>no access-control vmap &lt;1-256&gt; packet-format ethernet ip tagging</pre> <p>Disables filtering based on the specified packet format.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>access-control vmap &lt;1-256&gt; re-mark dot1p &lt;0-7&gt;</pre> <p>Sets the ACL re-mark configuration user update priority.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>no access-control vmap &lt;1-256&gt; re-mark dot1p &lt;0-7&gt;</pre> <p>Disables the use of dot1p for in-profile traffic ACL re-mark configuration.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>access-control vmap &lt;1-256&gt; re-mark in-profile out-profile dscp &lt;0-63&gt;</pre> <p>Sets the ACL re-mark configuration user update priority.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>no access-control vmap &lt;1-256&gt; re-mark in-profile out-profile</pre> <p>Removes all re-mark in-profile or out-profile settings.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>[no] access-control vmap &lt;1-256&gt; re-mark use-tos-precedence</pre> <p>Enables or disables the use of the TOS precedence for in-profile traffic.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>[no] access-control vmap &lt;1-256&gt; statistics</pre> <p>Enables or disables statistics for this access control list.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>access-control vmap &lt;1-256&gt; tcp-udp source-port destination-port &lt;1-65535&gt; &lt;port mask (0x0001 - 0xFFFF)&gt;</pre> <p>Sets the TCP/UDP filtering source port or destination port and port mask for this ACL.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>access-control vmap &lt;1-256&gt; tcp-udp [&lt;flags mask (0x0-0x3F)&gt;]</pre> <p>Sets the TCP flags for this ACL.</p> <p><b>Command mode:</b> Global configuration</p>

Table 212. VMAP Configuration Options

Command Syntax and Usage
<pre>no access-control vmap &lt;1-256&gt; tcp-udp</pre> <p>Removes TCP/UDP filtering for this ACL. <b>Command mode:</b> Global configuration</p>
<pre>default access-control vmap &lt;1-256&gt;</pre> <p>Resets the VMAP parameters to their default values. <b>Command mode:</b> Global configuration</p>
<pre>show access-control vmap &lt;1-256&gt;</pre> <p>Displays the current VMAP parameters. <b>Command mode:</b> All except User EXEC</p>

---

## Port Mirroring

Port mirroring is disabled by default. For more information about port mirroring on the G8264, see “Appendix A: Troubleshooting” in the *IBM N/OS 7.6 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 213. Port Mirroring Configuration Options

Command Syntax and Usage
<pre>[no] port-mirroring enable</pre> <p>Enables or disables port mirroring.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>show port-mirroring</pre> <p>Displays current settings of the mirrored and monitoring ports.</p> <p><b>Command mode:</b> All except User EXEC</p>

## Port-Mirroring Configuration

Table 214. Port-Based Port-Mirroring Configuration Options

Command Syntax and Usage
<pre>port-mirroring monitor-port &lt;port alias or number&gt; mirroring-port &lt;port alias or number&gt; {in out both}</pre> <p>Adds the port to be mirrored. This command also allows you to enter the direction of the traffic. It is necessary to specify the direction because:</p> <p>If the source port of the frame matches the mirrored port and the mirrored direction is ingress or both (ingress and egress), the frame is sent to the monitoring port.</p> <p>If the destination port of the frame matches the mirrored port and the mirrored direction is egress or both, the frame is sent to the monitoring port.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>no port-mirroring monitor-port &lt;port alias or number&gt; mirroring-port &lt;port alias or number&gt;</pre> <p>Removes the mirrored port.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>show port-mirroring</pre> <p>Displays the current settings of the monitoring port.</p> <p><b>Command mode:</b> All except User EXEC</p>

---

## Layer 2 Configuration

The following table describes basic Layer 2 Configuration commands. The following sections provide more detailed information and commands.

Table 215. Layer 2 Configuration Commands

Command Syntax and Usage
<code>vlan &lt;VLAN number&gt;</code> Enter VLAN configuration mode. To view command options, see <a href="#">page 366</a> . <b>Command mode:</b> Global configuration
<code>show layer2</code> Displays current Layer 2 parameters. <b>Command mode:</b> 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 216. 802.1x Configuration Options

Command Syntax and Usage
<code>dot1x enable</code> Globally enables 802.1X. <b>Command mode:</b> Global configuration
<code>no dot1x enable</code> Globally disables 802.1X. <b>Command mode:</b> Global configuration
<code>show dot1x</code> Displays current 802.1X parameters. <b>Command mode:</b> All

The following sections describe the 802.1x configuration options.

- “802.1X Global Configuration” on [page 334](#)
- “802.1X Guest VLAN Configuration” on [page 335](#)
- “802.1X Port Configuration” on [page 336](#)

## 802.1X Global Configuration

The global 802.1X commands allow you to configure parameters that affect all ports in the switch.

Table 217. 802.1X Global Configuration Options

Command Syntax and Usage
<pre>dot1x mode [force-unauthorized auto force-authorized]</pre> <p>Sets the type of access control for all ports:</p> <ul style="list-style-type: none"><li>– force-unauthorized - the port is unauthorized unconditionally.</li><li>– auto - the port is unauthorized until it is successfully authorized by the RADIUS server.</li><li>– force-authorized - the port is authorized unconditionally, allowing all traffic.</li></ul> <p>The default value is force-authorized.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>dot1x quiet-time &lt;0-65535&gt;</pre> <p>Sets the time, in seconds, the authenticator waits before transmitting an EAP-Request/ Identity frame to the supplicant (client) after an authentication failure in the previous round of authentication. The default value is 60 seconds.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>dot1x transmit-interval &lt;1-65535&gt;</pre> <p>Sets the time, in seconds, the authenticator waits for an EAP-Response/Identity frame from the supplicant (client) before retransmitting an EAP-Request/Identity frame. The default value is 30 seconds.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>dot1x supplicant-timeout &lt;1-65535&gt;</pre> <p>Sets the time, in seconds, the authenticator waits for an EAP-Response packet from the supplicant (client) before retransmitting the EAP-Request packet from the authentication server. The default value is 30 seconds.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>dot1x server-timeout &lt;1-65535&gt;</pre> <p>Sets the time, in seconds, the authenticator waits for a response from the RADIUS server before declaring an authentication timeout. The default value is 30 seconds.</p> <p>The time interval between transmissions of the RADIUS Access-Request packet containing the supplicant's (client's) EAP-Response packet is determined by the current setting of</p> <pre>radius-server timeout &lt;timeout-value&gt; (default is 3 seconds).</pre> <p><b>Command mode:</b> Global configuration</p>
<pre>dot1x max-request &lt;1-10&gt;</pre> <p>Sets the maximum number of times the authenticator retransmits an EAP-Request packet to the supplicant (client). The default value is 2.</p> <p><b>Command mode:</b> Global configuration</p>

Table 217. 802.1X Global Configuration Options (continued)

Command Syntax and Usage	
dot1x re-authentication-interval <1-604800>	<p>Sets the time, in seconds, the authenticator waits before re-authenticating a supplicant (client) when periodic re-authentication is enabled. The default value is 3600 seconds.</p> <p><b>Command mode:</b> Global configuration</p>
dot1x re-authenticate	<p>Sets the re-authentication status to <code>on</code>. The default value is <code>off</code>.</p> <p><b>Command mode:</b> Global configuration</p>
[no] dot1x re-authenticate	<p>Sets the re-authentication status to <code>off</code>. The default value is <code>off</code>.</p> <p><b>Command mode:</b> Global configuration</p>
[no] dot1x vlan-assign	<p>Sets the dynamic VLAN assignment status to <code>on</code> or <code>off</code>. The default value is <code>off</code>.</p> <p><b>Command mode:</b> Global configuration</p>
default dot1x	<p>Resets the global 802.1X parameters to their default values.</p> <p><b>Command mode:</b> Global configuration</p>
show dot1x	<p>Displays current global 802.1X parameters.</p> <p><b>Command mode:</b> All</p>

## 802.1X Guest VLAN Configuration

The 802.1X Guest VLAN commands allow you to configure a Guest VLAN for unauthenticated ports. The Guest VLAN provides limited access to switch functions.

Table 218. 802.1X Guest VLAN Configuration Options

Command Syntax and Usage	
[no] dot1x guest-vlan vlan <VLAN number>	<p>Configures the Guest VLAN number.</p> <p><b>Command mode:</b> Global configuration</p>
dot1x guest-vlan enable	<p>Enables the 802.1X Guest VLAN.</p> <p><b>Command mode:</b> Global configuration</p>

Table 218. 802.1X Guest VLAN Configuration Options

Command Syntax and Usage
<pre>no dot1x guest-vlan enable</pre> <p>Disables the 802.1X Guest VLAN.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>show dot1x</pre> <p>Displays current 802.1X parameters.</p> <p><b>Command mode:</b> All</p>

## 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 219. 802.1X Port Options

Command Syntax and Usage
<pre>dot1x mode force-unauthorized auto force-authorized</pre> <p>Sets the type of access control for the port:</p> <ul style="list-style-type: none"> <li>– force-unauthorized - the port is unauthorized unconditionally.</li> <li>– auto - the port is unauthorized until it is successfully authorized by the RADIUS server.</li> <li>– force-authorized - the port is authorized unconditionally, allowing all traffic.</li> </ul> <p>The default value is force-authorized.</p> <p><b>Command mode:</b> Interface port</p>
<pre>dot1x quiet-time &lt;0-65535&gt;</pre> <p>Sets the time, in seconds, the authenticator waits before transmitting an EAP-Request/ Identity frame to the supplicant (client) after an authentication failure in the previous round of authentication. The default value is 60 seconds.</p> <p><b>Command mode:</b> Interface port</p>
<pre>dot1x transmit-interval &lt;1-65535&gt;</pre> <p>Sets the time, in seconds, the authenticator waits for an EAP-Response/Identity frame from the supplicant (client) before retransmitting an EAP-Request/Identity frame. The default value is 30 seconds.</p> <p><b>Command mode:</b> Interface port</p>
<pre>dot1x supplicant-timeout &lt;1-65535&gt;</pre> <p>Sets the time, in seconds, the authenticator waits for an EAP-Response packet from the supplicant (client) before retransmitting the EAP-Request packet from the authentication server. The default value is 30 seconds.</p> <p><b>Command mode:</b> Interface port</p>



Table 219. 802.1X Port Options (continued)

Command Syntax and Usage	
dot1x server-timeout <1-65535>	<p>Sets the time, in seconds, the authenticator waits for a response from the RADIUS server before declaring an authentication timeout. The default value is 30 seconds.</p> <p>The time interval between transmissions of the RADIUS Access-Request packet containing the supplicant's (client's) EAP-Response packet is determined by the current setting of the <code>radius-server timeout</code> command.</p> <p><b>Command mode:</b> Interface port</p>
dot1x max-request <1-10>	<p>Sets the maximum number of times the authenticator retransmits an EAP-Request packet to the supplicant (client). The default value is 2.</p> <p><b>Command mode:</b> Interface port</p>
dot1x re-authentication-interval <1-604800>	<p>Sets the time, in seconds, the authenticator waits before re-authenticating a supplicant (client) when periodic re-authentication is enabled. The default value is 3600 seconds.</p> <p><b>Command mode:</b> Interface port</p>
dot1x re-authenticate	<p>Sets the re-authentication status to <code>on</code>. The default value is <code>off</code>.</p> <p><b>Command mode:</b> Interface port</p>
[no] dot1x re-authenticate	<p>Sets the re-authentication status <code>off</code>. The default value is <code>off</code>.</p> <p><b>Command mode:</b> Interface port</p>
[no] dot1x vlan-assign	<p>Sets the dynamic VLAN assignment status to <code>on</code> or <code>off</code>. The default value is <code>off</code>.</p> <p><b>Command mode:</b> Interface port</p>
default dot1x	<p>Resets the 802.1X port parameters to their default values.</p> <p><b>Command mode:</b> Interface port</p>
dot1x apply-global	<p>Applies current global 802.1X configuration parameters to the port.</p> <p><b>Command mode:</b> Interface port</p>
show interface port <port alias or number> dot1x	<p>Displays current 802.1X port parameters.</p> <p><b>Command mode:</b> All</p>

## Spanning Tree Configuration

IBM N/OS supports the IEEE 802.1w Rapid Spanning Tree Protocol (RSTP), the IEEE 802.1s Multiple Spanning Tree Protocol (MSTP), and Per VLAN Rapid Spanning Tree Protocol (PVRST). STP is used to prevent loops in the network topology. Up to 128 Spanning Tree Groups can be configured on the switch (STG 128 is reserved for management).

**Note:** When VRRP is used for active/active redundancy, STG must be enabled.

Table 220. Spanning Tree Configuration Options

Command Syntax and Usage	
<pre>spanning-tree mode [disable mst pvrst rstp]</pre>	<p>Selects and enables Multiple Spanning Tree mode (<i>mst</i>), Per VLAN Rapid Spanning Tree mode (<i>pvrst</i>), or Rapid Spanning Tree mode (<i>rstp</i>).</p> <p>The default mode is PVRST.</p> <p>When you select <code>spanning-tree mode disable</code>, the switch globally turns Spanning Tree <i>off</i>. All ports are placed into forwarding state. Any BPDU's received are flooded. BPDU Guard is not affected by this command.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>[no] spanning-tree stg-auto</pre>	<p>Enables or disables VLAN Automatic STG Assignment (VASA). When enabled, each time a new VLAN is configured, the switch will automatically assign the new VLAN its own STG. Conversely, when a VLAN is deleted, if its STG is not associated with any other VLAN, the STG is returned to the available pool.</p> <p><b>Note:</b> When using VASA, a maximum number of 127 automatically assigned STGs is supported.</p> <p><b>Note:</b> VASA applies only to PVRST mode.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>[no] spanning-tree pvst-compatibility</pre>	<p>Enables or disables VLAN tagging of Spanning Tree BPDUs. The default setting is <i>enabled</i>.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>[no] spanning-tree portfast</pre>	<p>Enables or disables this port as portfast or edge port. An edge port is not connected to a bridge, and can begin forwarding traffic as soon as the link is up. Configure server ports as edge ports (<i>enabled</i>).</p> <p><b>Note:</b> After you configure the port as an edge port, you must disable the port and then re-enable the port for the change to take effect.</p> <p><b>Command mode:</b> Interface port/Interface portchannel</p>

Table 220. Spanning Tree Configuration Options (continued)

<b>Command Syntax and Usage</b>	
<pre>[no] spanning-tree link-type {p2p shared auto}</pre>	<p>Defines the type of link connected to the port, as follows:</p> <ul style="list-style-type: none"> <li>– auto: Configures the port to detect the link type, and automatically match its settings.</li> <li>– p2p: Configures the port for Point-To-Point protocol.</li> <li>– shared: Configures the port to connect to a shared medium (usually a hub).</li> </ul> <p>The default link type is auto.</p> <p><b>Command mode:</b> Interface port/Interface portchannel</p>
<pre>spanning-tree guard loop</pre>	<p>Enables STP loop guard. STP loop guard prevents the port from forwarding traffic if no BPDUs are received. The port is placed into a loop-inconsistent blocking state until a BPDU is received.</p> <p><b>Command mode:</b> Interface port/Interface portchannel</p>
<pre>spanning-tree guard root</pre>	<p>Enables STP root guard. STP root guard enforces the position of the root bridge. If the bridge receives a superior BPDU, the port is placed into a root-inconsistent state (listening).</p> <p><b>Command mode:</b> Interface port/Interface portchannel</p>
<pre>spanning-tree guard none</pre>	<p>Disables STP loop guard and root guard.</p> <p><b>Command mode:</b> Interface port/Interface portchannel</p>
<pre>no spanning-tree guard</pre>	<p>Sets the Spanning Tree guard parameters to their default values.</p> <p><b>Command mode:</b> Interface port/Interface portchannel</p>
<pre>show spanning-tree</pre>	<p>Displays Spanning Tree information, including the status (on or off), Spanning Tree mode (RSTP, PVRST, or MSTP), and VLAN membership.</p> <p>In addition to seeing if STG is enabled or disabled, you can view the following STG bridge information:</p> <ul style="list-style-type: none"> <li>– Priority</li> <li>– Hello interval</li> <li>– Maximum age value</li> <li>– Forwarding delay</li> <li>– Aging time</li> </ul> <p>You can also see the following port-specific STG information:</p> <ul style="list-style-type: none"> <li>– Port alias and priority</li> <li>– Cost</li> <li>– State</li> </ul> <p><b>Command mode:</b> All</p>

Table 220. Spanning Tree Configuration Options (continued)

Command Syntax and Usage
<pre>show spanning-tree root</pre> <p>Displays the Spanning Tree configuration on the root bridge for each STP instance. For details, see <a href="#">page 51</a>.</p> <p><b>Command mode:</b> All</p>
<pre>show spanning-tree blockedports</pre> <p>Lists the ports blocked by each STP instance.</p> <p><b>Command mode:</b> All</p>
<pre>show spanning-tree [vlan &lt;VLAN ID&gt;] bridge</pre> <p>Displays Spanning Tree bridge information. For details, see <a href="#">page 51</a>.</p> <p><b>Command mode:</b> All</p>

## MSTP Configuration

Up to 32 Spanning Tree Groups can be configured in MSTP mode. MSTP is turned off by default and the default STP mode is PVRST.

**Note:** When Multiple Spanning Tree is turned on, VLAN 4095 is moved from Spanning Tree Group 128 to the Common Internal Spanning Tree (CIST). When Multiple Spanning Tree is turned off, VLAN 4095 is moved back to Spanning Tree Group 128.

Table 221. Multiple Spanning Tree Configuration Options

Command Syntax and Usage
<pre>spanning-tree mst configuration</pre> <p>Enables MSTP configuration mode.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>[no] name &lt;1-32 characters&gt;</pre> <p>Configures a name for the MSTP region. All devices within an MSTP region must have the same region name.</p> <p><b>Command mode:</b> MST configuration</p>
<pre>[no] revision &lt;0-65535&gt;</pre> <p>Configures a revision number for the MSTP region. The revision is used as a numerical identifier for the region. All devices within an MSTP region must have the same revision number.</p> <p><b>Command mode:</b> MST configuration</p>
<pre>spanning-tree mst max-hops &lt;4-60&gt;</pre> <p>Configures the maximum number of bridge hops a packet may traverse before it is dropped. The default value is 20.</p> <p><b>Command mode:</b> Global configuration</p>

Table 221. Multiple Spanning Tree Configuration Options (continued)

Command Syntax and Usage	
[no] spanning-tree mst <0-32> enable	<p>Enables or disables the specified MSTP instance.</p> <p><b>Command mode:</b> Global configuration</p>
spanning-tree mst forward-time <4-30>	<p>Configures the forward delay time in seconds. 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. Default value is 15.</p> <p><b>Command mode:</b> Global configuration</p>
spanning-tree mst max-age <6-40>	<p>Configures the maximum age interval in seconds. 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. Default value is 20.</p> <p><b>Command mode:</b> Global configuration</p>
default spanning-tree mst <0-32>	<p>Restores the Spanning Tree instance to its default configuration.</p> <p><b>Command mode:</b> Global configuration</p>
instance <0-32> vlan <VLAN numbers>	<p>Map the specified VLANs to the Spanning Tree instance. If a VLAN does not exist, it will be created automatically, but it will not be enabled by default.</p> <p><b>Command mode:</b> MST configuration</p>
no instance <0-32> vlan {<VLAN numbers> all}	<p>Remove the specified VLANs or all VLANs from the Spanning Tree instance.</p> <p><b>Command mode:</b> MST configuration</p>
spanning-tree mst <0-32> priority <0-65535>	<p>Configures the CIST bridge priority for the specified MSTP instance. 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...); the default value is 32768.</p> <p><b>Command mode:</b> Global configuration</p>
no spanning-tree mst configuration	<p>Returns the MST region to its default values: no VLAN is mapped to any MST instance. Revision number is 1.</p> <p><b>Command mode:</b> Global configuration</p>

Table 221. Multiple Spanning Tree Configuration Options (continued)

Command Syntax and Usage
<pre>show spanning-tree mst &lt;0-32&gt; information</pre> <p>Displays current MST information for the specified instance.</p> <p><b>Command mode:</b> All</p>
<pre>show spanning-tree mst configuration</pre> <p>Displays the current MSTP settings.</p> <p><b>Command mode:</b> All</p>

## MSTP Port Configuration

MSTP port parameters are used to modify MSTP operation on an individual port basis. MSTP parameters do not affect operation of STP/PVST+. For each port, RSTP/MSTP is turned on by default.

Table 222. MSTP Port Configuration Options

Command Syntax and Usage
<pre>spanning-tree mst &lt;0-32&gt; port-priority &lt;0-240&gt;</pre> <p>Configures the port priority for the specified MSTP instance. The port priority helps determine which bridge port becomes the designated port. In a network topology that has multiple bridge ports connected to a single segment, the port with the lowest port priority becomes the designated port for the segment.</p> <p>The range is 0 to 240, in steps of 16 (0, 16, 32...), and the default is 128.</p> <p><b>Command mode:</b> Interface port/Interface portchannel</p>
<pre>spanning-tree mst &lt;0-32&gt; cost &lt;0-2000000000&gt;</pre> <p>Configures the port path cost for the specified MSTP instance. The port path cost is used to help determine the designated port for a segment. Port path cost is based on the port speed, and is calculated as follows:</p> <ul style="list-style-type: none"> <li>– 1Gbps = 20000</li> <li>– 10Gbps = 2000</li> </ul> <p>The default value of 0 (zero) indicates that the default path cost will be computed for an auto negotiated link speed.</p> <p><b>Command mode:</b> Interface port/Interface portchannel</p>
<pre>spanning-tree mst hello-time &lt;1-10&gt;</pre> <p>Configures the port Hello time. The Hello time specifies how often the root bridge transmits a configuration bridge protocol data unit (BPDU). Any bridge that is not the root bridge uses the root bridge Hello value. The range is 1 to 10 seconds, and the default is 2 seconds.</p> <p><b>Command mode:</b> Interface port/Interface portchannel</p>

Table 222. MSTP Port Configuration Options (continued)

Command Syntax and Usage
<pre>[no] spanning-tree pvst-protection</pre> <p>Configures PVST Protection on the selected port. If the port receives any PVST+/PVRST BPDUs, it error disabled. PVST Protection works only in MSTP mode. The default setting is disabled.</p> <p><b>Note:</b> Not available in stacking.</p> <p><b>Command mode:</b> Interface port</p>
<pre>[no] spanning-tree mst &lt;0-32&gt; enable</pre> <p>Enables or disables the specified MSTP instance on the port.</p> <p><b>Command mode:</b> Interface port/Interface portchannel</p>
<pre>show interface port &lt;port alias or number&gt; spanning-tree mstp cist</pre> <p>Displays the current CIST port configuration.</p> <p><b>Command mode:</b> All</p>

## RSTP/PVRST Configuration

Table 223 describes the commands used to configure the Rapid Spanning Tree (RSTP) and Per VLAN Rapid Spanning Tree Protocol (PVRST) protocols.

Table 223. RSTP/PVRST Configuration Options

Command Syntax and Usage
<pre>spanning-tree stp &lt;STG number&gt; vlan &lt;VLAN number&gt;</pre> <p>Associates a VLAN with a Spanning Tree Group and requires a VLAN ID as a parameter. If the VLAN does not exist, it will be created automatically, but it will not be enabled by default.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>no spanning-tree stp &lt;STG number&gt; vlan &lt;VLAN number&gt;</pre> <p>Breaks the association between a VLAN and a Spanning Tree Group and requires a VLAN ID as a parameter.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>no spanning-tree stp &lt;STG number&gt; vlan all</pre> <p>Removes all VLANs from a Spanning Tree Group.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>spanning-tree stp &lt;STG number&gt; enable</pre> <p>Globally enables Spanning Tree Protocol. STG is turned on by default.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>no spanning-tree stp &lt;STG number&gt; enable</pre> <p>Globally disables Spanning Tree Protocol.</p> <p><b>Command mode:</b> Global configuration</p>

Table 223. RSTP/PVRST Configuration Options (continued)

Command Syntax and Usage
<pre>default spanning-tree &lt;STG number&gt;</pre> <p>Restores a Spanning Tree instance to its default configuration.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>show spanning-tree stp &lt;STG number&gt;</pre> <p>Displays current Spanning Tree Protocol parameters for the specified Spanning Tree Group. See <a href="#">page 47</a> for details about the <code>information</code> parameter.</p> <p><b>Command mode:</b> All</p>

## Bridge RSTP/PVRST Configuration

Spanning Tree bridge parameters affect the global STG operation of the switch. STG bridge parameters include:

- Bridge priority
- Bridge hello time
- Bridge maximum age
- Forwarding delay

Table 224. Bridge Spanning Tree Configuration Options

Command Syntax and Usage
<pre>spanning-tree stp &lt;STG number&gt; bridge priority &lt;0-65535&gt;</pre> <p>Configures the bridge priority. The bridge priority parameter controls which bridge on the network is the STG root bridge. To make this switch the root bridge, configure the bridge priority lower than all other switches and bridges on your network. The lower the value, the higher the bridge priority. Enter the value in multiples of 4096. Non-multiples are automatically rounded up to the closest valid priority. The default value is 61440.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>spanning-tree stp &lt;STG number&gt; bridge hello-time &lt;1-10&gt;</pre> <p>Configures the bridge Hello time. The Hello time specifies how often the root bridge transmits a configuration bridge protocol data unit (BPDU). Any bridge that is not the root bridge uses the root bridge Hello value. The range is 1 to 10 seconds, and the default is 2 seconds.</p> <p>This command does not apply to MSTP.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>spanning-tree stp &lt;STG number&gt; bridge maximum-age &lt;6-40&gt;</pre> <p>Configures the bridge maximum age. The maximum age parameter specifies the maximum time the bridge waits without receiving a configuration bridge protocol data unit before it re configures the STG network. The range is 6 to 40 seconds, and the default is 20 seconds.</p> <p>This command does not apply to MSTP.</p> <p><b>Command mode:</b> Global configuration</p>



Table 224. Bridge Spanning Tree Configuration Options

Command Syntax and Usage
<pre>spanning-tree stp &lt;STG number&gt; bridge forward-delay &lt;4-30&gt;</pre> <p>Configures the bridge forward delay parameter. The forward delay parameter specifies the amount of time that a bridge port has to wait before it changes from the listening state to the learning state and from the learning state to the forwarding state. The range is 4 to 30 seconds, and the default is 15 seconds.</p> <p>This command does not apply to MSTP</p> <p><b>Command mode:</b> Global configuration</p>
<pre>show spanning-tree [vlan &lt;VLAN ID&gt;] bridge</pre> <p>Displays the current Spanning Tree parameters either globally or for a specific VLAN. See <a href="#">page 51</a> for sample output.</p> <p><b>Command mode:</b> All</p>

When configuring STG bridge parameters, the following formulas must be used:

- $2*(fwd-1) \geq mxage$
- $2*(hello+1) \leq mxage$

### RSTP/PVRST Port Configuration

By default, Spanning Tree is turned `off` for management ports, and turned `on` for data ports. STG port parameters include:

- Port priority
- Port path cost

Table 225. Spanning Tree Port Options

Command Syntax and Usage
<pre>spanning-tree stp &lt;STG number&gt; priority &lt;0-240&gt;</pre> <p>Configures the port priority. The port priority helps determine which bridge port becomes the designated port. In a network topology that has multiple bridge ports connected to a single segment, the port with the lowest port priority becomes the designated port for the segment. The default value is 128.</p> <p><b>RSTP/MSTP:</b> The range is 0 to 240, in steps of 16 (0, 16, 32...) and the default is 128.</p> <p><b>Command mode:</b> Interface port</p>
<pre>spanning-tree stp &lt;STG number&gt; path-cost &lt;1-200000000, 0 for default&gt;</pre> <p>Configures the port path cost. The port path cost is used to help determine the designated port for a segment. Port path cost is based on the port speed, and is calculated as follows:</p> <ul style="list-style-type: none"> <li>– 1Gbps = 20000</li> <li>– 10Gbps = 2000</li> </ul> <p>The default value of 0 (zero) indicates that the default path cost will be computed for an auto negotiated link speed.</p> <p><b>Command mode:</b> Interface port</p>

Table 225. Spanning Tree Port Options (continued)

Command Syntax and Usage
<pre>spanning-tree stp link-type {auto p2p shared}</pre> <p>Defines the type of link connected to the port, as follows:</p> <ul style="list-style-type: none"> <li>– auto: Configures the port to detect the link type, and automatically match its settings.</li> <li>– p2p: Configures the port for Point-To-Point protocol.</li> <li>– shared: Configures the port to connect to a shared medium (usually a hub).</li> </ul> <p><b>Command mode:</b> Interface port</p>
<pre>spanning-tree stp &lt;STG number&gt; enable</pre> <p>Enables STG on the port.</p> <p><b>Command mode:</b> Interface port</p>
<pre>no spanning-tree stp &lt;STG number&gt; enable</pre> <p>Disables STG on the port.</p> <p><b>Command mode:</b> Interface port</p>
<pre>show interface port &lt;port alias or number&gt; spanning-tree stp &lt;STG number&gt;</pre> <p>Displays the current STG port parameters.</p> <p><b>Command mode:</b> All</p>

## Forwarding Database Configuration

Use the following commands to configure the Forwarding Database (FDB).

Table 226. FDB Configuration Options

Command Syntax and Usage
<pre>mac-address-table aging &lt;0-65535&gt;</pre> <p>Configures the aging value for FDB entries, in seconds. The default value is 300.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>show mac-address-table</pre> <p>Display current FDB configuration.</p> <p><b>Command mode:</b> All except User EXEC</p>

## Static Multicast MAC Configuration

The following options are available to control the forwarding of known and unknown multicast packets:

- All multicast packets are flooded to the entire VLAN. This is the default switch behavior.
- Known multicast packets are forwarded only to those ports specified. Unknown multicast packets are flooded to the entire VLAN. To configure this option, define the Multicast MAC address for the VLAN and specify ports that are to receive multicast packets (`mac-address-table multicast`).
- Known multicast packets are forwarded only to those ports specified. Unknown multicast packets are dropped. To configure this option:
  - Define the Multicast MAC address for the VLAN and specify ports that are to receive multicast packets (`mac-address-table multicast`).
  - Enable Flood Blocking on ports that are not to receive multicast packets (`interface port x`) (`flood-blocking`).

Use the following commands to configure static Multicast MAC entries in the Forwarding Database (FDB).

Table 227. Static Multicast MAC Configuration Options

Command Syntax and Usage
<pre>mac-address-table multicast &lt;MAC address&gt; &lt;VLAN number&gt;   {port &lt;port alias or number&gt;}</pre> <p>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:</p> <pre>mac-address-table multicast 01:00:00:23:3f:01 200 1-4</pre> <p><b>Command mode:</b> Global configuration</p>
<pre>mac-address-table multicast &lt;cluster MAC address&gt;   port &lt;port number or range&gt;}</pre> <p>Adds a static multicast entry for Network Load Balancing (NLB). You can list ports separated by a comma, or enter a range of ports separated by a hyphen (-). For example:</p> <pre>mac-address-table multicast 01:00:00:23:3f:01 port 1-4</pre> <p><b>Command mode:</b> Global configuration</p>
<pre>no mac-address-table multicast {all &lt;MAC address&gt; &lt;VLAN number&gt;}</pre> <p>Deletes a static multicast entry.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>show mac-address-table multicast</pre> <p>Display the current static multicast entries.</p> <p><b>Command mode:</b> All</p>

## Static FDB Configuration

Use the following commands to configure static entries in the Forwarding Database (FDB).

Table 228. FDB Configuration Options

Command Syntax and Usage
<pre>mac-address-table static &lt;MAC address&gt; vlan &lt;VLAN number&gt;   {port &lt;port alias or number&gt; portchannel &lt;trunk number&gt;    adminkey &lt;1-65535&gt;}   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:   xxxxxxxxxxxxxx   For example, 080020123456   <b>Command mode:</b> Global configuration</pre>
<pre>no mac-address-table static [&lt;MAC address&gt;] [&lt;VLAN number&gt;]  all   Deletes permanent FDB entries.   <b>Command mode:</b> Global configuration</pre>
<pre>show mac-address-table   Display current FDB configuration.   <b>Command mode:</b> All except User EXEC</pre>

## ECP Configuration

Use the following commands to configure Edge Control Protocol (ECP).

Table 229. ECP Configuration Options

Command Syntax and Usage
<pre>ecp retransmit-interval &lt;100-9000&gt;   Configures ECP retransmit interval in milliseconds. Default value is 1000.   <b>Command mode:</b> Global configuration</pre>
<pre>default ecp retransmit-interval   Resets the ECP retransmit interval to the default 1000 milliseconds.   <b>Command mode:</b> Global configuration</pre>
<pre>show ecp [channels upper-layer-protocols]   Displays settings for all ECP channels or registered ULPs.   <b>Command mode:</b> All</pre>

## LLDP Configuration

Use the following commands to configure Link Layer Detection Protocol (LLDP).

Table 230. LLDP Configuration Options

Command Syntax and Usage	
<code>lldp refresh-interval &lt;5-32768&gt;</code>	Configures the message transmission interval, in seconds. The default value is 30. <b>Command mode:</b> Global configuration
<code>lldp holdtime-multiplier &lt;2-10&gt;</code>	Configures the message hold time multiplier. The hold time is configured as a multiple of the message transmission interval. The default value is 4. <b>Command mode:</b> Global configuration
<code>lldp trap-notification-interval &lt;1-3600&gt;</code>	Configures the trap notification interval, in seconds. The default value is 5. <b>Command mode:</b> Global configuration
<code>lldp transmission-delay &lt;1-8192&gt;</code>	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. <b>Command mode:</b> Global configuration
<code>lldp reinit-delay &lt;1-10&gt;</code>	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. <b>Command mode:</b> Global configuration
<code>lldp enable</code>	Globally turns LLDP on. The default setting is on. <b>Command mode:</b> Global configuration
<code>no lldp enable</code>	Globally turns LLDP off. <b>Command mode:</b> Global configuration
<code>show lldp [port &lt;port_number&gt;]</code>	Display current LLDP configuration. <b>Command mode:</b> All

## LLDP Port Configuration

Use the following commands to configure LLDP port options.

Table 231. LLDP Port Options

Command Syntax and Usage
<pre>lldp admin-status {tx_only rx_only tx_rx}</pre> <p>Configures the LLDP transmission type for the port, as follows:</p> <ul style="list-style-type: none"><li>– Transmit only</li><li>– Receive only</li><li>– Transmit and receive</li><li>–</li></ul> <p>The default setting is <code>tx_rx</code>.</p> <p><b>Command mode:</b> Interface port</p>
<pre>no lldp admin-status</pre> <p>Disables the LLDP transmission type.</p> <p><b>Command mode:</b> Interface port</p>
<pre>[no] lldp trap-notification</pre> <p>Enables or disables SNMP trap notification for LLDP messages.</p> <p><b>Command mode:</b> Interface port</p>
<pre>show interface port &lt;port alias or number&gt; lldp</pre> <p>Display current LLDP port configuration.</p> <p><b>Command mode:</b> All</p>

## LLDP Optional TLV configuration

Use the following commands to configure LLDP port TLV (Type, Length, Value) options for the selected port.

Table 232. *Optional TLV Options*

Command Syntax and Usage
[no] lldp tlv portdesc Enables or disables the Port Description information type. <b>Command mode:</b> Interface port
[no] lldp tlv sysname Enables or disables the System Name information type. <b>Command mode:</b> Interface port
[no] lldp tlv sysdescr Enables or disables the System Description information type. <b>Command mode:</b> Interface port
[no] lldp tlv syscap Enables or disables the System Capabilities information type. <b>Command mode:</b> Interface port
[no] lldp tlv mgmtaddr Enables or disables the Management Address information type. <b>Command mode:</b> Interface port
[no] lldp tlv portvid Enables or disables the Port VLAN ID information type. <b>Command mode:</b> Interface port
[no] lldp tlv portprot Enables or disables the Port and VLAN Protocol ID information type. <b>Command mode:</b> Interface port
[no] lldp tlv vlanname Enables or disables the VLAN Name information type. <b>Command mode:</b> Interface port
[no] lldp tlv protid Enables or disables the Protocol ID information type. <b>Command mode:</b> Interface port
[no] lldp tlv macphy Enables or disables the MAC/Phy Configuration information type. <b>Command mode:</b> Interface port

Table 232. Optional TLV Options (continued)

Command Syntax and Usage
<pre>[no] lldp tlv powermdi</pre> <p>Enables or disables the Power via MDI information type.  <b>Command mode:</b> Interface port</p>
<pre>[no] lldp tlv linkaggr</pre> <p>Enables or disables the Link Aggregation information type.  <b>Command mode:</b> Interface port</p>
<pre>[no] lldp tlv framesz</pre> <p>Enables or disables the Maximum Frame Size information type.  <b>Command mode:</b> Interface port</p>
<pre>[no] lldp tlv dcbx</pre> <p>Enables or disables the Maximum Frame Size information type.  <b>Command mode:</b> Interface port</p>
<pre>[no] lldp tlv all</pre> <p>Enables or disables all optional TLV information types.  <b>Command mode:</b> Interface port</p>
<pre>show interface port &lt;port alias or number&gt; lldp</pre> <p>Display current LLDP port configuration.  <b>Command mode:</b> All</p>



## 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 32 ports can belong to the same trunk group.
- You must configure all ports in a trunk group with the same properties (speed, duplex, flow control, STG, VLAN, and so on).
- Trunking from non-IBM devices must comply with Cisco® EtherChannel® technology.

By default, each trunk group is empty and disabled.

Table 233. 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 ( - ). <b>Command mode:</b> Global configuration
no portchannel <1-64> port <port alias or number>	Removes a physical port or ports from the current trunk group. <b>Command mode:</b> Global configuration
[no] portchannel <1-64> enable	Enables or Disables the current trunk group. <b>Command mode:</b> Global configuration
no portchannel <1-64>	Removes the current trunk group configuration. <b>Command mode:</b> Global configuration
show portchannel <1-64>	Displays current trunk group parameters. <b>Command mode:</b> All

## Trunk Hash Configuration

Use the following commands to configure trunk hash settings 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 234](#) combined with the hash parameters listed in [Table 235](#) and [Table 236](#).

Table 234. Trunk Hash Options

Command Syntax and Usage
<pre>[no] portchannel thash ingress</pre> <p>Enables or disables trunk hash computation based on the ingress port. The default setting is disabled.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>[no] portchannel thash L4port</pre> <p>Enables or disables use of Layer 4 service ports (TCP, UDP, and so on) to compute the hash value. The default setting is disabled.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>show portchannel hash</pre> <p>Display current trunk hash configuration.</p> <p><b>Command mode:</b> All</p>

## Layer 2 Trunk Hash

Layer 2 trunk hash parameters are set globally. You can enable one or both parameters, to configure any of the following valid combinations:

- SMAC (source MAC only)
- DMAC (destination MAC only)
- SMAC and DMAC

Use the following commands to configure Layer 2 trunk hash parameters for the switch.

Table 235. Layer 2 Trunk Hash Options

Command Syntax and Usage
<pre>[no] portchannel thash l2hash l2-source-mac-address</pre> <p>Enables or disables Layer 2 trunk hashing on the source MAC.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>[no] portchannel thash l2hash l2-destination-mac-address</pre> <p>Enables or disables Layer 2 trunk hashing on the destination MAC.</p> <p><b>Command mode:</b> Global configuration</p>

Table 235. Layer 2 Trunk Hash Options

Command Syntax and Usage
<pre>[no] portchannel thash l2hash l2-source-destination-mac</pre> <p>Enables or disables Layer 2 trunk hashing on both the source and destination MAC.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>show portchannel hash</pre> <p>Displays the current trunk hash settings.</p> <p><b>Command mode:</b> All</p>

## Layer 3 Trunk Hash

Layer 3 trunk hash parameters are set globally. You can enable one or both parameters, to configure any of the following valid combinations:

- SIP (source IP only)
- DIP (destination IP only)
- SIP and DIP

Use the following commands to configure Layer 3 trunk hash parameters for the switch.

Table 236. Layer 3 Trunk Hash Options

Command Syntax and Usage
<pre>[no] portchannel thash l3thash l3-use-l2-hash</pre> <p>Enables or disables use of Layer 2 hash parameters only. When enabled, Layer 3 hashing parameters are cleared.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>[no] portchannel thash l3thash l3-source-ip-address</pre> <p>Enables or disables Layer 3 trunk hashing on the source IP address.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>[no] portchannel thash l3thash l3-destination-ip-address</pre> <p>Enables or disables Layer 3 trunk hashing on the destination IP address.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>[no] portchannel thash l3thash l3-source-destination-ip</pre> <p>Enables or disables Layer 3 trunk hashing on both the source and the destination IP address.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>show portchannel hash</pre> <p>Displays the current trunk hash settings.</p> <p><b>Command mode:</b> All</p>

## 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 237. vLAG Configuration Options

Command Syntax and Usage
<pre>[no] vlag portchannel &lt;trunk group number&gt; enable</pre> <p>Enables or disables vLAG on the selected trunk group.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>[no] vlag adminkey &lt;1-65535&gt; enable</pre> <p>Enables or disables vLAG on the selected LACP <i>admin key</i>. LACP trunks formed with this <i>admin key</i> will be included in the vLAG configuration.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>[no] vlag enable</pre> <p>Enables or disables vLAG globally.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>[no] vlag tier-id &lt;1-512&gt;</pre> <p>Sets the vLAG peer ID.</p>
<pre>vlag priority &lt;0-65535&gt;</pre> <p>Configures the vLAG priority for the switch, used for election of Primary and Secondary vLAG switches. The switch with lower priority is elected to the role of Primary vLAG switch.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>vlag auto-recovery &lt;240-3600&gt;</pre> <p>Sets the duration in seconds of the auto-recovery timer. This timer configures how long after boot-up configuration load, the switch can assume the Primary role from an unresponsive ISL peer and bring up the vLAG ports.</p> <p>The default value is 300.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>no vlag auto-recovery</pre> <p>Sets the auto-recovery timer to the default 300 seconds duration.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>vlag startup-delay &lt;0-3600&gt;</pre> <p>Sets, in seconds, the vLAG startup delay interval. The default value is 120.</p> <p><b>Command mode:</b> Global configuration</p>

Table 237. vLAG Configuration Options

Command Syntax and Usage
<pre>no vlag startup-delay</pre> <p>Sets the vLAG startup-delay timer to the default 120 seconds duration.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>show vlag</pre> <p>Displays current vLAG parameters.</p> <p><b>Command mode:</b> All</p>

## vLAG Health Check Configuration

These commands enable you to configure a way to check the health status of the vLAG peer.

Table 238. vLAG Health Check Configuration Options

Command Syntax and Usage
<pre>[no] vlag hlthchk peer-ip {&lt;IPv4 address&gt;/&lt;IPv6 address&gt;}</pre> <p>Configures the IP address of the peer switch, used for health checks. Use the management IP address of the peer switch. The default value is 0.0.0.0.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>[no] vlag hlthchk connect-retry-interval &lt;1-300&gt;</pre> <p>Sets, in seconds, the vLAG health check connect retry interval. The default value is 30.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>[no] vlag hlthchk keepalive-attempts &lt;1-24&gt;</pre> <p>Sets the number of vLAG keep alive attempts. The default value is 3.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>[no] vlag hlthchk keepalive-interval &lt;2-300&gt;</pre> <p>Sets, in seconds, the time between vLAG keep alive attempts. The default value is 5.</p> <p><b>Command mode:</b> Global configuration</p>

## vLAG ISL Configuration

These commands allow you to configure a dedicated inter-switch link (ISL) for synchronization between vLAG peers.

Table 239. vLAG ISL Configuration Options

Command Syntax and Usage
<pre>[no] vlag isl portchannel &lt;portchannel ID&gt;</pre> <p>Enables or disables vLAG Inter-Switch Link (ISL) on the selected trunk group.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>[no] vlag isl adminkey &lt;I-65535&gt;</pre> <p>Enables or disables vLAG Inter-Switch Link (ISL) on the selected LACP <i>admin key</i>. LACP trunks formed with this <i>admin key</i> will be included in the ISL.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>show vlag</pre> <p>Displays current vLAG parameters.</p> <p><b>Command mode:</b> All</p>

## Link Aggregation Control Protocol Configuration

Use the following commands to configure Link Aggregation Control Protocol (LACP) for the G8264.

Table 240. Link Aggregation Control Protocol Options

Command Syntax and Usage
<pre>lacp system-priority &lt;I-65535&gt;</pre> <p>Defines the priority value for the G8264. Lower numbers provide higher priority. The default value is 32768.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>lacp timeout {short long}</pre> <p>Defines the timeout period before invalidating LACP data from a remote partner. Choose <i>short</i> (3 seconds) or <i>long</i> (90 seconds). The default value is <i>long</i>.</p> <p><b>Note:</b> To reduce LACPDU processing, use a timeout value of <i>long</i>. If your G8264's CPU utilization rate remains at 100% for periods of 90 seconds or more, consider using static trunks instead of LACP.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>no lacp &lt;I-65535&gt;</pre> <p>Deletes a selected LACP trunk, based on its <i>admin key</i>. This command is equivalent to disabling LACP on each of the ports configured with the same <i>admin key</i>.</p> <p><b>Command mode:</b> Global configuration</p>

Table 240. Link Aggregation Control Protocol Options

Command Syntax and Usage
<pre>portchannel &lt;trunk ID&gt; lacp key &lt;1-65535&gt; suspend-individual</pre> <p>Enables a static LACP trunk. In this mode, ports sharing the same LACP admin key can form a single trunk, with the specified trunk ID. The active trunk is picked based on the ports which occupy first the trunk ID. Member ports that cannot join this trunk are prohibited from forming secondary LACP groups. Instead, they are set in a suspended state where they discard all non-LACP traffic.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>no portchannel &lt;trunk ID&gt;</pre> <p>Disables a static LACP trunk.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>show lacp</pre> <p>Display current LACP configuration.</p> <p><b>Command mode:</b> All</p>

## LACP Port Configuration

Use the following commands to configure Link Aggregation Control Protocol (LACP) for the selected port.

Table 241. LACP Port Options

Command Syntax and Usage
<pre>lacp mode {off active passive}</pre> <p>Set the LACP mode for this port, as follows:</p> <ul style="list-style-type: none"> <li>– <b>off</b> Turn LACP off for this port. You can use this port to manually configure a static trunk. The default value is <code>off</code>.</li> <li>– <b>active</b> Turn LACP on and set this port to active. Active ports initiate LACPDUs.</li> <li>– <b>passive</b> Turn LACP on and set this port to passive. Passive ports do not initiate LACPDUs, but respond to LACPDUs from active ports.</li> </ul> <p><b>Command mode:</b> Interface port</p>
<pre>lacp priority &lt;1-65535&gt;</pre> <p>Sets the priority value for the selected port. Lower numbers provide higher priority. The default value is 32768.</p> <p><b>Command mode:</b> Interface port</p>
<pre>lacp key &lt;1-65535&gt;</pre> <p>Set the <i>admin key</i> for this port. Only ports with the same <i>admin key</i> and <i>oper key</i> (operational state generated internally) can form a LACP trunk group.</p> <p><b>Command mode:</b> Interface port</p>

Table 241. LACP Port Options

Command Syntax and Usage
<pre>port-channel min-links &lt;1-32&gt;</pre> <p>Set the minimum number of links for this port. If the specified minimum number of ports are not available, the trunk is placed in the <code>down</code> state.</p> <p><b>Command mode:</b> Interface port</p>
<pre>default lacp [key   mode   priority]</pre> <p>Restores the selected parameters to their default values.</p> <p><b>Command mode:</b> Interface port</p>
<pre>default port-channel min-links</pre> <p>Restores the minimum number of links for this port to its default value.</p> <p><b>Command mode:</b> Interface port</p>
<pre>show interface port &lt;port alias or number&gt; lacp</pre> <p>Displays the current LACP configuration for this port.</p> <p><b>Command mode:</b> All</p>

## Layer 2 Failover Configuration

Use these commands to configure Layer 2 Failover. For more information about Layer 2 Failover, see “High Availability” in the *IBM N/OS Application Guide*.

Table 242. Layer 2 Failover Configuration Options

Command Syntax and Usage
<pre>failover enable</pre> <p>Globally turns Layer 2 Failover <code>on</code>.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>no failover enable</pre> <p>Globally turns Layer 2 Failover <code>off</code>.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>show failover trigger</pre> <p>Displays current Layer 2 Failover parameters.</p> <p><b>Command mode:</b> All</p>



## Failover Trigger Configuration

Table 243. Failover Trigger Configuration Options

Command Syntax and Usage
<pre>[no] failover trigger &lt;I-8&gt; enable</pre> <p>Enables or disables the Failover trigger. <b>Command mode:</b> Global configuration</p>
<pre>no failover trigger &lt;I-8&gt;</pre> <p>Deletes the Failover trigger. <b>Command mode:</b> Global configuration</p>
<pre>failover trigger &lt;I-8&gt; limit &lt;0-1024&gt;</pre> <p>Configures the minimum number of operational links allowed within each trigger before the trigger initiates a failover event. If you enter a value of zero (0), the switch triggers a failover event only when no links in the trigger are operational. <b>Command mode:</b> Global configuration</p>
<pre>show failover trigger &lt;I-8&gt;</pre> <p>Displays the current failover trigger settings. <b>Command mode:</b> All</p>

## 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 244. Failover Manual Monitor Port Options

Command Syntax and Usage
<pre>failover trigger &lt;I-8&gt; mmon monitor member &lt;port alias or number&gt;</pre> <p>Adds the selected port to the Manual Monitor Port configuration. <b>Command mode:</b> Global configuration</p>
<pre>no failover trigger &lt;I-8&gt; mmon monitor member &lt;port alias or number&gt;</pre> <p>Removes the selected port from the Manual Monitor Port configuration. <b>Command mode:</b> Global configuration</p>
<pre>failover trigger &lt;I-8&gt; mmon monitor portchannel &lt;trunk number&gt;</pre> <p>Adds the selected trunk group to the Manual Monitor Port configuration. <b>Command mode:</b> Global configuration</p>
<pre>no failover trigger &lt;I-8&gt; mmon monitor portchannel &lt;trunk number&gt;</pre> <p>Removes the selected trunk group from the Manual Monitor Port configuration. <b>Command mode:</b> Global configuration</p>

Table 244. Failover Manual Monitor Port Options

Command Syntax and Usage
<pre>failover trigger &lt;I-8&gt; mmon monitor adminkey &lt;I-65535&gt;</pre> <p>Adds an LACP <i>admin key</i> to the Manual Monitor Port configuration. LACP trunks formed with this admin key will be included in the Manual Monitor Port configuration.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>no failover trigger &lt;I-8&gt; mmon monitor adminkey &lt;I-65535&gt;</pre> <p>Removes an LACP <i>admin key</i> from the Manual Monitor Port configuration.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>show failover trigger &lt;I-8&gt;</pre> <p>Displays the current Failover settings.</p> <p><b>Command mode:</b> All</p>

## 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 245. Failover Manual Monitor Control Options

Command Syntax and Usage
<pre>failover trigger &lt;I-8&gt; mmon control member &lt;port alias or number&gt;</pre> <p>Adds the selected port to the Manual Monitor Control configuration.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>no failover trigger &lt;I-8&gt; mmon control member &lt;port alias or number&gt;</pre> <p>Removes the selected port from the Manual Monitor Control configuration.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>failover trigger &lt;I-8&gt; mmon control portchannel &lt;trunk number&gt;</pre> <p>Adds the selected trunk group to the Manual Monitor Control configuration.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>no failover trigger &lt;I-8&gt; mmon control portchannel &lt;trunk number&gt;</pre> <p>Removes the selected trunk group from the Manual Monitor Control configuration.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>failover trigger &lt;I-8&gt; mmon control adminkey &lt;I-65535&gt;</pre> <p>Adds an LACP <i>admin key</i> to the Manual Monitor Control configuration. LACP trunks formed with this admin key will be included in the Manual Monitor Control configuration.</p> <p><b>Command mode:</b> Global configuration</p>

Table 245. Failover Manual Monitor Control Options

Command Syntax and Usage
<pre>no failover trigger &lt;1-8&gt; mmon control adminkey &lt;1-65535&gt;</pre> <p>Removes an LACP <i>admin key</i> from the Manual Monitor Control configuration.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>show failover trigger &lt;1-8&gt;</pre> <p>Displays the current Failover settings.</p> <p><b>Command mode:</b> All</p>

## Hot Links Configuration

Use these commands to configure Hot Links. For more information about Hot Links, see “Hot Links” in the *IBM N/OS 7.6 Application Guide*.

Table 246. Hot Links Configuration Options

Command Syntax and Usage
<pre>[no] hotlinks bpdu</pre> <p>Enables or disables flooding of Spanning-Tree BPDUs on the active Hot Links interface when the interface belongs to a Spanning Tree group that is globally turned <code>off</code>. This feature can prevent unintentional loop scenarios (for example, if two uplinks come up at the same time).</p> <p>The default setting is <code>disabled</code>.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>[no] hotlinks fdb-update</pre> <p>Enables or disables FDB Update, which allows the switch to send FDB and MAC update packets over the active interface.</p> <p>The default value is <code>disabled</code>.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>hotlinks fdb-update-rate &lt;10-1000&gt;</pre> <p>Configures the FDB Update rate in packets per second.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>hotlinks enable</pre> <p>Globally enables Hot Links.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>no hotlinks enable</pre> <p>Globally disables Hot Links.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>show hotlinks</pre> <p>Displays current Hot Links parameters.</p> <p><b>Command mode:</b> All</p>

## Hot Links Trigger Configuration

Table 247. Hot Links Trigger Configuration Options

Command Syntax and Usage	
hotlinks trigger <1-200> forward-delay <0-3600>	Configures the Forward Delay interval, in seconds. The default value is 1. <b>Command mode:</b> Global configuration
[no] hotlinks trigger <1-200> name <1-32 characters>	Defines a name for the Hot Links trigger. <b>Command mode:</b> Global configuration
[no] hotlinks trigger <1-200> preemption	Enables or disables pre-emption, which allows the Master interface to transition to the Active state whenever it becomes available. The default setting is enabled. <b>Command mode:</b> Global configuration
[no] hotlinks trigger <1-200> enable	Enables or disables the Hot Links trigger. <b>Command mode:</b> Global configuration
no hotlinks trigger <1-200>	Deletes the Hot Links trigger. <b>Command mode:</b> Global configuration
show hotlinks trigger <1-200>	Displays the current Hot Links trigger settings. <b>Command mode:</b> All

## Hot Links Master Configuration

Use the following commands to configure the Hot Links Master interface.

Table 248. Hot Links Master Configuration Options

Command Syntax and Usage
<pre>[no] hotlinks trigger &lt;1-200&gt; master port &lt;port alias or number&gt;</pre> <p>Adds or removes the selected port to the Hot Links Master interface.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>[no] hotlinks trigger &lt;1-200&gt; master portchannel &lt;trunk group number&gt;</pre> <p>Adds or removes the selected trunk group to the Master interface.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>[no] hotlinks trigger &lt;1-200&gt; master adminkey &lt;0-65535&gt;</pre> <p>Adds or removes an LACP <i>admin key</i> to the Master interface. LACP trunks formed with this <i>admin key</i> will be included in the Master interface.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>show hotlinks trigger &lt;1-200&gt;</pre> <p>Displays the current Hot Links trigger settings.</p> <p><b>Command mode:</b> All</p>

## Hot Links Backup Configuration

Use the following commands to configure the Hot Links Backup interface.

Table 249. Hot Links Backup Configuration Options

Command Syntax and Usage
<pre>[no] hotlinks trigger &lt;1-200&gt; backup port &lt;port alias or number&gt;</pre> <p>Adds or removes the selected port to the Hot Links Backup interface.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>[no] hotlinks trigger &lt;1-200&gt; backup portchannel &lt;trunk group number&gt;</pre> <p>Adds or removes the selected trunk group to the Backup interface.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>[no] hotlinks trigger &lt;1-200&gt; backup adminkey &lt;0-65535&gt;</pre> <p>Adds or removes an LACP <i>admin key</i> to the Backup interface. LACP trunks formed with this <i>admin key</i> will be included in the Backup interface.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>show hotlinks trigger &lt;1-200&gt;</pre> <p>Displays the current Hot Links trigger settings.</p> <p><b>Command mode:</b> All</p>

## VLAN Configuration

These commands configure VLAN attributes, change the status of each VLAN, change the port membership of each VLAN, and delete VLANs.

By default, VLAN 1 is the only VLAN configured on the switch. All ports are members of VLAN 1 by default. Up to 4094 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 250. VLAN Configuration Options

Command Syntax and Usage	
<code>vlan &lt;VLAN number&gt;</code>	Enter VLAN configuration mode. <b>Command mode:</b> Global configuration
<code>protocol-vlan &lt;1-8&gt;</code>	Configures the Protocol-based VLAN (PVLAN). <b>Command mode:</b> VLAN
<code>name &lt;1-32 characters&gt;</code>	Assigns a name to the VLAN or changes the existing name. The default VLAN name is the first one. <b>Command mode:</b> VLAN
<code>[no] shutdown</code>	Disables or enables local traffic on the specified VLAN. Default setting is enabled ( <code>no shutdown</code> ) <b>Command mode:</b> VLAN
<code>stg &lt;STG number&gt;</code>	Assigns a VLAN to a Spanning Tree Group. <b>Note:</b> For MST no VLAN assignment is required. VLANs are mapped from CIST. <b>Command mode:</b> VLAN
<code>[no] vmap &lt;1-256&gt; [serverports non-serverports]</code>	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. <b>Command mode:</b> VLAN
<code>[no] flood</code>	Configures the switch to flood unregistered IP multicast traffic to all ports. The default setting is enabled. <b>Note:</b> 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. <b>Command mode:</b> VLAN

Table 250. VLAN Configuration Options (continued)

Command Syntax and Usage	
<pre>[no] cpu</pre>	<p>Configures the switch to forward unregistered IP multicast traffic to the MP, which adds an entry in the IPMC table, as follows:</p> <ul style="list-style-type: none"> <li>– If no Mrouter is present, drop subsequent packets with same IPMC.</li> <li>– If an Mrouter is present, forward subsequent packets to the Mrouter(s) on the ingress VLAN.</li> </ul> <p>The default setting is <code>enabled</code>.</p> <p><b>Note:</b> If both <code>flood</code> and <code>cpu</code> are disabled, the switch drops all unregistered IPMC traffic.</p> <p><b>Command mode:</b> VLAN</p>
<pre>[no] optflood</pre>	<p>Enables or disables optimized flooding. When enabled, optimized flooding avoids packet loss during the learning period. The default setting is <code>disabled</code>.</p> <p><b>Command mode:</b> VLAN</p>
<pre>no vlan &lt;VLAN number&gt;</pre>	<p>Deletes this VLAN.</p> <p><b>Command mode:</b> VLAN</p>
<pre>show vlan information</pre>	<p>Displays the current VLAN configuration.</p> <p><b>Command mode:</b> All</p>

**Note:** All ports must belong to at least one VLAN. Any port which is removed from a VLAN and which is not a member of any other VLAN is automatically added to default VLAN 1. You cannot remove a port from VLAN 1 if the port has no membership in any other VLAN. Also, you cannot add a port to more than one VLAN unless the port has VLAN tagging turned on.

## Protocol-Based VLAN Configuration

Use the following commands to configure Protocol-based VLAN for the selected VLAN.

Table 251. Protocol VLAN Configuration Options

Command Syntax and Usage
<pre>protocol-vlan &lt;1-8&gt; frame-type {ether2 llc snap} &lt;Ethernet type&gt;</pre> <p>Configures the frame type and the Ethernet type for the selected protocol. Ethernet type consists of a 4-digit (16 bit) hex code, such as 0080 (IPv4).</p> <p><b>Command mode:</b> VLAN</p>
<pre>protocol-vlan &lt;1-8&gt; protocol &lt;protocol type&gt;</pre> <p>Selects a pre-defined protocol, as follows:</p> <ul style="list-style-type: none"> <li>- decEther2: DEC Local Area Transport</li> <li>- ipv4Ether2: Internet IP (IPv4)</li> <li>- ipv6Ether2: IPv6</li> <li>- ipx802.2: Novell IPX 802.2</li> <li>- ipx802.3: Novell IPX 802.3</li> <li>- ipxEther2: Novell IPX</li> <li>- ipxSnap: Novell IPX SNAP</li> <li>- netbios: NetBIOS 802.2</li> <li>- rarpEther2: Reverse ARP</li> <li>- sna802.2: SNA 802.2</li> <li>- snaEther2: IBM SNA Service on Ethernet</li> <li>- vinesEther2: Banyan VINES</li> <li>- xnsEther2: XNS Compatibility</li> </ul> <p><b>Command mode:</b> VLAN</p>
<pre>protocol-vlan &lt;1-8&gt; priority &lt;0-7&gt;</pre> <p>Configures the priority value for this PVLAN.</p> <p><b>Command mode:</b> VLAN</p>
<pre>protocol-vlan &lt;1-8&gt; member &lt;port alias or number&gt;</pre> <p>Adds a port to the selected PVLAN.</p> <p><b>Command mode:</b> VLAN</p>
<pre>no protocol-vlan &lt;1-8&gt; member &lt;port alias or number&gt;</pre> <p>Removes a port from the selected PVLAN.</p> <p><b>Command mode:</b> VLAN</p>
<pre>[no] protocol-vlan &lt;1-8&gt; tag-pvlan &lt;port alias or number&gt;</pre> <p>Defines a port that will be tagged by the selected protocol on this VLAN.</p> <p><b>Command mode:</b> VLAN</p>



Table 251. Protocol VLAN Configuration Options (continued)

Command Syntax and Usage	
protocol-vlan <I-8> enable	Enables the selected protocol on the VLAN. <b>Command mode:</b> VLAN
no protocol-vlan <I-8> enable	Disables the selected protocol on the VLAN. <b>Command mode:</b> VLAN
no protocol-vlan <I-8>	Deletes the selected protocol configuration from the VLAN. <b>Command mode:</b> VLAN
show protocol-vlan <I-8>	Displays current parameters for the selected PVLAN. <b>Command mode:</b> All

## Private VLAN Configuration

Use the following commands to configure Private VLANs.

Table 252. Private VLAN Options

Command Syntax and Usage
<pre>[no] private-vlan primary</pre> <p>Enables or disables 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.</p> <p><b>Command mode:</b> VLAN</p>
<pre>[no] private-vlan community</pre> <p>Enables or disables the VLAN type as a community VLAN. Community VLANs carry upstream traffic from host ports. A Private VLAN may have multiple community VLANs.</p> <p><b>Command mode:</b> VLAN</p>
<pre>[no] private-vlan isolated</pre> <p>Enables or disables 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.</p> <p><b>Command mode:</b> VLAN</p>
<pre>private-vlan association [add remove] &lt;secondary VLAN list&gt;</pre> <p>Configures Private VLAN mapping between a primary VLAN and secondary VLANs. If no optional parameter is specified, the list of secondary VLANs, replaces the currently associated secondary VLANs. Otherwise:</p> <ul style="list-style-type: none"><li>– <code>add</code> appends the secondary VLANs to the ones currently associated</li><li>– <code>remove</code> excludes the secondary VLANs from the ones currently associated</li></ul> <p><b>Command mode:</b> VLAN</p>
<pre>show vlan private-vlan [type]</pre> <p>Displays current parameters for the selected Private VLAN(s).</p> <ul style="list-style-type: none"><li>– <code>type</code> lists only the VLAN type for each private VLAN: community, isolated or primary</li></ul> <p><b>Command mode:</b> VLAN</p>

---

## Layer 3 Configuration

The following table describes basic Layer 3 Configuration commands. The following sections provide more detailed information and commands.

Table 253. Layer 3 Configuration Commands

Command Syntax and Usage	
<code>interface ip &lt;interface number&gt;</code>	Configures the IP Interface. The G8264 supports up to 126 IP interfaces. However, IP interface 127 and 126 are reserved for switch management. To view command options, see <a href="#">page 373</a> . <b>Command mode:</b> Global configuration
<code>route-map {&lt;1-64&gt;}</code>	Enters IP Route Map mode. To view command options, see <a href="#">page 385</a> . <b>Command mode:</b> Global configuration
<code>router rip</code>	Enters the Routing Interface Protocol (RIP) configuration mode. To view command options, see <a href="#">page 390</a> . <b>Command mode:</b> Global configuration
<code>router ospf</code>	Enters OSPF configuration mode. To view command options, see <a href="#">page 394</a> . <b>Command mode:</b> Global configuration
<code>ipv6 router ospf</code>	Enters OSPFv3 configuration mode. To view command options, see <a href="#">page 405</a> . <b>Command mode:</b> Global configuration
<code>router bgp</code>	Enters Border Gateway Protocol (BGP) configuration mode. To view command options, see <a href="#">page 419</a> . <b>Command mode:</b> Global configuration
<code>router vrrp</code>	Enters Virtual Router Redundancy (VRRP) configuration mode. To view command options, see <a href="#">page 453</a> . <b>Command mode:</b> Global configuration
<code>ip pim component &lt;1-2&gt;</code>	Enters Protocol Independent Multicast (PIM) component configuration mode. To view command options, see <a href="#">page 462</a> . <b>Command mode:</b> Global configuration

Table 253. Layer 3 Configuration Commands (continued)

Command Syntax and Usage
<pre>ip router-id &lt;IP address&gt;</pre> <p>Sets the router ID.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>show layer3</pre> <p>Displays the current IP configuration.</p> <p><b>Command mode:</b> All</p>

## IP Interface Configuration

The G8264 supports up to 126 IP interfaces. Each IP interface represents the G8264 on an IP subnet on your network. The Interface option is disabled by default.

Interface 127 and interface 126 are reserved for switch management..

Table 254. IP Interface Configuration Options

Command Syntax and Usage	
interface ip <interface number>	Enter IP interface mode. <b>Command mode:</b> Global configuration
ip address <IP address> [<IP netmask>]	Configures the IP address of the switch interface, using dotted decimal notation. <b>Command mode:</b> Interface IP
ip netmask <IP netmask>	Configures the IP subnet address mask for the interface, using dotted decimal notation. <b>Command mode:</b> 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. <b>Command mode:</b> 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. <b>Command mode:</b> Interface IP
ipv6 prefixlen <IPv6 prefix length (1-128)>	Configures the subnet IPv6 prefix length. The default value is 0 (zero). <b>Command mode:</b> Interface IP
vlan <VLAN number>	Configures the VLAN number for this interface. Each interface can belong to one VLAN. <b>IPv4:</b> Each VLAN can contain multiple IPv4 interfaces. <b>IPv6:</b> Each VLAN can contain only one IPv6 interface. <b>Command mode:</b> Interface IP
[no] relay	Enables or disables the BOOTP relay on this interface. The default setting is enabled. <b>Command mode:</b> Interface IP

Table 254. IP Interface Configuration Options (continued)

Command Syntax and Usage	
[no] ip6host	<p>Enables or disables the IPv6 Host Mode on this interface. The default setting is disabled for data interfaces, and enabled for the management interface.</p> <p><b>Command mode:</b> Interface IP</p>
[no] ipv6 unreachable	<p>Enables or disables sending of ICMP Unreachable messages. The default setting is enabled.</p> <p><b>Command mode:</b> Interface IP</p>
enable	<p>Enables this IP interface.</p> <p><b>Command mode:</b> Interface IP</p>
no enable	<p>Disables this IP interface.</p> <p><b>Command mode:</b> Interface IP</p>
no interface ip <interface number>	<p>Removes this IP interface.</p> <p><b>Command mode:</b> Interface IP</p>
show interface ip <interface number>	<p>Displays the current interface settings.</p> <p><b>Command mode:</b> All</p>

## IPv6 Neighbor Discovery Configuration

The following table describes the IPv6 Neighbor Discovery configuration commands.

Table 255. IPv6 Neighbor Discovery Configuration Options

Command Syntax and Usage	
[no] ipv6 nd suppress-ra	<p>Enables or disables IPv6 Router Advertisements on the interface. The default setting is disabled (suppress Router Advertisements).</p> <p><b>Command mode:</b> Interface IP</p>
[no] ipv6 nd managed-config	<p>Enables or disables the managed address configuration flag of the interface. When enabled, the host IP address can be set automatically through DHCP. The default setting is disabled.</p> <p><b>Command mode:</b> Interface IP</p>
[no] ipv6 nd other-config	<p>Enables or disables the other stateful configuration flag, which allows the interface to use DHCP for other stateful configuration. The default setting is disabled.</p> <p><b>Command mode:</b> Interface IP</p>
ipv6 nd ra-lifetime <0-9000>	<p>Configures the IPv6 Router Advertisement lifetime interval. The RA lifetime interval must be greater than or equal to the RA maximum interval (advint). The default value is 1800 seconds.</p> <p><b>Command mode:</b> Interface IP</p>
[no] ipv6 nd dad-attempts <1-10>	<p>Configures the maximum number of duplicate address detection attempts. The default value is 1.</p> <p><b>Command mode:</b> Interface IP</p>
[no] ipv6 nd reachable-time <1-3600> [no] ipv6 nd reachable-time <1-3600000> ms	<p>Configures the advertised reachability time, in seconds or milliseconds (ms). The default value is 30 seconds.</p> <p><b>Command mode:</b> Interface IP</p>
[no] ipv6 nd ra-interval <4-1800>	<p>Configures the Router Advertisement maximum interval. The default value is 600 seconds.</p> <p><b>Note:</b> Set the maximum RA interval to a value greater than or equal to 4/3 of the minimum RA interval.</p> <p><b>Command mode:</b> Interface IP</p>

Table 255. IPv6 Neighbor Discovery Configuration Options (continued)

Command Syntax and Usage	
[no] ipv6 nd ra-intervalmin <3-1800>	<p>Configures the Router Advertisement minimum interval. The default value is 198 seconds.</p> <p><b>Note:</b> Set the minimum RA interval to a value less than or equal to 0.75 of the maximum RA interval.</p> <p><b>Command mode:</b> Interface IP</p>
[no] ipv6 nd retransmit-time <0-4294967> [no] ipv6 nd retransmit-time <0-4294967295> ms	<p>Configures the Router Advertisement re-transmit timer, in seconds or milliseconds (ms). The default value is 1 second.</p> <p><b>Command mode:</b> Interface IP</p>
[no] ipv6 nd hops-limit <0-255>	<p>Configures the Router Advertisement hop limit.</p> <p>The default value is 64.</p> <p><b>Command mode:</b> Interface IP</p>
[no] ipv6 nd advmtu	<p>Enables or disables the MTU option in Router Advertisements. The default setting is enabled.</p> <p><b>Command mode:</b> Interface IP</p>



## Default Gateway Configuration

The switch can be configured with up to four IPv2562564 gateways, as follows:

- Gateway 1 and 2: data traffic
- Gateway 3: management traffic for interface 127
- Gateway 4: management traffic for interface 128

This option is disabled by default.

Table 256. 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. <b>Command mode:</b> 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. <b>Command mode:</b> 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. <b>Command mode:</b> Global configuration
[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. <b>Command mode:</b> Global configuration
ip gateway <1-4> enable	Enables the gateway for use. <b>Command mode:</b> Global configuration
no ip gateway <1-4> enable	Disables the gateway. <b>Command mode:</b> Global configuration

Table 256. IPv4 Default Gateway Options

Command Syntax and Usage
<pre>no ip gateway &lt;I-4&gt;</pre> <p>Deletes the gateway from the configuration.</p> <p><b>Note:</b> In stacking mode, <code>no ip gateway 4</code> command deletes only the master gateway. To individually delete non-master gateways, use:</p> <pre>no ip gateway 4 mac &lt;MAC address&gt;</pre> <p><b>Command mode:</b> Global configuration</p>
<pre>show ip gateway &lt;I-4&gt;</pre> <p>Displays the current gateway settings.</p> <p><b>Command mode:</b> All</p>

## IPv4 Static Route Configuration

Up to 128 IPv4 static routes can be configured.

Table 257. IPv4 Static Route Configuration Options

Command Syntax and Usage
<pre>ip route &lt;IP subnet&gt; &lt;IP netmask&gt; &lt;IP nexthop&gt; [&lt;interface number&gt;]</pre> <p>Adds a static route. You will be prompted to enter a destination IP address, destination subnet mask, and gateway address. Enter all addresses using dotted decimal notation.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>no ip route &lt;IP subnet&gt; &lt;IP netmask&gt; [&lt;interface number&gt;]</pre> <p>Removes a static route. The destination address of the route to remove must be specified using dotted decimal notation.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>no ip route destination-address &lt;IP address&gt;</pre> <p>Clears all IP static routes with this destination.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>no ip route gateway &lt;IP address&gt;</pre> <p>Clears all IP static routes that use this gateway.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>ip route ecmp hash [dipsip] [sip]</pre> <p>Configures ECMP hashing parameters. You may choose one or more of the following parameters:</p> <ul style="list-style-type: none"> <li>- <code>dipsip</code>: Destination IP and source IP address</li> <li>- <code>sip</code>: Source IP address</li> </ul> <p><b>Command mode:</b> Global configuration</p>

Table 257. IPv4 Static Route Configuration Options (continued)

Command Syntax and Usage	
<pre>ip route interval &lt;1-60&gt;</pre>	<p>Configures the ECMP health-check ping interval, in seconds. The default value is 1 second.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>ip route retries &lt;1-60&gt;</pre>	<p>Configures the number of ECMP health-check retries. The default value is 3.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>[no] ip route healthcheck</pre>	<p>Enables or disables static route health checks. The default setting is disabled.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>show ip route static</pre>	<p>Displays the current IP static routes.</p> <p><b>Command mode:</b> All</p>

## IP Multicast Route Configuration

The following table describes the IP Multicast (IPMC) route commands.

**Note:** Before you can add an IPMC route, IGMP must be turned on, IGMP Snooping/Relay must be enabled, and the required VLANs must be added to IGMP Snooping/Relay.

Table 258. IP Multicast Route Configuration Commands

Command Syntax and Usage	
<pre>ip mroute &lt;IPMC destination&gt; &lt;VLAN number&gt; &lt;port alias or number&gt;] [primary backup host] [&lt;virtual router ID&gt;]</pre>	<p>Adds a static multicast route. The destination address, VLAN, and member port of the route must be specified.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>no ip mroute &lt;IPMC destination&gt; &lt;VLAN number&gt; &lt;port alias or number&gt; [primary backup host] [&lt;virtual router ID&gt;]</pre>	<p>Removes a static multicast route. The destination address, VLAN, and member port of the route to remove must be specified.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>ip mroute &lt;IP address&gt; &lt;VLAN number&gt; portchannel &lt;trunk group number&gt; [primary backup host] [&lt;virtual router ID&gt;]</pre>	<p>Adds a static multicast route. The destination address, VLAN, and member trunk group of the route must be specified.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>no ip mroute &lt;IP address&gt; &lt;VLAN number&gt; portchannel &lt;trunk group number&gt; [primary backup host] [&lt;virtual router ID&gt;]</pre>	<p>Removes a static multicast route. The destination address, VLAN, and member trunk group of the route to remove must be specified.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>ip mroute &lt;IP address&gt; &lt;VLAN number&gt; adminkey &lt;1-65535&gt; [primary backup host] [&lt;virtual router ID&gt; none]</pre>	<p>Adds a static multicast route. The destination address, VLAN, and LACP <i>admin key</i> of the route must be specified.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>no ip mroute &lt;IP address&gt; &lt;VLAN number&gt; adminkey &lt;1-65535&gt; [primary backup host] [&lt;virtual router ID&gt; none]</pre>	<p>Removes a static multicast route. The destination address, VLAN, and LACP <i>admin key</i> of the route to remove must be specified.</p> <p><b>Command mode:</b> Global configuration</p>

Table 258. IP Multicast Route Configuration Commands

Command Syntax and Usage
<pre>no ip mroute all</pre> <p>Removes all the static multicast routes configured.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>show ip mroute</pre> <p>Displays the current IP multicast routes.</p> <p><b>Command mode:</b> All except User EXEC</p>

## ARP Configuration

Address Resolution Protocol (ARP) is the TCP/IP protocol that resides within the Internet layer. ARP resolves a physical address from an IP address. ARP queries machines on the local network for their physical addresses. ARP also maintains IP to physical address pairs in its cache memory. In any IP communication, the ARP cache is consulted to see if the IP address of the computer or the router is present in the ARP cache. Then the corresponding physical address is used to send a packet.

Table 259. ARP Configuration Options

Command Syntax and Usage
<pre>ip arp rearp &lt;2-120&gt;</pre> <p>Defines re-ARP period, in minutes, for entries in the switch arp table. When ARP entries reach this value the switch will re-ARP for the address to attempt to refresh the ARP cache. The default value is 5 minutes.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>show ip arp</pre> <p>Displays the current ARP configurations.</p> <p><b>Command mode:</b> All except User EXEC</p>

## ARP Static Configuration

Static ARP entries are permanent in the ARP cache and do not age out like the ARP entries that are learned dynamically. Static ARP entries enable the switch to reach the hosts without sending an ARP broadcast request to the network. Static ARPs are also useful to communicate with devices that do not respond to ARP requests. Static ARPs can also be configured on some gateways as a protection against malicious ARP Cache corruption and possible DOS attacks.

Table 260. ARP Static Configuration Options

Command Syntax and Usage
<pre>ip arp &lt;IP address&gt; &lt;MAC address&gt; vlan &lt;vlan number&gt; port &lt;port alias or number&gt;</pre> <p>Adds a permanent ARP entry.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>ip arp &lt;destination unicast IP address&gt; &lt;destination multicast MAC address&gt; vlan &lt;cluster vlan number&gt;</pre> <p>Adds a static multicast ARP entry for Network Load Balancing (NLB).</p> <p><b>Command mode:</b> Global configuration</p>
<pre>no ip arp &lt;IP address&gt;</pre> <p>Deletes a permanent ARP entry.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>no ip arp all</pre> <p>Deletes all static ARP entries.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>show ip arp static</pre> <p>Displays current static ARP configuration.</p> <p><b>Command mode:</b> All</p>

## ARP Local Proxy Configuration

By using ARP local proxy feature, the router mediates the ARP traffic performed within a subnet. Each ARP request is received by the router. In response, the router sends its own MAC address. Any traffic between hosts is forwarded via the router's layer 3 interface.

**Note:** For a routed interface, enabling ARP local proxy feature requires disabling all ICMP redirects.

Table 261. ARP Local Proxy Configuration Options

Command Syntax and Usage
<pre>[no] ip local-proxy-arp</pre> <p>Enables or disables the ARP local proxy.</p> <p><b>Command mode:</b> Interface IP</p>
<pre>show interface ip</pre> <p>Displays the current interface settings.</p> <p><b>Command mode:</b> All</p>

## IP Forwarding Configuration

Table 262. IP Forwarding Configuration Options

Command Syntax and Usage
<pre>[no] ip routing directed-broadcasts</pre> <p>Enables or disables forwarding directed broadcasts. The default setting is disabled.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>[no] ip routing no-icmp-redirect</pre> <p>Enables or disables ICMP re-redirects. The default setting is disabled.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>[no] ip routing icmp6-redirect</pre> <p>Enables or disables IPv6 ICMP re-redirects. The default setting is disabled.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>ip routing</pre> <p>Enables IP forwarding (routing) on the G8264. Forwarding is turned on by default.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>no ip routing</pre> <p>Disables IP forwarding (routing) on the G8264.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>show ip routing</pre> <p>Displays the current IP forwarding settings.</p> <p><b>Command mode:</b> All except User EXEC</p>

## Network Filter Configuration

Table 263. IP Network Filter Configuration Options

Command Syntax and Usage	
<pre>ip match-address &lt;1-256&gt; &lt;IP address&gt; &lt;IP netmask&gt;</pre>	<p>Sets the starting IP address and IP Netmask for this filter to define the range of IP addresses that will be accepted by the peer when the filter is enabled. The default address is 0.0.0.0 0.0.0.0</p> <p><b>Command mode:</b> Global configuration.</p>
<pre>ip match-address &lt;1-256&gt; enable</pre>	<p>Enables the Network Filter configuration.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>no ip match-address &lt;1-256&gt; enable</pre>	<p>Disables the Network Filter configuration.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>no ip match-address &lt;1-256&gt;</pre>	<p>Deletes the Network Filter configuration.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>show ip match-address [&lt;1-256&gt;]</pre>	<p>Displays the current the Network Filter configuration.</p> <p><b>Command mode:</b> All except User EXEC</p>



## 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 264. Routing Map Configuration Options

Command Syntax and Usage	
route-map <1-64>	Enter route map configuration mode. <b>Command mode:</b> Global configuration
[no] access-list <1-32>	Configures the Access List. <b>Command mode:</b> Route map For more information, see <a href="#">page 387</a> .
[no] as-path-list <1-8>	Configures the Autonomous System (AS) Filter. <b>Command mode:</b> Route map For more information, see <a href="#">page 389</a> .
[no] as-path-preference <1-65535>	Sets the AS path preference of the matched route. You can configure up to three path preferences. <b>Command mode:</b> 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. <b>Command mode:</b> Route map
[no] metric <1-4294967294>	Sets the metric of the matched route. <b>Command mode:</b> Route map
[no] metric-type {1 2}	Assigns the type of OSPF metric. The default is type 1. <ul style="list-style-type: none"> <li>– <b>Type 1</b>—External routes are calculated using both internal and external metrics.</li> <li>– <b>Type 2</b>—External routes are calculated using only the external metrics. Type 1 routes have more cost than Type 2.</li> <li>– <b>none</b>—Removes the OSPF metric.</li> </ul> <b>Command mode:</b> Route map
precedence <1-255>	Sets the precedence of the route map. The smaller the value, the higher the precedence. Default value is 10. <b>Command mode:</b> Route map

Table 264. Routing Map Configuration Options (continued)

Command Syntax and Usage	
[no] weight <0-65534>	Sets the weight of the route map. <b>Command mode:</b> Route map
enable	Enables the route map. <b>Command mode:</b> Route map
no enable	Disables the route map. <b>Command mode:</b> Route map
no route-map <1-64>	Deletes the route map. <b>Command mode:</b> Route map
show route-map [<1-255>]	Displays the current route configuration. <b>Command mode:</b> All except User EXEC

## IP Access List Configuration

**Note:** The *route map number* (1-64) and the *access list number* (1-32) represent the IP access list you wish to configure.

Table 265. IP Access List Configuration Options

Command Syntax and Usage	
<code>[no] access-list &lt;1-32&gt; match-address &lt;1-256&gt;</code>	Sets the network filter number. <b>Command mode:</b> Route map See <a href="#">“Network Filter Configuration” on page 384</a> for details.
<code>[no] access-list &lt;1-32&gt; metric &lt;1-4294967294&gt;</code>	Sets the metric value in the AS-External (ASE) LSA. <b>Command mode:</b> Route map
<code>access-list &lt;1-32&gt; action {permit deny}</code>	Permits or denies action for the access list. <b>Command mode:</b> Route map
<code>access-list &lt;1-32&gt; enable</code>	Enables the access list. <b>Command mode:</b> Route map
<code>no access-list &lt;1-32&gt; enable</code>	Disables the access list. <b>Command mode:</b> Route map
<code>[no] access-list &lt;1-32&gt; match-access-control &lt;1-640&gt;</code>	Sets the network filter number. <b>Command mode:</b> Route map
<code>no access-list &lt;1-32&gt;</code>	Deletes the access list. <b>Command mode:</b> Route map
<code>show route-map &lt;1-64&gt; access-list &lt;1-32&gt;</code>	Displays the current Access List configuration. <b>Command mode:</b> All

## Policy-Based Routing Configuration

Use the following commands to set up policy-based routing.

**Note:** Multiple access lists can be entered separated by a comma (for example, “2,5,17”); a range of access lists can be entered using a hyphen (such as “2-23”).

Table 266. IP Next Hop Configuration Options

Command Syntax and Usage	
<pre>[no] set ip next-hop &lt;IPv4_addresses&gt; access-list &lt;I-32&gt;</pre>	<p>Sets the IP addresses for the next-hop to which packets are forwarded for each specified access list. When multiple addresses are specified they are prioritized in the order in which they are entered. Each next-hop must be an adjacent router.</p> <p>Use the <code>no</code> form of the command to remove the entry.</p> <p><b>Command mode:</b> Route map</p>
<pre>[no] set ip next-hop verify-availability &lt;IPv4_address&gt; &lt;sequence (1-255)&gt; [arp   icmp] [interval &lt;I-60&gt;] [retry &lt;I-3&gt;] [access-list &lt;I-32&gt;]</pre>	<p>Performs health-checking on and inserts the next hop IP address at the specified place (<i>sequence</i>) in the specified access list using ARP or ICMP as the tracking protocol. If not successful, the command will retry the health check at regular intervals of the specified number of seconds for the number of retries specified by <code>retry</code>. Use the <code>no</code> form of the command to remove the entry.</p> <p>Default values are <code>arp</code>, 2 seconds, and 3 retries.</p> <p><b>Note:</b> This command overrides the “<code>set ip next-hop &lt;IPv4_address&gt;</code>” command.</p> <p><b>Command mode:</b> Route map</p>
<pre>[no] set ip precedence &lt;precedence_value&gt; [access-list &lt;I-32&gt;]</pre>	<p>Sets the IP precedence value in the IP header for packets that match route map policy.</p> <p><b>Command mode:</b> Route map</p>
<pre>[no] set ip dscp &lt;0-63&gt; [access-list &lt;I-32&gt;]</pre>	<p>Sets the IP DSCP value in the IP header for packets that match route map policy.</p> <p><b>Command mode:</b> Route map</p>
<pre>[no] ip policy route-map &lt;I-255&gt;</pre>	<p>Applies the route map to an IP interface that has a VLAN configured.</p> <p><b>Command mode:</b> Interface IP</p>
<pre>show route-map &lt;I-255&gt;</pre>	<p>Displays the current route map configuration.</p> <p><b>Command mode:</b> All</p>
<pre>show route-map &lt;I-255&gt; access-list &lt;I-32&gt;</pre>	<p>Displays the current Access List configuration.</p> <p><b>Command mode:</b> All</p>

Table 266. IP Next Hop Configuration Options

Command Syntax and Usage
<pre>show ip policy</pre> <p>Displays the current routing policy information. <b>Command mode:</b> All</p>
<pre>show ip policy statistics</pre> <p>Displays statistics for the current routing policy. <b>Command mode:</b> All</p>

## Autonomous System Filter Path Configuration

**Note:** The *rmap number* and the *path number* represent the AS path you wish to configure.

Table 267. AS Filter Configuration Options

Command Syntax and Usage
<pre>as-path-list &lt;1-8&gt; as-path &lt;1-65535&gt;</pre> <p>Sets the Autonomous System filter's path number. <b>Command mode:</b> Route map</p>
<pre>as-path-list &lt;1-8&gt; action {permit deny}</pre> <p>Permits or denies Autonomous System filter action. <b>Command mode:</b> Route map</p>
<pre>as-path-list &lt;1-8&gt; enable</pre> <p>Enables the Autonomous System filter. <b>Command mode:</b> Route map</p>
<pre>no as-path-list &lt;1-8&gt; enable</pre> <p>Disables the Autonomous System filter. <b>Command mode:</b> Route map</p>
<pre>no as-path-list &lt;1-8&gt;</pre> <p>Deletes the Autonomous System filter. <b>Command mode:</b> Route map</p>
<pre>show route-map &lt;1-64&gt; as-path-list &lt;1-8&gt;</pre> <p>Displays the current Autonomous System filter configuration. <b>Command mode:</b> All</p>

## Routing Information Protocol Configuration

RIP commands are used for configuring Routing Information Protocol parameters. This option is turned off by default.

Table 268. Routing Information Protocol Options

Command Syntax and Usage
<pre>router rip</pre> <p>Enter Router RIP configuration mode. <b>Command mode:</b> Router RIP</p>
<pre>timers update &lt;1-120&gt;</pre> <p>Configures the time interval for sending for RIP table updates, in seconds. The default value is 30 seconds. <b>Command mode:</b> Router RIP</p>
<pre>enable</pre> <p>Globally turns RIP on. <b>Command mode:</b> Router RIP</p>
<pre>no enable</pre> <p>Globally turns RIP off. <b>Command mode:</b> Router RIP</p>
<pre>show ip rip</pre> <p>Displays the current RIP configuration. <b>Command mode:</b> All except User EXEC</p>

## Routing Information Protocol Interface Configuration

The RIP Interface commands are used for configuring Routing Information Protocol parameters for the selected interface.

**Note:** Do not configure RIP version 1 parameters if your routing equipment uses RIP version 2.

Table 269. RIP Interface Options

Command Syntax and Usage	
<code>ip rip version {1 2 both}</code>	Configures the RIP version used by this interface. The default value is version 2. <b>Command mode:</b> Interface IP
<code>[no] ip rip supply</code>	When enabled, the switch supplies routes to other routers. The default value is enabled. <b>Command mode:</b> Interface IP
<code>[no] ip rip listen</code>	When enabled, the switch learns routes from other routers. The default value is enabled. <b>Command mode:</b> Interface IP
<code>[no] ip rip poison</code>	When enabled, the switch uses split horizon with poisoned reverse. When disabled, the switch uses only split horizon. The default value is disabled. <b>Command mode:</b> Interface IP
<code>[no] ip rip split-horizon</code>	Enables or disables split horizon. The default value is enabled. <b>Command mode:</b> Interface IP
<code>[no] ip rip triggered</code>	Enables or disables Triggered Updates. Triggered Updates are used to speed convergence. When enabled, Triggered Updates force a router to send update messages immediately, even if it is not yet time for the update message. The default value is enabled. <b>Command mode:</b> Interface IP
<code>[no] ip rip multicast-updates</code>	Enables or disables multicast updates of the routing table (using address 224.0.0.9). The default value is enabled. <b>Command mode:</b> Interface IP
<code>[no] ip rip default-action {listen supply both}</code>	When enabled, the switch accepts RIP default routes from other routers, but gives them lower priority than configured default gateways. When disabled, the switch rejects RIP default routes. The default value is none. <b>Command mode:</b> Interface IP

Table 269. RIP Interface Options (continued)

Command Syntax and Usage	
[no] ip rip metric [ <i>&lt;1-15&gt;</i> ]	Configures the route metric, which indicates the relative distance to the destination. The default value is 1. <b>Command mode:</b> Interface IP
[no] ip rip authentication type [ <i>&lt;password&gt;</i> ]	Configures the authentication type. The default is none. <b>Command mode:</b> Interface IP
[no] ip rip authentication key <i>&lt;password&gt;</i>	Configures the authentication key password. <b>Command mode:</b> Interface IP
ip rip enable	Enables this RIP interface. <b>Command mode:</b> Interface IP
no ip rip enable	Disables this RIP interface. <b>Command mode:</b> Interface IP
show interface ip <i>&lt;interface number&gt;</i> rip	Displays the current RIP configuration. <b>Command mode:</b> All



## RIP Route Redistribution Configuration

The following table describes the RIP Route Redistribution commands.

Table 270. RIP Redistribution Options

Command Syntax and Usage
<pre>redistribute {fixed static ospf eospf ebgp ibgp} &lt;1-64&gt;</pre> <p>Adds selected routing maps to the RIP route redistribution list. To add specific route maps, enter routing map numbers, separated by a comma ( , ). To add all 64 route maps, type <code>all</code>.</p> <p>The routes of the redistribution protocol matched by the route maps in the route redistribution list will be redistributed.</p> <p><b>Command mode:</b> Router RIP</p>
<pre>no redistribute {fixed static ospf eospf ebgp ibgp} &lt;1-64&gt;</pre> <p>Removes the route map from the RIP route redistribution list.</p> <p>To remove specific route maps, enter routing map numbers, separated by a comma ( , ). To remove all 64 route maps, type <code>all</code>.</p> <p><b>Command mode:</b> Router RIP</p>
<pre>redistribute {fixed static ospf eospf ebgp ibgp} export &lt;1-15&gt;</pre> <p>Exports the routes of this protocol in which the metric and metric type are specified. To remove a previous configuration and stop exporting the routes of the protocol, enter <code>none</code>.</p> <p><b>Command mode:</b> Router RIP</p>
<pre>show ip rip redistribute</pre> <p>Displays the current RIP route redistribute configuration.</p> <p><b>Command mode:</b> All</p>

## Open Shortest Path First Configuration

Table 271. OSPF Configuration Options

Command Syntax and Usage	
router ospf	Enter Router OSPF configuration mode. <b>Command mode:</b> Global configuration
area-range <1-16>	Configures summary routes for up to 16 IP addresses. See <a href="#">page 398</a> to view command options. <b>Command mode:</b> Router OSPF
ip ospf <1-126>	Configures the OSPF interface. See <a href="#">page 399</a> to view command options. <b>Command mode:</b> Interface IP
area-virtual-link <1-3>	Configures the Virtual Links used to configure OSPF for a Virtual Link. See <a href="#">page 401</a> to view command options. <b>Command mode:</b> Router OSPF
message-digest-key <1-255> md5-key <text string>	Assigns a string to MD5 authentication key. <b>Command mode:</b> 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 <a href="#">page 403</a> to view command options. <b>Command mode:</b> Router OSPF
lsdb-limit <LSDB limit (0-16384, 0 for no limit)>	Sets the link state database limit. <b>Command mode:</b> Router OSPF
[no] default-information <1-16777214> {<AS external metric type (1-2)>}	Sets one default route among multiple choices in an area. Use none for no default. <b>Command mode:</b> Router OSPF

Table 271. OSPF Configuration Options (continued)

Command Syntax and Usage	
enable	Enables OSPF on the G8264. <b>Command mode:</b> Router OSPF
no enable	Disables OSPF on the G8264. <b>Command mode:</b> Router OSPF
show ip ospf	Displays the current OSPF configuration settings. <b>Command mode:</b> All except User EXEC

## Area Index Configuration

Table 272. Area Index Configuration Options

Command Syntax and Usage
<p>area &lt;0-19&gt; area-id &lt;IP address&gt;</p> <p>Defines the IP address of the OSPF area number.</p> <p><b>Command mode:</b> Router OSPF</p>
<p>area &lt;0-19&gt; type {transit stub nssa}</p> <p>Defines the type of area. For example, when a virtual link has to be established with the backbone, the area type must be defined as transit.</p> <ul style="list-style-type: none"> <li>– <b>Transit area:</b> 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.</li> <li>– <b>Stub area:</b> is an area where external routing information is not distributed. Typically, a stub area is connected to only one other area.</li> <li>– <b>NSSA:</b> 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.</li> </ul> <p><b>Command mode:</b> Router OSPF</p>
<p>area &lt;0-19&gt; stub-metric &lt;1-65535&gt;</p> <p>Configures a stub area to send a numeric metric value. All routes received via that stub area carry the configured metric to potentially influencing routing decisions.</p> <p>Metric value assigns the priority for choosing the switch for default route. Metric type determines the method for influencing routing decisions for external routes.</p> <p><b>Command mode:</b> Router OSPF</p>
<p>[no] area &lt;0-19&gt; authentication-type {password md5}</p> <p><b>None:</b> No authentication required.</p> <p><b>Password:</b> Authenticates simple passwords so that only trusted routing devices can participate.</p> <p><b>MD5:</b> This parameter is used when MD5 cryptographic authentication is required.</p> <p><b>Command mode:</b> Router OSPF</p>
<p>area &lt;0-19&gt; spf-interval &lt;1-255&gt;</p> <p>Configures the minimum time interval, in seconds, between two successive SPF (shortest path first) calculations of the shortest path tree using the Dijkstra's algorithm. The default value is 10 seconds.</p> <p><b>Command mode:</b> Router OSPF</p>
<p>area &lt;0-19&gt; enable</p> <p>Enables the OSPF area.</p> <p><b>Command mode:</b> Router OSPF</p>

Table 272. Area Index Configuration Options (continued)

Command Syntax and Usage
<pre>no area &lt;0-19&gt; enable</pre> <p>Disables the OSPF area.</p> <p><b>Command mode:</b> Router OSPF</p>
<pre>no area &lt;0-19&gt;</pre> <p>Deletes the OSPF area.</p> <p><b>Command mode:</b> Router OSPF</p>
<pre>show ip ospf area &lt;0-19&gt;</pre> <p>Displays the current OSPF configuration.</p> <p><b>Command mode:</b> All except User EXEC</p>

## OSPF Summary Range Configuration

Table 273. OSPF Summary Range Configuration Options

Command Syntax and Usage
<pre>area-range &lt;1-16&gt; address &lt;IP address&gt; &lt;IP netmask&gt;</pre> <p>Displays the base IP address or the IP address mask for the range. <b>Command mode:</b> Router OSPF</p>
<pre>area-range &lt;1-16&gt; area &lt;0-19&gt;</pre> <p>Displays the area index used by the G8264. <b>Command mode:</b> Router OSPF</p>
<pre>[no] area-range &lt;1-16&gt; hide</pre> <p>Hides the OSPF summary range. <b>Command mode:</b> Router OSPF</p>
<pre>area-range &lt;1-16&gt; enable</pre> <p>Enables the OSPF summary range. <b>Command mode:</b> Router OSPF</p>
<pre>no area-range &lt;1-16&gt; enable</pre> <p>Disables the OSPF summary range. <b>Command mode:</b> Router OSPF</p>
<pre>no area-range &lt;1-16&gt;</pre> <p>Deletes the OSPF summary range. <b>Command mode:</b> Router OSPF</p>
<pre>show ip ospf area-range &lt;1-16&gt;</pre> <p>Displays the current OSPF summary range. <b>Command mode:</b> Router OSPF</p>

## OSPF Interface Configuration

Table 274. OSPF Interface Configuration Options

Command Syntax and Usage	
ip ospf area <0-19>	Configures the OSPF area index. <b>Command mode:</b> 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). <b>Command mode:</b> 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. <b>Command mode:</b> 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. <b>Command mode:</b> 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. <b>Command mode:</b> Interface IP
ip ospf transit-delay <1-3600>	Configures the transit delay in seconds. <b>Command mode:</b> Interface IP
ip ospf retransmit-interval <1-3600>	Configures the retransmit interval in seconds. <b>Command mode:</b> Interface IP
[no] ip ospf key <key string>	Sets the authentication key to clear the password. <b>Command mode:</b> Interface IP

Table 274. OSPF Interface Configuration Options (continued)

<b>Command Syntax and Usage</b>	
[no] ip ospf message-digest-key <I-255>	<p>Assigns an MD5 key to the interface.</p> <p><b>Command mode:</b> Interface IP</p>
[no] ip ospf passive-interface	<p>Sets the interface as passive. On a passive interface, you can disable OSPF protocol exchanges, but the router advertises the interface in its LSAs so that IP connectivity to the attached network segment will be established.</p> <p><b>Command mode:</b> Interface IP</p>
[no] ip ospf point-to-point	<p>Sets the interface as point-to-point.</p> <p><b>Command mode:</b> Interface IP</p>
ip ospf enable	<p>Enables OSPF interface.</p> <p><b>Command mode:</b> Interface IP</p>
no ip ospf enable	<p>Disables OSPF interface.</p> <p><b>Command mode:</b> Interface IP</p>
no ip ospf	<p>Deletes the OSPF interface.</p> <p><b>Command mode:</b> Interface IP</p>
Show interface ip <interface number> ospf	<p>Displays the current settings for OSPF interface.</p> <p><b>Command mode:</b> All except User EXEC</p>



## OSPF Virtual Link Configuration

Table 275. OSPF Virtual Link Configuration Options

Command Syntax and Usage
<pre>area-virtual-link &lt;I-3&gt; area &lt;0-19&gt;</pre> <p>Configures the OSPF area index for the virtual link.  <b>Command mode:</b> Router OSPF</p>
<pre>area-virtual-link &lt;I-3&gt; hello-interval &lt;1-65535&gt;</pre> <pre>area-virtual-link &lt;I-3&gt; hello-interval &lt;50-65535ms&gt;</pre> <p>Configures the authentication parameters of a hello packet, in seconds or milliseconds. The default value is 10 seconds.  <b>Command mode:</b> Router OSPF</p>
<pre>area-virtual-link &lt;I-3&gt; dead-interval &lt;1-65535&gt;</pre> <pre>area-virtual-link &lt;I-3&gt; dead-interval &lt;1000-65535ms&gt;</pre> <p>Configures the health parameters of a hello packet, in seconds or milliseconds. The default value is 40 seconds.  <b>Command mode:</b> Router OSPF</p>
<pre>area-virtual-link &lt;I-3&gt; transit-delay &lt;1-3600&gt;</pre> <p>Configures the delay in transit, in seconds. The default value is one second.  <b>Command mode:</b> Router OSPF</p>
<pre>area-virtual-link &lt;I-3&gt; retransmit-interval &lt;1-3600&gt;</pre> <p>Configures the retransmit interval, in seconds. The default value is five seconds.  <b>Command mode:</b> Router OSPF</p>
<pre>area-virtual-link &lt;I-3&gt; neighbor-router &lt;IP address&gt;</pre> <p>Configures the router ID of the virtual neighbor. The default value is 0.0.0.0.  <b>Command mode:</b> Router OSPF</p>
<pre>[no] area-virtual-link &lt;I-3&gt; key &lt;password&gt;</pre> <p>Configures the password (up to eight characters) for each virtual link. The default setting is none.  <b>Command mode:</b> Router OSPF</p>
<pre>area-virtual-link &lt;I-3&gt; message-digest-key &lt;1-255&gt;</pre> <p>Sets MD5 key ID for each virtual link. The default setting is none.  <b>Command mode:</b> Router OSPF</p>
<pre>area-virtual-link &lt;I-3&gt; enable</pre> <p>Enables OSPF virtual link.  <b>Command mode:</b> Router OSPF</p>

Table 275. OSPF Virtual Link Configuration Options (continued)

Command Syntax and Usage
<pre>no area-virtual-link &lt;1-3&gt; enable</pre> <p>Disables OSPF virtual link. <b>Command mode:</b> Router OSPF</p>
<pre>no area-virtual-link &lt;1-3&gt;</pre> <p>Deletes OSPF virtual link. <b>Command mode:</b> Router OSPF</p>
<pre>show ip ospf area-virtual-link &lt;1-3&gt;</pre> <p>Displays the current OSPF virtual link settings. <b>Command mode:</b> All except User EXEC</p>

## OSPF Host Entry Configuration

Table 276. OSPF Host Entry Configuration Options

Command Syntax and Usage	
host <I-128> address <IP address>	Configures the base IP address for the host entry. <b>Command mode:</b> Router OSPF
host <I-128> area <0-19>	Configures the area index of the host. <b>Command mode:</b> Router OSPF
host <I-128> cost <I-65535>	Configures the cost value of the host. <b>Command mode:</b> Router OSPF
host <I-128> enable	Enables OSPF host entry. <b>Command mode:</b> Router OSPF
no host <I-128> enable	Disables OSPF host entry. <b>Command mode:</b> Router OSPF
no host <I-128>	Deletes OSPF host entry. <b>Command mode:</b> Router OSPF
show ip ospf host <I-128>	Displays the current OSPF host entries. <b>Command mode:</b> All except User EXEC

## OSPF Route Redistribution Configuration

Table 277. OSPF Route Redistribution Configuration Options

Command Syntax and Usage
<pre>redistribute {fixed static rip ebgp ibgp} &lt;rmap ID (1-64)&gt;</pre> <p>Adds selected routing map to the rmap list.</p> <p>This option adds a route map to the route redistribution list. The routes of the redistribution protocol matched by the route maps in the route redistribution list will be redistributed.</p> <p><b>Command mode:</b> Router OSPF</p>
<pre>no redistribute {fixed static rip ebgp ibgp} &lt;rmap ID (1-64)&gt;</pre> <p>Removes the route map from the route redistribution list.</p> <p>Removes routing maps from the rmap list.</p> <p><b>Command mode:</b> Router OSPF</p>
<pre>[no] redistribute {fixed static rip ebgp ibgp} export metric &lt;1-16777214&gt; metric-type {type1 type2}</pre> <p>Exports the routes of this protocol as external OSPF AS-external LSAs in which the metric and metric type are specified. To remove a previous configuration and stop exporting the routes of the protocol, enter none.</p> <p><b>Command mode:</b> Router OSPF</p>
<pre>show ip ospf redistribute</pre> <p>Displays the current route map settings.</p> <p><b>Command mode:</b> All except User EXEC</p>

## OSPF MD5 Key Configuration

Table 278. OSPF MD5 Key Options

Command Syntax and Usage
<pre>message-digest-key &lt;1-255&gt; md5-key &lt;1-16 characters&gt;</pre> <p>Sets the authentication key for this OSPF packet.</p> <p><b>Command mode:</b> Router OSPF</p>
<pre>no message-digest-key &lt;1-255&gt;</pre> <p>Deletes the authentication key for this OSPF packet.</p> <p><b>Command mode:</b> Router OSPF</p>
<pre>show ip ospf message-digest-key &lt;1-255&gt;</pre> <p>Displays the current MD5 key configuration.</p> <p><b>Command mode:</b> All except User EXEC</p>

## Open Shortest Path First Version 3 Configuration

Table 279. OSPFv3 Configuration Options

Command Syntax and Usage
<pre>[no] ipv6 router ospf</pre> <p>Enter OSPFv3 configuration mode. Enables or disables OSPFv3 routing protocol.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>abr-type [standard cisco ibm]</pre> <p>Configures the Area Border Router (ABR) type, as follows:</p> <ul style="list-style-type: none"> <li>– Standard</li> <li>– Cisco</li> <li>– IBM</li> </ul> <p>The default setting is <code>standard</code>.</p> <p><b>Command mode:</b> Router OSPF3</p>
<pre>as-external lsdB-limit &lt;LSDB limit (0-2147483647, -1 for no limit)&gt;</pre> <p>Sets the link state database limit.</p> <p><b>Command mode:</b> Router OSPF3</p>
<pre>exit-overflow-interval &lt;0-4294967295&gt;</pre> <p>Configures the number of seconds that a router takes to exit Overflow State. The default value is 0 (zero).</p> <p><b>Command mode:</b> Router OSPF3</p>
<pre>neighbor &lt;1-256&gt; {address &lt;IPv6 address&gt; enable interface &lt;1-126&gt; priority &lt;0-255&gt;}</pre> <p>Configures directly reachable routers over non-broadcast networks. This is required for non-broadcast multiple access (NBMA) networks and optional for Point-to-Multipoint networks.</p> <ul style="list-style-type: none"> <li>– <code>address</code> configures the neighbor's IPv6 address</li> <li>– <code>enable</code> activates a previously disabled neighbor</li> <li>– <code>interface</code> configures the OSPFv3 interface used for the neighbor entry</li> <li>– <code>priority</code> configures the priority value used for the neighbor entry. A priority value of 255 is the highest and 1 is the lowest. A priority value of 0 specifies that the neighbor cannot be used as Designated Router. The default value is 1.</li> </ul> <p><b>Command mode:</b> Router OSPF3</p>
<pre>no neighbor &lt;1-256&gt; [enable]</pre> <p>Deletes the neighbor entry.</p> <p>Using the <code>enable</code> option only disables the neighbor, while preserving its settings.</p> <p><b>Command mode:</b> Router OSPF3</p>

Table 279. OSPFv3 Configuration Options (continued)

Command Syntax and Usage	
reference-bandwidth <0-4294967295>	<p>Configures the reference bandwidth, in kilobits per second, used to calculate the default interface metric. The default value is 100,000.</p> <p><b>Command mode:</b> Router OSPF3</p>
timers spf {<SPF delay (0-65535)>} {<SPF hold time (0-65535)>}	<p>Configures the number of seconds that SPF calculation is delayed after a topology change message is received. The default value is 5.</p> <p>Configures the number of seconds between SPF calculations. The default value is 10.</p> <p><b>Command mode:</b> Router OSPF3</p>
router-id <IPv4 address>	<p>Defines the router ID.</p> <p><b>Command mode:</b> Router OSPF3</p>
[no] nssaAsbrDfRtTrans	<p>Enables or disables setting of the P-bit in the default Type 7 LSA generated by an NSSA internal ASBR. The default setting is disabled.</p> <p><b>Command mode:</b> Router OSPF3</p>
enable	<p>Enables OSPFv3 on the switch.</p> <p><b>Command mode:</b> Router OSPF3</p>
no enable	<p>Disables OSPFv3 on the switch.</p> <p><b>Command mode:</b> Router OSPF3</p>
show ipv6 ospf	<p>Displays the current OSPF configuration settings.</p> <p><b>Command mode:</b> All</p>

## OSPFv3 Area Index Configuration

Table 280. OSPFv3 Area Index Configuration Options

Command Syntax and Usage
<pre>area &lt;area index&gt; area-id &lt;IP address&gt;</pre> <p>Defines the IP address of the OSPFv3 area number.</p> <p><b>Command mode:</b> Router OSPF3</p>
<pre>area &lt;area index&gt; type {transit stub nssa} {no-summary}</pre> <p>Defines the type of area. For example, when a virtual link has to be established with the backbone, the area type must be defined as transit.</p> <p><b>Transit area:</b> allows area summary information to be exchanged between routing devices. Any area that is not a stub area or NSSA is considered to be transit area.</p> <p><b>Stub area:</b> is an area where external routing information is not distributed. Typically, a stub area is connected to only one other area.</p> <p><b>NSSA:</b> Not-So-Stubby Area (NSSA) is similar to stub area with additional capabilities. For example, routes originating from within the NSSA can be propagated to adjacent transit and backbone areas. External routes from outside the Autonomous System (AS) can be advertised within the NSSA but are not distributed into other areas.</p> <p>Enables or disables the no-summary option. When enabled, the area-border router neither originates nor propagates Inter-Area-Prefix LSAs into stub/NSSA areas. Instead it generates a default Inter-Area-Prefix LSA.</p> <p>The default setting is disabled.</p> <p><b>Command mode:</b> Router OSPF3</p>
<pre>area &lt;area index&gt; default-metric &lt;metric value (1-16777215)&gt;</pre> <p>Configures the cost for the default summary route in a stub area or NSSA.</p> <p><b>Command mode:</b> Router OSPF3</p>
<pre>area &lt;area index&gt; default-metric type &lt;1-3&gt;</pre> <p>Configures the default metric type applied to the route.</p> <p>This command applies only to area type of Stub/NSSA.</p> <p><b>Command mode:</b> Router OSPF3</p>
<pre>area &lt;area index&gt; stability-interval &lt;1-255&gt;</pre> <p>Configures the stability interval for an NSSA, in seconds. When the interval expires, an elected translator determines that its services are no longer required. The default value is 40.</p> <p><b>Command mode:</b> Router OSPF3</p>

Table 280. OSPFv3 Area Index Configuration Options (continued)

Command Syntax and Usage	
<pre>area &lt;area index&gt; translation-role always candidate</pre>	<p>Configures the translation role for an NSSA area, as follows:</p> <ul style="list-style-type: none"> <li>– Always: Type 7 LSAs are always translated into Type 5 LSAs.</li> <li>– Candidate: An NSSA border router participates in the translator election process.</li> </ul> <p>The default setting is candidate.</p> <p><b>Command mode:</b> Router OSPF3</p>
<pre>area &lt;area index&gt; enable</pre>	<p>Enables the OSPF area.</p> <p><b>Command mode:</b> Router OSPF3</p>
<pre>area &lt;area index&gt; no enable</pre>	<p>Disables the OSPF area.</p> <p><b>Command mode:</b> Router OSPF3</p>
<pre>no area &lt;area index&gt;</pre>	<p>Deletes the OSPF area.</p> <p><b>Command mode:</b> Router OSPF3</p>
<pre>show ipv6 ospf areas</pre>	<p>Displays the current OSPFv3 area configuration.</p> <p><b>Command mode:</b> All</p>



## OSPFv3 Summary Range Configuration

Table 281. 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. <b>Command mode:</b> Router OSPF3
area-range <1-16> area <area index (0-2)>	Configures the area index used by the switch. <b>Command mode:</b> Router OSPF3
area-range <1-16> lsa-type summary Type7	Configures the LSA type, as follows: – Summary LSA – Type7 LSA <b>Command mode:</b> Router OSPF3
area-range <1-16> tag <0-4294967295>	Configures the route tag. <b>Command mode:</b> Router OSPF3
[no] area-range <1-16> hide	Hides the OSPFv3 summary range. <b>Command mode:</b> Router OSPF3
area-range <1-16> enable	Enables the OSPFv3 summary range. <b>Command mode:</b> Router OSPF3
area-range <1-16> no enable	Disables the OSPFv3 summary range. <b>Command mode:</b> Router OSPF3
no area-range <1-16>	Deletes the OSPFv3 summary range. <b>Command mode:</b> Router OSPF3
show ipv6 ospf area-range	Displays the current OSPFv3 summary range. <b>Command mode:</b> All

## OSPFv3 AS-External Range Configuration

Table 282. OSPFv3 AS\_External Range Configuration Options

Command Syntax and Usage
<pre>summary-prefix &lt;I-16&gt; address &lt;IPv6 address&gt; &lt;IPv6 prefix length (1-128)&gt;</pre> <p>Configures the base IPv6 address and the subnet prefix length for the range.  <b>Command mode:</b> Router OSPF3</p>
<pre>summary-prefix &lt;I-16&gt; area &lt;area index (0-2)&gt;</pre> <p>Configures the area index used by the switch.  <b>Command mode:</b> Router OSPF3</p>
<pre>summary-prefix &lt;I-16&gt; aggregation-effect {allowAll denyAll advertise not-advertise}</pre> <p>Configures the aggregation effect, as follows:</p> <ul style="list-style-type: none"> <li>– 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.</li> <li>– denyAll: Type-5 and Type-7 LSAs are not generated.</li> <li>– 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.</li> <li>– 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.</li> </ul> <p><b>Command mode:</b> Router OSPF3</p>
<pre>[no] summary-prefix &lt;I-16&gt; translation</pre> <p>When enabled, the P-bit is set in the generated Type-7 LSA. When disabled, the P-bit is cleared. The default setting is disabled.  <b>Command mode:</b> Router OSPF3</p>
<pre>summary-prefix &lt;I-16&gt; enable</pre> <p>Enables the OSPFv3 AS-external range.  <b>Command mode:</b> Router OSPF3</p>
<pre>summary-prefix &lt;I-16&gt; no enable</pre> <p>Disables the OSPFv3 AS-external range.  <b>Command mode:</b> Router OSPF3</p>
<pre>no summary-prefix &lt;I-16&gt;</pre> <p>Deletes the OSPFv3 AS-external range.  <b>Command mode:</b> Router OSPF3</p>
<pre>show ipv6 ospf summary-prefix &lt;I-16&gt;</pre> <p>Displays the current OSPFv3 AS-external range.  <b>Command mode:</b> All</p>

## OSPFv3 Interface Configuration

Table 283. OSPFv3 Interface Configuration Options

Command Syntax and Usage
<pre>interface ip &lt;interface number&gt;</pre> <p>Enter Interface IP mode, from Global Configuration mode.  <b>Command mode:</b> Global configuration</p>
<pre>ipv6 ospf area &lt;area index (0-2)&gt;</pre> <p>Configures the OSPFv3 area index.  <b>Command mode:</b> Interface IP</p>
<pre>ipv6 ospf area &lt;area index (0-2)&gt; instance &lt;0-255&gt;</pre> <p>Configures the instance ID for the interface.  <b>Command mode:</b> Interface IP</p>
<pre>[no] ipv6 ospf priority &lt;priority value (0-255)&gt;</pre> <p>Configures the priority value for the switch's OSPFv3 interface.  A priority value of 255 is the highest and 1 is the lowest. A priority value of 0 specifies that the interface cannot be used as Designated Router (DR).  <b>Command mode:</b> Interface IP</p>
<pre>[no] ipv6 ospf cost &lt;1-65535&gt;</pre> <p>Configures the metric value for sending a packet on the interface.  <b>Command mode:</b> Interface IP</p>
<pre>[no] ipv6 ospf hello-interval &lt;1-65535&gt;</pre> <p>Configures the indicated interval, in seconds, between the hello packets, that the router sends on the interface.  <b>Command mode:</b> Interface IP</p>
<pre>[no] ipv6 ospf linklsasuppress</pre> <p>Enables or disables Link LSA suppression. When suppressed, no Link LSAs are originated. Default setting is disabled.  <b>Command mode:</b> Interface IP</p>

Table 283. OSPFv3 Interface Configuration Options (continued)

Command Syntax and Usage	
<pre>ipv6 ospf network {broadcast non-broadcast point-to-multipoint  point-to-point}</pre>	<p>Configures the network type for the OSPFv3 interface:</p> <ul style="list-style-type: none"> <li>– broadcast: network where all routers use the broadcast capability</li> <li>– non-broadcast: non-broadcast multiple access (NBMA) network supporting pseudo-broadcast (multicast and broadcast traffic is configured manually)</li> <li>– point-to-multipoint: network where multiple point-to-point links are set up on the same interface</li> <li>– point-to-point: network that joins a single pair of routers</li> </ul> <p>The default value is broadcast.</p> <p><b>Command mode:</b> Interface IP</p>
<pre>ipv6 ospf poll-interval &lt;0-4294967295&gt;</pre>	<p>Configures the poll interval in seconds for neighbors in NBMA networks. Default value is 120.</p> <p><b>Command mode:</b> Interface IP</p>
<pre>no ipv6 ospf poll-interval</pre>	<p>Configures the poll interval in seconds for neighbors in NBMA and point-to-multipoint networks to its default 120 seconds value.</p> <p><b>Command mode:</b> Interface IP</p>
<pre>[no] ipv6 ospf dead-interval &lt;1-65535&gt;</pre>	<p>Configures the time period, in seconds, for which the router waits for hello packet from the neighbor before declaring this neighbor down.</p> <p><b>Command mode:</b> Interface IP</p>
<pre>[no] ipv6 ospf transmit-delay &lt;1-1800&gt;</pre>	<p>Configures the estimated time, in seconds, taken to transmit LS update packet over this interface.</p> <p><b>Command mode:</b> Interface IP</p>
<pre>[no] ipv6 ospf retransmit-interval &lt;1-1800&gt;</pre>	<p>Configures the interval in seconds, between LSA retransmissions for adjacencies belonging to interface.</p> <p><b>Command mode:</b> Interface IP</p>
<pre>[no] ipv6 ospf passive-interface</pre>	<p>Enables or disables the passive setting on the interface. On a passive interface, OSPFv3 protocol packets are suppressed.</p> <p><b>Command mode:</b> Interface IP</p>
<pre>ipv6 ospf enable</pre>	<p>Enables OSPFv3 on the interface.</p> <p><b>Command mode:</b> Interface IP</p>

Table 283. OSPFv3 Interface Configuration Options (continued)

Command Syntax and Usage
<pre>ipv6 ospf no enable</pre> <p>Disables OSPFv3 on the interface. <b>Command mode:</b> Interface IP</p>
<pre>no ipv6 ospf</pre> <p>Deletes OSPFv3 from interface. <b>Command mode:</b> Interface IP</p>
<pre>show ipv6 ospf interface</pre> <p>Displays the current settings for OSPFv3 interface. <b>Command mode:</b> Interface IP</p>

### OSPFv3 over IPsec Configuration

The following table describes the OSPFv3 over IPsec Configuration commands.

Table 284. Layer 3 IPsec Configuration Options

Command Syntax and Usage
<pre>ipv6 ospf authentication ipsec spi &lt;256-4294967295&gt; {md5 sha1} &lt;authentication key (hexadecimal)&gt;</pre> <p>Configures the Security Parameters Index (SPI), algorithm, and authentication key for the Authentication Header (AH). The algorithms supported are:</p> <ul style="list-style-type: none"> <li>– MD5 (hexadecimal key length is 32)</li> <li>– SHA1 (hexadecimal key length is 40)</li> </ul> <p><b>Command mode:</b> Interface IP</p>
<pre>[no] ipv6 ospf authentication ipsec enable</pre> <p>Enables or disables IPsec. <b>Command mode:</b> Interface IP</p>
<pre>no ipv6 ospf authentication ipsec spi &lt;256-4294967295&gt;</pre> <p>Disables the specified Authentication Header (AH) SPI. <b>Command mode:</b> Interface IP</p>
<pre>ipv6 ospf authentication ipsec default</pre> <p>Resets the Authentication Header (AH) configuration to default values. <b>Command mode:</b> Interface IP</p>

Table 284. Layer 3 IPsec Configuration Options (continued)

Command Syntax and Usage	
<pre>ipv6 ospf encryption ipsec spi &lt;256-4294967295&gt;  esp {3des aes-cbc des null} &lt;encryption key (hexadecimal)&gt;[null]  {md5 sha1 none} &lt;authentication key (hexadecimal)&gt;</pre>	<p>Configures the Security Parameters Index (SPI), encryption algorithm, authentication algorithm, and authentication key for the Encapsulating Security Payload (ESP). The ESP algorithms supported are:</p> <ul style="list-style-type: none"> <li>– 3DES (hexadecimal key length is 48)</li> <li>– AES-CBC (hexadecimal key length is 32)</li> <li>– DES (hexadecimal key length is 16)</li> </ul> <p>The authentication algorithms supported are:</p> <ul style="list-style-type: none"> <li>– MD5 (hexadecimal key length is 32)</li> <li>– SHA1 (hexadecimal key length is 40)</li> <li>– none</li> </ul> <p><b>Note:</b> If the encryption algorithm is null, the authentication algorithm must be either MD5 or SHA1. (hexadecimal key length is 40). If an encryption algorithm is specified (3DES, AES-CBC, or DES), the authentication algorithm can be none.</p> <p><b>Command mode:</b> Interface IP</p>
<pre>ipv6 ospf encryption ipsec enable</pre>	<p>Enables OSPFv3 encryption for this interface.</p> <p><b>Command mode:</b> Interface IP</p>
<pre>no ipv6 ospf encryption ipsec spi &lt;256-4294967295&gt;</pre>	<p>Disables the specified Encapsulating Security Payload (ESP) SPI.</p> <p><b>Command mode:</b> Interface IP</p>
<pre>ipv6 ospf encryption ipsec default</pre>	<p>Resets the Encapsulating Security Payload (ESP) configuration to default values.</p> <p><b>Command mode:</b> Interface IP</p>

## OSPFv3 Virtual Link Configuration

Table 285. OSPFv3 Virtual Link Configuration Options

Command Syntax and Usage	
area-virtual-link <I-3> area <area index (0-2)>	Configures the OSPF area index. <b>Command mode:</b> Router OSPF3
area-virtual-link <I-3> hello-interval <I-65535>	Configures the indicated interval, in seconds, between the hello packets, that the router sends on the interface. <b>Command mode:</b> Router OSPF3
area-virtual-link <I-3> dead-interval <I-65535>	Configures the time period, in seconds, for which the router waits for hello packet from the neighbor before declaring this neighbor down. <b>Command mode:</b> Router OSPF3
area-virtual-link <I-3> transmit-delay <I-1800>	Configures the estimated time, in seconds, taken to transmit LS update packet over this interface. <b>Command mode:</b> Router OSPF3
area-virtual-link <I-3> retransmit-interval <I-1800>	Configures the interval, in seconds, between link-state advertisement (LSA) retransmissions for adjacencies belonging to the OSPFv3 virtual link interface. The default value is five seconds. <b>Command mode:</b> Router OSPF3
area-virtual-link <I-3> neighbor-router <NBR router ID (IP address)>	Configures the router ID of the virtual neighbor. The default setting is 0.0.0.0 <b>Command mode:</b> Router OSPF3
area-virtual-link <I-3> enable	Enables OSPF virtual link. <b>Command mode:</b> Router OSPF3
area-virtual-link <I-3> no enable	Disables OSPF virtual link. <b>Command mode:</b> Router OSPF3
no area-virtual-link <I-3>	Deletes OSPF virtual link. <b>Command mode:</b> Router OSPF3
show ipv6 ospf area-virtual-link	Displays the current OSPFv3 virtual link settings. <b>Command mode:</b> All

## OSPFv3 Host Entry Configuration

Table 286. OSPFv3 Host Entry Configuration Options

Command Syntax and Usage	
<pre>host &lt;1-128&gt; address &lt;IPv6 address&gt; &lt;prefix length (1-128)&gt;</pre>	<p>Configures the base IPv6 address and the subnet prefix length for the host entry.</p> <p><b>Command mode:</b> Router OSPF3</p>
<pre>host &lt;1-128&gt; area &lt;area index (0-2)&gt;</pre>	<p>Configures the area index of the host.</p> <p><b>Command mode:</b> Router OSPF3</p>
<pre>host &lt;1-128&gt; cost &lt;1-65535&gt;</pre>	<p>Configures the cost value of the host.</p> <p><b>Command mode:</b> Router OSPF3</p>
<pre>host &lt;1-128&gt; enable</pre>	<p>Enables the host entry.</p> <p><b>Command mode:</b> Router OSPF3</p>
<pre>no host &lt;1-128&gt; enable</pre>	<p>Disables the host entry.</p> <p><b>Command mode:</b> Router OSPF3</p>
<pre>no host &lt;1-128&gt;</pre>	<p>Deletes the host entry.</p> <p><b>Command mode:</b> Router OSPF3</p>
<pre>show ipv6 ospf host [&lt;1-128&gt;]</pre>	<p>Displays the current OSPFv3 host entries.</p> <p><b>Command mode:</b> All</p>



## OSPFv3 Redistribute Entry Configuration

Table 287. OSPFv3 Redist Entry Configuration Options

Command Syntax and Usage	
<pre>redist-config &lt;I-128&gt; address &lt;IPv6 address&gt; &lt;IPv6 prefix length (1-128)&gt;</pre>	<p>Configures the base IPv6 address and the subnet prefix length for the redistribution entry.</p> <p><b>Command mode:</b> Router OSPF3</p>
<pre>redist-config &lt;I-128&gt; metric-value &lt;I-16777215&gt;</pre>	<p>Configures the route metric value applied to the route before it is advertised into the OSPFv3 domain.</p> <p><b>Command mode:</b> Router OSPF3</p>
<pre>redist-config &lt;I-128&gt; metric-type asExtttype1 asExtttype2</pre>	<p>Configures the metric type applied to the route before it is advertised into the OSPFv3 domain.</p> <p><b>Command mode:</b> Router OSPF3</p>
<pre>[no] redist-config &lt;I-128&gt; tag &lt;0-4294967295&gt;</pre>	<p>Configures the route tag.</p> <p><b>Command mode:</b> Router OSPF3</p>
<pre>redist-config &lt;I-128&gt; enable</pre>	<p>Enables the OSPFv3 redistribution entry.</p> <p><b>Command mode:</b> Router OSPF3</p>
<pre>no redist-config &lt;I-128&gt; enable</pre>	<p>Disables the OSPFv3 redistribution entry.</p> <p><b>Command mode:</b> Router OSPF3</p>
<pre>no redist-config &lt;I-128&gt;</pre>	<p>Deletes the OSPFv3 redistribution entry.</p> <p><b>Command mode:</b> Router OSPF3</p>
<pre>show ipv6 ospf redist-config</pre>	<p>Displays the current OSPFv3 redistribution configuration entries.</p> <p><b>Command mode:</b> Router OSPF3</p>

## OSPFv3 Redistribute Configuration

Table 288. OSPFv3 Redistribute Configuration Options

Command Syntax and Usage
<pre>[no] redistribute {connected static} export &lt;metric value (1-16777215)&gt; &lt;metric type (1-2)&gt; &lt;tag (0-4294967295)&gt;</pre> <p>Exports the routes of this protocol as external OSPFv3 AS-external LSAs in which the metric, metric type, and route tag are specified. To remove a previous configuration and stop exporting the routes of the protocol, use the <code>no</code> form of the command.</p> <p><b>Command mode:</b> Router OSPF3</p>
<pre>show ipv6 ospf</pre> <p>Displays the current OSPFv3 route redistribution settings.</p> <p><b>Command mode:</b> All</p>

## Border Gateway Protocol Configuration

Border Gateway Protocol (BGP) is an Internet protocol that enables routers on a network to share routing information with each other and advertise information about the segments of the IP address space they can access within their network with routers on external networks. BGP allows you to decide what is the “best” route for a packet to take from your network to a destination on another network, rather than simply setting a default route from your border router(s) to your upstream provider(s). You can configure BGP either within an autonomous system or between different autonomous systems. When run within an autonomous system, it’s called internal BGP (iBGP). When run between different autonomous systems, it’s called external BGP (eBGP). BGP is defined in RFC 1771.

BGP commands enable you to configure the switch to receive routes and to advertise static routes, fixed routes and virtual server IP addresses with other internal and external routers. In the current IBM N/OS 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 289. Border Gateway Protocol Options

Command Syntax and Usage	
<code>router bgp</code>	Enter Router BGP configuration mode. <b>Command mode:</b> Global configuration
<code>neighbor &lt;peer number (1-96)&gt;</code>	Configures each BGP <i>peer</i> . Each border router, within an autonomous system, exchanges routing information with routers on other external networks. To view command options, see <a href="#">page 421</a> . <b>Command mode:</b> Router BGP
<code>as &lt;0-65535&gt;</code>	Set Autonomous System number. <b>Command mode:</b> Router BGP
<code>asn4comp</code>	Enables ASN4 to ASN2 compatibility. <b>Command mode:</b> Router BGP
<code>cluster-id &lt;IP address&gt;</code>	Specifies the router’s Cluster ID used when operating as a route reflector. Route reflectors that are part of the same cluster (assigned to the same group of clients) must use identical Cluster IDs. <b>Command mode:</b> Router BGP
<code>no cluster-id</code>	Removes the router’s Cluster ID. <b>Command mode:</b> Router BGP

Table 289. Border Gateway Protocol Options (continued)

<b>Command Syntax and Usage</b>	
[no] client-to-client reflection	<p>Enables or disables client-to-client IBGP route reflection when operating as a route reflector. The default state is enabled.</p> <p><b>Command mode:</b> Router BGP</p>
dscp <0-63>	<p>Set the DSCP marking value.</p> <p><b>Command mode:</b> Router BGP</p>
local-preference <0-4294967294>	<p>Sets the local preference. The path with the higher value is preferred.</p> <p>When multiple peers advertise the same route, use the route with the shortest AS path as the preferred route if you are using eBGP, or use the local preference if you are using iBGP.</p> <p><b>Command mode:</b> Router BGP</p>
maximum-paths <1-32>	<p>Set maximum paths allowed for an external route.</p> <p>By default, BGP will install only one path to the IP routing table.</p> <p><b>Command mode:</b> Router BGP</p>
maximum-paths ibgp <1-32>	<p>Set maximum paths allowed for an internal route.</p> <p>By default, BGP will install only one path to the IP routing table.</p> <p><b>Command mode:</b> Router BGP</p>
enable	<p>Globally turns BGP on.</p> <p><b>Command mode:</b> Router BGP</p>
no enable	<p>Globally turns BGP off.</p> <p><b>Command mode:</b> Router BGP</p>
[no] set ip next-hop peer-address	<p>Applied on output, sets the next-hop of the advertised matching routes to the current peer address of the local router. Applied on input, sets the next-hop of the received matching routes to the neighbor address, overriding other existing next-hops.</p> <p>Use the <code>no</code> form of the command to remove the entry.</p> <p><b>Command mode:</b> Route map</p>
show ip bgp	<p>Displays the current BGP configuration.</p> <p><b>Command mode:</b> All</p>

## BGP Peer Configuration

Use these commands 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 290. BGP Peer Configuration Options

Command Syntax and Usage
<pre>neighbor &lt;peer number&gt; remote-address &lt;IP address&gt;</pre> <p>Defines the IP address for the specified peer (border router), using dotted decimal notation. The default address is 0.0.0.0.</p> <p><b>Command mode:</b> Router BGP</p>
<pre>neighbor &lt;peer number&gt; remote-as &lt;1-65535&gt;</pre> <p>Sets the remote autonomous system number for the specified peer.</p> <p><b>Command mode:</b> Router BGP</p>
<pre>[no] neighbor &lt;peer number&gt; route-reflector-client</pre> <p>Enables or disables the peer as a route reflector client. Configuring route reflector clients, implicitly sets up the local router as a route reflector.</p> <p><b>Command mode:</b> Router BGP</p>
<pre>neighbor &lt;peer number&gt; update-source {&lt;interface number&gt; loopback &lt;1-5&gt;}</pre> <p>Sets the source interface number for this peer.</p> <p><b>Command mode:</b> Router BGP</p>
<pre>neighbor &lt;peer number&gt; timers hold-time &lt;0, 3-65535&gt;</pre> <p>Sets the period of time, in seconds, that will elapse before the peer session is torn down because the switch hasn't received a "keep alive" message from the peer. The default value is 180 seconds.</p> <p><b>Command mode:</b> Router BGP</p>
<pre>neighbor &lt;peer number&gt; timers keep-alive &lt;0, 1-21845&gt;</pre> <p>Sets the keep-alive time for the specified peer, in seconds. The default value is 60 seconds.</p> <p><b>Command mode:</b> Router BGP</p>
<pre>neighbor &lt;peer number&gt; advertisement-interval &lt;1-65535&gt;</pre> <p>Sets time, in seconds, between advertisements. The default value is 60 seconds.</p> <p><b>Command mode:</b> Router BGP</p>
<pre>neighbor &lt;peer number&gt; retry-interval &lt;1-65535&gt;</pre> <p>Sets connection retry interval, in seconds. The default value is 120 seconds.</p> <p><b>Command mode:</b> Router BGP</p>
<pre>neighbor &lt;peer number&gt; route-origination-interval &lt;1-65535&gt;</pre> <p>Sets the minimum time between route originations, in seconds. The default value is 15 seconds.</p> <p><b>Command mode:</b> Router BGP</p>

Table 290. BGP Peer Configuration Options (continued)

Command Syntax and Usage	
neighbor <peer number> time-to-live <1-255>	<p>Time-to-live (TTL) is a value in an IP packet that tells a network router whether or not the packet has been in the network too long and should be discarded. TTL specifies a certain time span in seconds that, when exhausted, would cause the packet to be discarded. The TTL is determined by the number of router hops the packet is allowed before it must be discarded.</p> <p>This command specifies the number of router hops that the IP packet can make. This value is used to restrict the number of “hops” the advertisement makes. It is also used to support multi-hops, which allow BGP peers to talk across a routed network. The default number is set at 1.</p> <p><b>Note:</b> The TTL value is significant only to eBGP peers, for iBGP peers the TTL value in the IP packets is always 255 (regardless of the configured value).</p> <p><b>Command mode:</b> Router BGP</p>
no neighbor <peer number> time-to-live	<p>Disables the TTL feature.</p> <p><b>Command mode:</b> Router BGP</p>
neighbor <peer number> ttl-security hops <1-254>	<p>Sets the minimum number of time-to-live (TTL) router hops an IP packet must make to not be discarded.</p> <p><b>Command mode:</b> Router BGP</p>
no neighbor <peer number> ttl-security hops	<p>Disables the TTL security feature.</p> <p><b>Command mode:</b> Router BGP</p>
neighbor <peer number> route-map in <1-255>	<p>Adds route map into in-route map list.</p> <p><b>Command mode:</b> Router BGP</p>
neighbor <peer number> route-map out <1-255>	<p>Adds route map into out-route map list.</p> <p><b>Command mode:</b> Router BGP</p>
no neighbor <peer number> route-map in <1-255>	<p>Removes route map from in-route map list.</p> <p><b>Command mode:</b> Router BGP</p>
no neighbor <peer number> route-map out <1-255>	<p>Removes route map from out-route map list.</p> <p><b>Command mode:</b> Router BGP</p>
no neighbor <peer number> shutdown	<p>Enables this peer configuration.</p> <p><b>Command mode:</b> Router BGP</p>

Table 290. BGP Peer Configuration Options (continued)

Command Syntax and Usage	
neighbor <peer number> shutdown	Disables this peer configuration. <b>Command mode:</b> Router BGP
no neighbor <peer number>	Deletes this peer configuration. <b>Command mode:</b> Router BGP
[no] neighbor <peer number> password <1-16 characters>	Configures the BGP peer password. <b>Command mode:</b> 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. <b>Command mode:</b> Router BGP
show ip bgp neighbor [<peer number>]	Displays the current BGP peer configuration. <b>Command mode:</b> All
neighbor <peer number> next-hop-self	Enforces using the router's own IP address as next-hop attribute when sending BGP updates to the peer. Applicable only for EBGP routes. <b>Command mode:</b> Router BGP
no neighbor <peer number> next-hop-self	Doesn't enforce using the router's own IP address as next-hop attribute when sending BGP updates to the peer. <b>Command mode:</b> Router BGP

## BGP Peering Group Configuration

These commands enable you to configure BGP peering for a group of remote neighbors defined by a range of IP addresses. Each range can be configured as a subnet IP address. After a subnet range is configured for a BGP peer group and a TCP session is established for an IP address in that subnet range, a new BGP neighbor is dynamically created as a member of that group and inherits the configuration from the peer group.

Table 291. BGP Peering Group Configuration Options

Command Syntax and Usage
<pre>[no] neighbor group &lt;group number&gt; name &lt;1-32 characters&gt;</pre> <p>Sets the name for the group.</p> <p><b>Command mode:</b> Router BGP</p>
<pre>neighbor group &lt;group number&gt; listen range &lt;IPv4 address&gt; &lt;IPv4 subnet mask &gt;</pre> <p>Defines the range of IP addresses that will be accepted for the group.</p> <p><b>Command mode:</b> Router BGP</p>
<pre>neighbor group &lt;group number&gt; remote-as &lt;AS number (1-65535)&gt; [alternate-as &lt;AS number (1-65535)&gt;]</pre> <p>Adds a remote access server (RAS) into the RAS list.</p> <p><b>Command mode:</b> Router BGP</p>
<pre>[no] neighbor group &lt;peer number&gt; route-reflector-client</pre> <p>Enables or disables the group as a route reflector client. Configuring route reflector clients, implicitly sets up the local router as a route reflector.</p> <p><b>Command mode:</b> Router BGP</p>
<pre>neighbor group &lt;group number&gt; listen limit &lt;group limit (1-96)&gt;</pre> <p>Sets the maximum number of BGP dynamic peers.</p> <p><b>Command mode:</b> Router BGP</p>
<pre>neighbor group &lt;group number&gt; update-source &lt;interface number (1-126)&gt;</pre> <p>Sets the local IP interface.</p> <p><b>Command mode:</b> Router BGP</p>
<pre>neighbor group &lt;group number&gt; update-source loopback &lt;interface number (1-5)&gt;</pre> <p>Sets the loopback interface number for this peering group.</p> <p><b>Command mode:</b> Router BGP</p>
<pre>neighbor group &lt;group number&gt; timers hold-time &lt;hold time (0, 3-65535)&gt;</pre> <p>Sets the period of time, in seconds, that will elapse before the peering group session is torn down because the switch hasn't received a "keep alive" message from the peer. The default value is 180.</p> <p><b>Command mode:</b> Router BGP</p>



Table 291. BGP Peering Group Configuration Options (continued)

Command Syntax and Usage
<pre>neighbor group &lt;group number&gt; timers keep-alive &lt;keepalive time (0, 1-21845)&gt;</pre> <p>Sets the keep-alive time for the specified peering group in seconds. The default value is 60.</p> <p><b>Command mode:</b> Router BGP</p>
<pre>neighbor group &lt;group number&gt; advertisement-interval &lt;min adv time (1-65535)&gt;</pre> <p>Sets time, in seconds, between advertisements. The default value is 60 seconds.</p> <p><b>Command mode:</b> Router BGP</p>
<pre>neighbor group &lt;group number&gt; route-origin-interval &lt;min orig time (1-65535)&gt;</pre> <p>Sets the minimum time between route originations, in seconds. The default value is 15 seconds.</p> <p><b>Command mode:</b> Router BGP</p>
<pre>neighbor group &lt;group number&gt; time-to-live &lt;number of router hops (1-255)&gt;</pre> <p>Time-to-live (TTL) is a value in an IP packet that tells a network router whether or not the packet has been in the network too long and must be discarded. TTL specifies a certain time span in seconds that, when exhausted, would cause the packet to be discarded. The TTL is determined by the number of router hops the packet is allowed before it must be discarded.</p> <p>This command specifies the number of router hops that the IP packet can make. This value is used to restrict the number of “hops” the advertisement makes. It is also used to support multi-hops, which allow BGP peering groups to talk across a routed network. The default number is set at 1.</p> <p><b>Note:</b> The TTL value is significant only to eBGP peering groups; for iBGP peering groups the TTL value in the IP packets is always 255 (regardless of the configured value).</p> <p><b>Command mode:</b> Router BGP</p>
<pre>no neighbor group &lt;group number&gt; time-to-live &lt;1-255&gt;</pre> <p>Disables the TTL feature.</p> <p><b>Command mode:</b> Router BGP</p>
<pre>neighbor group &lt;group number&gt; ttl-security hops &lt;1-254&gt;</pre> <p>Sets the minimum number of time-to-live (TTL) router hops an IP packet must make to not be discarded.</p> <p><b>Command mode:</b> Router BGP</p>
<pre>no neighbor group &lt;group number&gt; ttl-security hops</pre> <p>Disables the TTL security feature.</p> <p><b>Command mode:</b> Router BGP</p>

Table 291. BGP Peering Group Configuration Options (continued)

Command Syntax and Usage
<p>neighbor group &lt;group number&gt; route-map in &lt;route map ID (1-255)&gt;                      Adds route map into in-route map list.  <b>Command mode:</b> Router BGP</p>
<p>neighbor group &lt;group number&gt; route-map out &lt;route map ID (1-255)&gt;                      Adds route map into out-route map list.  <b>Command mode:</b> Router BGP</p>
<p>[no] neighbor group &lt;group number&gt; route-map in &lt;route map ID (1-255)&gt;                      Removes route map from in-route map list.  <b>Command mode:</b> Router BGP</p>
<p>[no] neighbor group &lt;group number&gt; route-map out &lt;route map ID (1-255)&gt;                      Removes route map from out-route map list.  <b>Command mode:</b> Router BGP</p>
<p>[no] neighbor group &lt;group number&gt; password                      Configures the BGP peer password.  <b>Command mode:</b> Router BGP</p>
<p>[no] neighbor group &lt;group number&gt; shutdown                      Enables this peering group configuration.  <b>Command mode:</b> Router BGP</p>
<p>neighbor group &lt;group number&gt; shutdown                      Disables this peering group configuration.  <b>Command mode:</b> Router BGP</p>
<p>no [no] neighbor group &lt;group number&gt;                      Deletes this peering group configuration.  <b>Command mode:</b> Router BGP</p>
<p>neighbor group &lt;group number&gt; next-hop-self                      Enforces using the router's own IP address as next-hop attribute when sending BGP updates to the peering group. Applicable only for EBGP routes.  <b>Command mode:</b> Router BGP</p>
<p>no neighbor group &lt;group number&gt; next-hop-self                      Doesn't enforce using the router's own IP address as next-hop attribute when sending BGP updates to the peering group.  <b>Command mode:</b> Router BGP</p>
<p>show ip bgp neighbor group [&lt;neighbor group number&gt;]                      Displays the current peering group configuration.  <b>Command mode:</b> All</p>

## BGP Neighbor Redistribution Configuration

This menu enables you to redistribute BGP routes for a group of remote neighbors defined by a range of IP addresses.

Table 292. BGP Neighbor Redistribution Configuration Options

Command Syntax and Usage
<pre>[no] neighbor group &lt;group number&gt; redistribute default-metric &lt;1-4294967294&gt;</pre> <p>Sets default metric of advertised routes.</p> <p><b>Command mode:</b> Router BGP</p>
<pre>[no] neighbor group &lt;group number&gt; redistribute default-action {import originate redistribute}</pre> <p>Sets default route action.</p> <p>Defaults routes can be configured as import, originate, redistribute, or none.</p> <p><b>None:</b> No routes are configured</p> <p><b>Import:</b> Import these routes.</p> <p><b>Originate:</b> The switch sends a default route to peers if it does not have any default routes in its routing table.</p> <p><b>Redistribute:</b> Default routes are either configured through default gateway or learned through other protocols and redistributed to peer. If the routes are learned from default gateway configuration, you have to enable static routes since the routes from default gateway are static routes. Similarly, if the routes are learned from a certain routing protocol, you have to enable that protocol.</p> <p><b>Command mode:</b> Router BGP</p>
<pre>[no] neighbor group &lt;group number&gt; redistribute rip</pre> <p>Enables or disables advertising RIP routes.</p> <p><b>Command mode:</b> Router BGP</p>
<pre>[no] neighbor group &lt;group number&gt; redistribute ospf</pre> <p>Enables or disables advertising OSPF routes.</p> <p><b>Command mode:</b> Router BGP</p>
<pre>[no] neighbor group &lt;group number&gt; redistribute fixed</pre> <p>Enables or disables advertising fixed routes.</p> <p><b>Command mode:</b> Router BGP</p>
<pre>[no] neighbor group &lt;group number&gt; redistribute static</pre> <p>Enables or disables advertising static routes.</p> <p><b>Command mode:</b> Router BGP</p>
<pre>show ip bgp neighbor group &lt;group number&gt; redistribute</pre> <p>Displays current redistribution configuration.</p> <p><b>Command mode:</b> All except User EXEC</p>

## BGP Aggregation Configuration

These commands enable you to configure BGP aggregation to specify the routes/range of IP destinations a peer router accepts from other peers. All matched routes are aggregated to one route, to reduce the size of the routing table. By default, the first aggregation number is enabled and the rest are disabled.

Table 293. BGP Aggregation Configuration Options

Command Syntax and Usage
<pre>aggregate-address &lt;1-16&gt; &lt;IP address&gt; &lt;IP netmask&gt;</pre> <p>Defines the starting subnet IP address for this aggregation, using dotted decimal notation. The default address is 0.0.0.0.</p> <p><b>Command mode:</b> Router BGP</p>
<pre>aggregate-address &lt;1-16&gt; enable</pre> <p>Enables this BGP aggregation.</p> <p><b>Command mode:</b> Router BGP</p>
<pre>no aggregate-address &lt;1-16&gt; enable</pre> <p>Disables this BGP aggregation.</p> <p><b>Command mode:</b> Router BGP</p>
<pre>no aggregate-address &lt;1-16&gt;</pre> <p>Deletes this BGP aggregation.</p> <p><b>Command mode:</b> Router BGP</p>
<pre>show ip bgp aggregate-address [&lt;1-16&gt;]</pre> <p>Displays the current BGP aggregation configuration.</p> <p><b>Command mode:</b> All</p>

## MLD Global Configuration

Table 294 describes the commands used to configure global MLD parameters.

Table 294. MLD Global Configuration Commands

Command Syntax and Usage
<code>ipv6 mld</code> Enter MLD global configuration mode. <b>Command mode:</b> Global configuration
<code>default</code> Resets MLD parameters to their default values. <b>Command mode:</b> MLD
<code>enable</code> Globally turns MLD on. <b>Command mode:</b> MLD
<code>no enable</code> Globally turns MLD off. <b>Command mode:</b> MLD
<code>exit</code> Exit from MLD configuration mode. <b>Command mode:</b> MLD
<code>show ipv6 mld</code> Displays the current MLD configuration parameters. <b>Command mode:</b> All

## MLD Interface Configuration

Table 295 describes the commands used to configure MLD parameters for an interface.

Table 295. MLD Interface Configuration Commands

Command Syntax and Usage	
<pre>ipv6 mld default</pre>	<p>Resets MLD parameters for the selected interface to their default values.</p> <p><b>Command mode:</b> Interface IP</p>
<pre>ipv6 mld dmrtr enable disable</pre>	<p>Enables or disables dynamic Mrouter learning on the interface. The default setting is disabled.</p> <p><b>Command mode:</b> Interface IP</p>
<pre>ipv6 mld enable</pre>	<p>Enables this MLD interface.</p> <p><b>Command mode:</b> Interface IP</p>
<pre>no ipv6 mld enable</pre>	<p>Disables this MLD interface.</p> <p><b>Command mode:</b> Interface IP</p>
<pre>ipv6 mld llistnr &lt;1-32&gt;</pre>	<p>Configures the Last Listener query interval. The default value is 1 second.</p> <p><b>Command mode:</b> Interface IP</p>
<pre>ipv6 mld qinterval &lt;2-65535&gt;</pre>	<p>Configures the interval for MLD Query Reports. The default value is 125 seconds.</p> <p><b>Command mode:</b> Interface IP</p>
<pre>ipv6 mld qri &lt;1000-65535&gt;</pre>	<p>Configures the interval for MLD Query Response Reports. The default value is 10,000 milliseconds.</p> <p><b>Command mode:</b> Interface IP</p>
<pre>ipv6 mld robust &lt;1-10&gt;</pre>	<p>Configures the MLD Robustness variable, which allows you to tune the switch for expected packet loss on the subnet. If the subnet is expected to be lossy (high rate of packet loss), increase the value. The default value is 1.</p> <p><b>Command mode:</b> Interface IP</p>

Table 295. MLD Interface Configuration Commands (continued)

Command Syntax and Usage
<pre>ipv6 mld version &lt;1-2&gt;</pre> <p>Defines the MLD protocol version number.  <b>Command mode:</b> Interface IP</p>
<pre>show ipv6 mld interface &lt;interface number&gt;</pre> <p>Displays the current MLD interface configuration.  <b>Command mode:</b> All</p>

## IGMP Configuration

Table 296 describes the commands used to configure basic IGMP parameters.

Table 296. IGMP Configuration Options

Command Syntax and Usage
<pre>ip igmp enable</pre> <p>Globally turns IGMP on.  <b>Command mode:</b> Global configuration</p>
<pre>no ip igmp enable</pre> <p>Globally turns IGMP off.  <b>Command mode:</b> Global configuration</p>
<pre>[no] ip igmp aggregate</pre> <p>Enables or disables IGMP Membership Report aggregation.  <b>Command mode:</b> Global configuration</p>
<pre>show ip igmp</pre> <p>Displays the current IGMP configuration parameters.  <b>Command mode:</b> All</p>

The following sections describe the IGMP configuration options.

- [“IGMP Snooping Configuration” on page 432](#)
- [“IGMP Relay Configuration” on page 434](#)
- [“IGMP Relay Multicast Router Configuration” on page 435](#)
- [“IGMP Static Multicast Router Configuration” on page 436](#)
- [“IGMP Filtering Configuration” on page 437](#)
- [“IGMP Advanced Configuration” on page 439](#)
- [“IGMP Querier Configuration” on page 440](#)

## 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 297](#) describes the commands used to configure IGMP Snooping.

Table 297. IGMP Snooping Configuration Options

Command Syntax and Usage	
<pre>ip igmp snoop mrouter-timeout &lt;1-600&gt;</pre>	<p>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.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>[no] ip igmp aggregate</pre>	<p>Enables or disables IGMP Membership Report aggregation.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>ip igmp snoop source-ip &lt;IP address&gt;</pre>	<p>Configures the source IP address used as a proxy for IGMP Group Specific Queries.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>ip igmp snoop vlan &lt;VLAN number&gt;</pre>	<p>Adds the selected VLAN(s) to IGMP Snooping.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>no ip igmp snoop vlan &lt;VLAN number&gt;</pre>	<p>Removes the selected VLAN(s) from IGMP Snooping.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>no ip igmp snoop vlan all</pre>	<p>Removes all VLANs from IGMP Snooping.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>ip igmp snoop enable</pre>	<p>Enables IGMP Snooping.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>no ip igmp snoop enable</pre>	<p>Disables IGMP Snooping.</p> <p><b>Command mode:</b> Global configuration</p>



Table 297. IGMP Snooping Configuration Options (continued)

Command Syntax and Usage
<pre>default ip igmp snoop</pre> <p>Resets IGMP Snooping parameters to their default values.  <b>Command mode:</b> Global configuration</p>
<pre>show ip igmp snoop</pre> <p>Displays the current IGMP Snooping parameters.  <b>Command mode:</b> All</p>

## IGMPv3 Configuration

Table 298 describes the commands used to configure IGMP version 3.

Table 298. IGMP Version 3 Configuration Options

Command Syntax and Usage
<pre>ip igmp snoop igmpv3 sources &lt;1-64&gt;</pre> <p>Configures the maximum number of IGMP multicast sources to snoop from within the group record. Use this command to limit the number of IGMP sources to provide more refined control. The default value is 8.  <b>Command mode:</b> Global configuration</p>
<pre>[no] ip igmp snoop igmpv3 v1v2</pre> <p>Enables or disables snooping on IGMP version 1 and version 2 reports. When disabled, the switch drops IGMPv1 and IGMPv2 reports. The default value is enabled.  <b>Command mode:</b> Global configuration</p>
<pre>[no] ip igmp snoop igmpv3 exclude</pre> <p>Enables or disables snooping on IGMPv3 Exclude Reports. When disabled, the switch ignores Exclude Reports. The default value is enabled.  <b>Command mode:</b> Global configuration</p>
<pre>ip igmp snoop igmpv3 enable</pre> <p>Enables IGMP version 3. The default value is disabled.  <b>Command mode:</b> Global configuration</p>
<pre>no ip igmp snoop igmpv3 enable</pre> <p>Disables IGMP version 3.  <b>Command mode:</b> Global configuration</p>
<pre>show ip igmp snoop igmpv3</pre> <p>Displays the current IGMP v3 Snooping configuration.  <b>Command mode:</b> All except User EXEC</p>

## IGMP Relay Configuration

When you configure IGMP Relay, also configure the IGMP Relay multicast routers.

[Table 299](#) describes the commands used to configure IGMP Relay.

Table 299. IGMP Relay Configuration Options

Command Syntax and Usage
<pre>ip igmp relay enable</pre> <p>Enables IGMP Relay.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>no ip igmp relay enable</pre> <p>Disables IGMP Relay.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>ip igmp relay vlan &lt;VLAN number&gt;</pre> <p>Adds the VLAN to the list of IGMP Relay VLANs.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>no ip igmp relay vlan &lt;VLAN number&gt;</pre> <p>Removes the VLAN from the list of IGMP Relay VLANs.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>ip igmp relay report &lt;0-150&gt;</pre> <p>Configures the interval between unsolicited Join reports sent by the switch, in seconds.</p> <p>The default value is 10.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>show ip igmp relay</pre> <p>Displays the current IGMP Relay configuration.</p> <p><b>Command mode:</b> All</p>

## IGMP Relay Multicast Router Configuration

Table 300 describes the commands used to configure multicast routers for IGMP Relay.

Table 300. 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. <b>Command mode:</b> 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. <b>Command mode:</b> Global configuration
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. <b>Command mode:</b> 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. <b>Command mode:</b> Global configuration
ip igmp relay mrouter <1-2> version <1-2>	Configures the IGMP version (1 or 2) of the multicast router. <b>Command mode:</b> Global configuration
ip igmp relay mrouter <1-2> enable	Enables the multicast router. <b>Command mode:</b> Global configuration
no ip igmp relay mrouter <1-2> enable	Disables the multicast router. <b>Command mode:</b> Global configuration
no ip igmp relay mrouter <1-2>	Deletes the multicast router from IGMP Relay. <b>Command mode:</b> Global configuration

## IGMP Static Multicast Router Configuration

Table 301 describes the commands used to configure a static multicast router.

**Note:** When static M routers are used, the switch continues learning dynamic M routers via IGMP snooping. However, dynamic M routers may not replace static M routers. If a dynamic M router has the same port and VLAN combination as a static M router, the dynamic M router is not learned.

Table 301. IGMP Static Multicast Router Configuration Options

Command Syntax and Usage
<pre>ip igmp mrouter &lt;port alias or number&gt; &lt;VLAN number&gt; &lt;version (1-3)&gt;</pre> <p>Selects a port/VLAN combination on which the static multicast router is connected, and configures the IGMP version of the multicast router.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>no ip igmp mrouter &lt;port alias or number&gt; &lt;VLAN number&gt; &lt;version (1-3)&gt;</pre> <p>Removes a static multicast router from the selected port/VLAN combination.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>no ip igmp mrouter all</pre> <p>Removes all static multicast routers.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>clear ip igmp mrouter</pre> <p>Clears the multicast router port table.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>show ip igmp mrouter</pre> <p>Displays the current IGMP Static Multicast Router parameters.</p> <p><b>Command mode:</b> All except User EXEC</p>

## IGMP Filtering Configuration

[Table 302](#) describes the commands used to configure an IGMP filter.

*Table 302. IGMP Filtering Configuration Options*

Command Syntax and Usage
<pre>ip igmp profile &lt;1-16&gt;</pre> <p>Configures the IGMP filter. <b>Command mode:</b> Global configuration To view command options, see <a href="#">page 437</a>.</p>
<pre>ip igmp filtering</pre> <p>Enables IGMP filtering globally. <b>Command mode:</b> Global configuration</p>
<pre>no ip igmp filtering</pre> <p>Disables IGMP filtering globally. <b>Command mode:</b> Global configuration</p>
<pre>show ip igmp filtering</pre> <p>Displays the current IGMP Filtering parameters. <b>Command mode:</b> All</p>

### IGMP Filter Definition

[Table 303](#) describes the commands used to define an IGMP filter.

*Table 303. IGMP Filter Definition Options*

Command Syntax and Usage
<pre>ip igmp profile &lt;1-16&gt; range &lt;IP address 1&gt; &lt;IP address 2&gt;</pre> <p>Configures the range of IP multicast addresses for this filter. <b>Command mode:</b> Global configuration</p>
<pre>ip igmp profile &lt;1-16&gt; action {allow deny}</pre> <p>Allows or denies multicast traffic for the IP multicast addresses specified. The default action is deny. <b>Command mode:</b> Global configuration</p>
<pre>ip igmp profile &lt;1-16&gt; enable</pre> <p>Enables this IGMP filter. <b>Command mode:</b> Global configuration</p>
<pre>no ip igmp profile &lt;1-16&gt; enable</pre> <p>Disables this IGMP filter. <b>Command mode:</b> Global configuration</p>

Table 303. IGMP Filter Definition Options (continued)

Command Syntax and Usage
<pre>no ip igmp profile &lt;1-16&gt;</pre> <p>Deletes this filter's parameter definitions.  <b>Command mode:</b> Global configuration</p>
<pre>show ip igmp profile &lt;1-16&gt;</pre> <p>Displays the current IGMP filter.  <b>Command mode:</b> All</p>

## IGMP Filtering Port Configuration

[Table 304](#) describes the commands used to configure a port for IGMP filtering.

Table 304. IGMP Filter Port Configuration Options

Command Syntax and Usage
<pre>[no] ip igmp filtering</pre> <p>Enables or disables IGMP filtering on this port.  <b>Command mode:</b> Interface port</p>
<pre>ip igmp profile &lt;1-16&gt;</pre> <p>Adds an IGMP filter to this port.  <b>Command mode:</b> Interface port</p>
<pre>no ip igmp profile &lt;1-16&gt;</pre> <p>Removes an IGMP filter from this port.  <b>Command mode:</b> Interface port</p>
<pre>show interface port &lt;port alias or number&gt; igmp-filtering</pre> <p>Displays the current IGMP filter parameters for this port.  <b>Command mode:</b> All except User EXEC</p>

## IGMP Advanced Configuration

Table 301 describes the commands used to configure advanced IGMP parameters.

Table 305. IGMP Advanced Configuration Options

Command Syntax and Usage	
ip igmp query-interval <1-600>	<p>Sets the IGMP router query interval, in seconds. The default value is 125.</p> <p><b>Command mode:</b> Global configuration</p>
ip igmp robust <1-10>	<p>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 1.</p> <p><b>Command mode:</b> Global configuration</p>
ip igmp timeout <1-255>	<p>Configures the timeout value for IGMP Membership Reports (host). Once the timeout value is reached, the switch removes the host from its IGMP table, if the conditions are met. The range is from 1 to 255 seconds. The default is 10 seconds.</p> <p><b>Command mode:</b> Global configuration</p>
[no] ip igmp fastleave <VLAN number>	<p>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.</p> <p><b>Command mode:</b> Global configuration</p>
[no] ip igmp snoop rtralert	<p>Enables or disables the Router Alert option in IGMP messages.</p> <p><b>Command mode:</b> Global configuration</p>

## IGMP Querier Configuration

Table 306 describes the commands used to configure IGMP Querier.

Table 306. IGMP Querier Configuration Options

Command Syntax and Usage	
<pre>ip igmp querier vlan &lt;VLAN number&gt; source-ip &lt;IP address&gt;</pre>	<p>Configures the IGMP source IP address for the selected VLAN.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>ip igmp querier vlan &lt;VLAN number&gt; max-response &lt;1-256&gt;</pre>	<p>Configures the maximum time, in tenths of a second, allowed before responding to a Membership Query message. The default value is 100.</p> <p>By varying the Query Response Interval, an administrator may tune the burstiness of IGMP messages on the subnet; larger values make the traffic less bursty, as host responses are spread out over a larger interval.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>ip igmp querier vlan &lt;VLAN number&gt; query-interval &lt;1-608&gt;</pre>	<p>Configures the interval between IGMP Query broadcasts. The default value is 125 seconds.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>ip igmp querier vlan &lt;VLAN number&gt; robustness &lt;1-10&gt;</pre>	<p>Configures the IGMP Robustness variable, which is the number of times that the switch sends each IGMP message. The default value is 1.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>ip igmp querier vlan &lt;VLAN number&gt; election-type [ipv4 mac]</pre>	<p>Sets the IGMP Querier election criteria as IP address or Mac address. The default setting is IPv4.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>ip igmp querier vlan &lt;VLAN number&gt; startup-interval &lt;1-608&gt;</pre>	<p>Configures the Startup Query Interval, which is the interval between General Queries sent out at startup.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>ip igmp querier vlan &lt;VLAN number&gt; startup-count &lt;1-10&gt;</pre>	<p>Configures the Startup Query Count, which is the number of IGMP Queries sent out at startup. Each Query is separated by the Startup Query Interval. The default value is 2.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>ip igmp querier vlan &lt;VLAN number&gt; version [v1 v2 v3]</pre>	<p>Configures the IGMP version. The default version is v3.</p> <p><b>Command mode:</b> Global configuration</p>



Table 306. IGMP Querier Configuration Options (continued)

Command Syntax and Usage
<pre>ip igmp querier enable</pre> <p>Enables IGMP Querier. <b>Command mode:</b> Global configuration</p>
<pre>no ip igmp querier enable</pre> <p>Disables IGMP Querier. <b>Command mode:</b> Global configuration</p>
<pre>show ip igmp querier vlan &lt;VLAN number&gt;</pre> <p>Displays IGMP Querier information for the selected VLAN. <b>Command mode:</b> Global configuration</p>
<pre>show ip igmp querier</pre> <p>Displays the current IGMP Querier parameters. <b>Command mode:</b> All</p>

## IKEv2 Configuration

Table 307 describes the commands used to configure IKEv2.

Table 307. IKEv2 Options

Command Syntax and Usage
<pre>ikev2 retransmit-interval &lt;1-20&gt;</pre> <p>Sets the interval, in seconds, the timeout value in case a packet is not received by the peer and needs to be retransmitted. The default value is 20 seconds. <b>Command mode:</b> Global configuration</p>
<pre>[no] ikev2 cookie</pre> <p>Enables or disables cookie notification. <b>Command mode:</b> Global configuration</p>
<pre>show ikev2</pre> <p>Displays the current IKEv2 settings. <b>Command mode:</b> All</p>

## IKEv2 Proposal Configuration

Table 308 describes the commands used to configure an IKEv2 proposal.

Table 308. IKEv2 Proposal Options

Command Syntax and Usage
<pre>ikev2 proposal</pre> <p>Enter IKEv2 proposal mode. <b>Command mode:</b> Global configuration</p>
<pre>encryption {3des aes-cbc des}</pre> <p>Configures IKEv2 encryption mode. The default value is 3des. <b>Command mode:</b> IKEv2 proposal</p>
<pre>integrity {md5 sha1}</pre> <p>Configures the IKEv2 authentication algorithm type. The default value is sha1. <b>Command mode:</b> IKEv2 proposal</p>
<pre>group {1 2 5 14 24}</pre> <p>Configures the the DH group. The default group is 2. <b>Command mode:</b> IKEv2 proposal</p>

## IKEv2 Preshare Key Configuration

Table 309 describes the commands used to configure IKEv2 preshare keys.

Table 309. IKEv2 Preshare Key Options

Command Syntax and Usage
<pre>ikev2 preshare-key local &lt;1-32 characters&gt;</pre> <p>Configures the local preshare key. The default value is ibm123. <b>Command mode:</b> Global configuration</p>
<pre>ikev2 preshare-key remote &lt;1-32 characters&gt; &lt;IPv6 address&gt;</pre> <p>Configures the remote preshare key for the IPv6 address. <b>Command mode:</b> Global configuration</p>
<pre>show ikev2 preshare-key</pre> <p>Displays the current IKEv2 Preshare key settings. <b>Command mode:</b> Global configuration</p>

## IKEv2 Identification Configuration

Table 310 describes the commands used to configure IKEv2 identification.

Table 310. IKEv2 Identification Options

Command Syntax and Usage
<pre>ikev2 identity local address</pre> <p>Configures the switch to use the supplied IPv6 address as identification. <b>Command mode:</b> Global configuration</p>
<pre>ikev2 identity local fqdn &lt;1-32 characters&gt;</pre> <p>Configures the switch to use the fully-qualified domain name (such as "example.com") as identification. <b>Command mode:</b> Global configuration</p>
<pre>ikev2 identity local email &lt;1-32 characters&gt;</pre> <p>Configures the switch to use the supplied email address (such as "xyz@example.com") as identification. <b>Command mode:</b> Global configuration</p>
<pre>show ikev2 identity</pre> <p>Displays the current IKEv2 identification settings. <b>Command mode:</b> All</p>

## IPsec Configuration

Table 311 describes the commands used to configure IPsec.

Table 311. IPsec Options

Command Syntax and Usage
<pre>ipsec enable</pre> <p>Enables IPsec. <b>Command mode:</b> Global configuration</p>
<pre>no ipsec enable</pre> <p>Disables IPsec. <b>Command mode:</b> Global configuration</p>
<pre>show ipsec</pre> <p>Displays the current IPsec settings. <b>Command mode:</b> All</p>

## IPsec Transform Set Configuration

Table 312 describes the commands used to configure IPsec transforms.

Table 312. IPsec Transform Set Options

Command Syntax and Usage
<pre>ipsec transform-set &lt;I-IO&gt; {ah-md5 ah-sha1 esp-3des esp-aes-cbc    esp-des esp-md5 esp-null esp sha1}</pre> <p>Sets the AH or ESP authentication, encryption, or integrity algorithm. The available algorithms are as follows:</p> <ul style="list-style-type: none"> <li>- ah-md5</li> <li>- ah-sha1</li> <li>- esp-3des</li> <li>- esp-aes-cbc</li> <li>- esp-des</li> <li>- esp-md5</li> <li>- esp-null</li> <li>- esp-sha1</li> </ul> <p><b>Command mode:</b> Global configuration</p>
<pre>ipsec transform-set &lt;I-IO&gt; transport {ah-md5 ah-sha1 esp-3des    esp-aes-cbc esp-des esp-md5 esp-null esp sha1}</pre> <p>Sets transport mode and the AH or ESP authentication, encryption, or integrity algorithm.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>ipsec transform-set &lt;I-IO&gt; tunnel {ah-md5 ah-sha1 esp-3des    esp-aes-cbc esp-des esp-md5 esp-null esp sha1}</pre> <p>Sets tunnel mode and the AH or ESP authentication, encryption, or integrity algorithm.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>no ipsec transform &lt;I-IO&gt;</pre> <p>Deletes the transform set.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>show ipsec transform-set &lt;I-IO&gt;</pre> <p>Displays the current IPsec Transform Set settings.</p> <p><b>Command mode:</b> All</p>

## IPsec Traffic Selector Configuration

Table 313 describes the commands used to configure an IPsec traffic selector.

Table 313. IPsec Traffic Selector Options

Command Syntax and Usage	
<pre>ipsec traffic-selector &lt;1-10&gt; action {permit deny} {any icmp tcp} {&lt;IPv6 address&gt; any}</pre>	<p>Sets the traffic-selector to permit or deny the specified type of traffic.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>src &lt;IPv6 address&gt; any</pre>	<p>Sets the source IPv6 address.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>ipv6 prefixlen &lt;1-128&gt;</pre>	<p>Sets the destination IPv6 prefix length.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>dst &lt;IPv6 address&gt; any</pre>	<p>Sets the destination IP address.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>del</pre>	<p>Deletes the traffic selector.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>cur</pre>	<p>Displays the current IPsec Traffic Selector settings.</p> <p><b>Command mode:</b> All</p>

## IPsec Dynamic Policy Configuration

Table 314 describes the commands used to configure an IPsec dynamic policy.

Table 314. IPsec Dynamic Policy Options

Command Syntax and Usage
<pre>ipsec dynamic-policy &lt;1-10&gt;</pre> <p>Enter IPsec dynamic policy mode. <b>Command mode:</b> Global configuration</p>
<pre>peer &lt;IPv6 address&gt;</pre> <p>Sets the remote peer IP address. <b>Command mode:</b> IPsec dynamic policy</p>
<pre>traffic-selector &lt;1-10&gt;</pre> <p>Sets the traffic selector for the IPsec policy. <b>Command mode:</b> IPsec dynamic policy</p>
<pre>transform-set &lt;1-10&gt;</pre> <p>Sets the transform set for the IPsec policy. <b>Command mode:</b> IPsec dynamic policy</p>
<pre>sa-lifetime &lt;120-86400&gt;</pre> <p>Sets the IPsec SA lifetime in seconds. The default value is 86400 seconds. <b>Command mode:</b> IPsec dynamic policy</p>
<pre>pfs enable disable</pre> <p>Enables/disables perfect forward security. <b>Command mode:</b> IPsec dynamic policy</p>
<pre>show ipsec dynamic-policy &lt;1-10&gt;</pre> <p>Displays the current IPsec dynamic policy settings. <b>Command mode:</b> All</p>

## IPsec Manual Policy Configuration

Table 315 describes the commands used to configure an IPsec manual policy.

Table 315. IPsec Manual Policy Options

Command Syntax and Usage
<pre>ipsec manual-policy &lt;I-10&gt;</pre> <p>Enter IPsec manual policy mode.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>in-ah auth-key &lt;key code (hexadecimal)&gt;</pre> <p>Sets inbound Authentication Header (AH) authenticator key.</p> <p><b>Note:</b> For manual policies, when peering with a third-party device, key lengths are fixed to 20 characters for SHA1 and 16 characters for MD5 encryption.</p> <p><b>Command mode:</b> IPsec manual policy</p>
<pre>peer &lt;IPv6 address&gt;</pre> <p>Sets the remote peer IP address.</p> <p><b>Command mode:</b> IPsec manual policy</p>
<pre>traffic-selector &lt;I-10&gt;</pre> <p>Sets the traffic selector for the IPsec policy.</p> <p><b>Command mode:</b> IPsec manual policy</p>
<pre>transform-set &lt;I-10&gt;</pre> <p>Sets the transform set for the IPsec policy.</p> <p><b>Command mode:</b> IPsec manual policy</p>
<pre>in-ah spi &lt;256-4294967295&gt;</pre> <p>Sets the inbound Authentication Header (AH) Security Parameter Index (SPI).</p> <p><b>Note:</b> For manual policies, when peering with a third-party device, key lengths are fixed to 20 characters for SHA1 and 16 characters for MD5 encryption.</p> <p><b>Command mode:</b> IPsec manual policy</p>
<pre>in-esp cipher-key &lt;key code (hexadecimal)&gt;</pre> <p>Sets the inbound Encapsulating Security Payload (ESP) cipher key.</p> <p><b>Note:</b> For manual policies, when peering with a third-party device, key lengths are fixed to 8 characters for DES and to 24 characters for 3DES and AES-CBC encryption.</p> <p><b>Command mode:</b> IPsec manual policy</p>
<pre>in-esp auth-key &lt;key code (hexadecimal)&gt;</pre> <p>Sets the inbound Encapsulating Security Payload (ESP) authenticator key.</p> <p><b>Note:</b> For manual policies, when peering with a third-party device, key lengths are fixed to 8 characters for DES and to 24 characters for 3DES and AES-CBC encryption.</p> <p><b>Command mode:</b> IPsec manual policy</p>

Table 315. IPsec Manual Policy Options (continued)

Command Syntax and Usage	
<pre>in-esp auth-key spi &lt;256-4294967295&gt;</pre>	<p>Sets the inbound Encapsulating Security Payload (ESP) Security Parameter Index (SPI).</p> <p><b>Note:</b> For manual policies, when peering with a third-party device, key lengths are fixed to 20 characters for SHA1 and 16 characters for MD5 encryption.</p> <p><b>Command mode:</b> IPsec manual policy</p>
<pre>out-ah auth-key &lt;key code (hexadecimal)&gt;</pre>	<p>Sets the outbound Authentication Header (AH) authenticator key.</p> <p><b>Note:</b> For manual policies, when peering with a third-party device, key lengths are fixed to 20 characters for SHA1 and 16 characters for MD5 encryption.</p> <p><b>Command mode:</b> IPsec manual policy</p>
<pre>out-ah spi &lt;256-4294967295&gt;</pre>	<p>Sets the outbound Authentication Header (AH) Security Parameter Index (SPI).</p> <p><b>Note:</b> For manual policies, when peering with a third-party device, key lengths are fixed to 20 characters for SHA1 and 16 characters for MD5 encryption.</p> <p><b>Command mode:</b> IPsec manual policy</p>
<pre>out-esp auth-key &lt;key code (hexadecimal)&gt;</pre>	<p>Sets the outbound Encapsulating Security Payload (ESP) authenticator key.</p> <p><b>Note:</b> For manual policies, when peering with a third-party device, key lengths are fixed to 8 characters for DES and to 24 characters for 3DES and AES-CBC encryption.</p> <p><b>Command mode:</b> IPsec manual policy</p>
<pre>out-esp cipher-key &lt;key code (hexadecimal)&gt;</pre>	<p>Sets the outbound Encapsulating Security Payload (ESP) cipher key.</p> <p><b>Note:</b> For manual policies, when peering with a third-party device, key lengths are fixed to 8 characters for DES and to 24 characters for 3DES and AES-CBC encryption.</p> <p><b>Command mode:</b> IPsec manual policy</p>
<pre>out-esp auth-key spi &lt;256-4294967295&gt;</pre>	<p>Sets the outbound Encapsulating Security Payload (ESP) Security Parameter Index (SPI).</p> <p><b>Note:</b> For manual policies, when peering with a third-party device, key lengths are fixed to 20 characters for SHA1 and 16 characters for MD5 encryption.</p> <p><b>Command mode:</b> IPsec manual policy</p>
<pre>show ipsec manual-policy &lt;1-10&gt;</pre>	<p>Displays the current IPsec manual policy settings.</p> <p><b>Command mode:</b> All</p>



## Domain Name System Configuration

The Domain Name System (DNS) commands are used for defining the primary and secondary DNS servers on your local network, and for setting the default domain name served by the switch services. DNS parameters must be configured prior to using hostname parameters with the `ping`, `traceroute`, and `tftp` commands.

Table 316. Domain Name Service Options

Command Syntax and Usage	
<pre>[no] ip dns primary-server &lt;IP address&gt; [mgt-port data-port]</pre>	<p>You are prompted to set the IPv4 address for your primary DNS server, using dotted decimal notation.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>[no] ip dns secondary-server &lt;IP address&gt; [mgt-port data-port]</pre>	<p>You are prompted to set the IPv4 address for your secondary DNS server, using dotted decimal notation. If the primary DNS server fails, the configured secondary will be used instead.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>[no] ip dns ipv6 primary-server &lt;IP address&gt; [mgt-port data-port]</pre>	<p>You are prompted to set the IPv6 address for your primary DNS server, using hexadecimal format with colons.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>[no] ip dns ipv6 secondary-server &lt;IP address&gt; [mgt-port data-port]</pre>	<p>You are prompted to set the IPv6 address for your secondary DNS server, using hexadecimal format with colons. If the primary DNS server fails, the configured secondary will be used instead.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>ip dns ipv6 request-version {ipv4 ipv6}</pre>	<p>Sets the protocol used for the first request to the DNS server, as follows:</p> <ul style="list-style-type: none"> <li>– IPv4</li> <li>– IPv6</li> </ul> <p><b>Command mode:</b> Global configuration</p>
<pre>[no] ip dns domain-name &lt;string&gt;</pre>	<p>Sets the default domain name used by the switch. For example: <code>mycompany.com</code></p> <p><b>Command mode:</b> Global configuration</p>
<pre>show ip dns</pre>	<p>Displays the current Domain Name System settings.</p> <p><b>Command mode:</b> All except User EXEC</p>

## 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 317. Global BOOTP Relay Configuration Options

Command Syntax and Usage
<pre>[no] ip bootp-relay server &lt;1-5&gt; address &lt;IP address&gt;</pre> <p>Sets the IP address of the selected global BOOTP server.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>ip bootp-relay enable</pre> <p>Globally turns on BOOTP relay.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>no ip bootp-relay enable</pre> <p>Globally turns off BOOTP relay.</p> <p><b>Command mode:</b> Global configuration</p>

## 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 318. BOOTP Relay Broadcast Domain Configuration Options

Command Syntax and Usage
<pre>ip bootp-relay bcast-domain &lt;1-10&gt; vlan &lt;VLAN number&gt;</pre> <p>Configures the VLAN of the broadcast domain. Each broadcast domain must have a unique VLAN.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>ip bootp-relay bcast-domain &lt;1-10&gt; server &lt;1-5&gt; address &lt;IPv4 address&gt;</pre> <p>Sets the IP address of the BOOTP server.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>ip bootp-relay bcast-domain &lt;1-10&gt; enable</pre> <p>Enables BOOTP Relay for the broadcast domain.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>no ip bootp-relay bcast-domain &lt;1-10&gt; enable</pre> <p>Disables BOOTP Relay for the broadcast domain. When disabled, BOOTP Relay is performed by one of the global BOOTP servers.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>no ip bootp-relay bcast-domain &lt;1-10&gt;</pre> <p>Deletes the selected broadcast domain configuration.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>show ip bootp-relay</pre> <p>Displays the current parameters for the BOOTP Relay broadcast domain.</p> <p><b>Command mode:</b> All</p>

## 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 319. Option 82 Configuration Options

Command Syntax and Usage
<pre>ip bootp-relay information enable</pre> <p>Turns BOOTP Option 82 on.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>[no] ip bootp-relay information enable</pre> <p>Turns BOOTP Option 82 off.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>ip bootp-relay information policy {keep drop replace}</pre> <p>Configures the DHCP re-forwarding policy, as follows:</p> <ul style="list-style-type: none"><li>– <b>Keep:</b> Retains requests that contain relay information if the option 82 information is also present.</li><li>– <b>Drop:</b> Discards requests that contain relay information if the option 82 information is also present.</li><li>– <b>Replace:</b> Replace the relay information in requests that also contain option 82 information.</li></ul> <p><b>Command mode:</b> Global configuration</p>
<pre>show ip bootp-relay</pre> <p>Displays the current BOOTP Option 82 parameters.</p> <p><b>Command mode:</b> All</p>

## 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. IBM N/OS has extended VRRP to include virtual servers as well, allowing for full active/active redundancy between switches. For more information on VRRP, see the “High Availability” chapter in the *IBM N/OS 7.6 Application Guide*.

Table 320. Virtual Router Redundancy Protocol Options

Command Syntax and Usage	
<code>router vrrp</code>	Enter Router VRRP configuration mode. <b>Command mode:</b> Global configuration
<code>holdoff &lt;0-255&gt;</code>	Globally sets the time, in seconds, VRRP waits from when the master switch goes down until elevating a new switch to be the master switch. <b>Command mode:</b> Router VRRP
<code>enable</code>	Globally enables VRRP on this switch. <b>Command mode:</b> Router VRRP
<code>no enable</code>	Globally disables VRRP on this switch. <b>Command mode:</b> Router VRRP
<code>show ip vrrp</code>	Displays the current VRRP parameters. <b>Command mode:</b> 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 321. VRRP Virtual Router Configuration Options

Command Syntax and Usage
<pre>virtual-router &lt;1-128&gt; virtual-router-id &lt;1-128&gt;</pre> <p>Defines the virtual router ID (VRID). This is used in conjunction with the <code>[no] virtual-router &lt;VRID&gt; address &lt;IP address&gt;</code> command below to define a virtual router on this switch. To create a pool of VRRP-enabled routing devices which can provide redundancy to each other, each participating VRRP device must be configured with the same virtual router.</p> <p>The VRID for standard virtual routers (where the virtual router IP address is not the same as any virtual server) can be any integer between 1 and 128. The default value is 1.</p> <p>All VRID values must be unique within the VLAN to which the virtual router's IP interface belongs.</p> <p><b>Command mode:</b> Router VRRP</p>
<pre>[no] virtual-router &lt;1-128&gt; address &lt;IP address&gt;</pre> <p>Defines the IP address for this virtual router using dotted decimal notation. This is used in conjunction with the preceding VRID to configure the same virtual router on each participating VRRP device. The default address is 0.0.0.0.</p> <p><b>Command mode:</b> Router VRRP</p>
<pre>virtual-router &lt;1-128&gt; interface &lt;interface number&gt;</pre> <p>Selects a switch IP interface. If the IP interface has the same IP address as the <code>address</code> option, this switch is considered the "owner" of the defined virtual router. An owner has a special priority of 255 (highest) and will always assume the role of master router, even if it must pre-empt another virtual router which has assumed master routing authority. This pre-emption occurs even if the <code>preem</code> option below is disabled. The default value is 1.</p> <p><b>Command mode:</b> Router VRRP</p>
<pre>[no] virtual-router &lt;1-126&gt; next-hop &lt;IP address&gt; [arp   icmp] [interval &lt;1-60&gt;] [retry &lt;1-3&gt;]</pre> <p>Defines the next-hop IP address and tracking parameters. If not successful, the command will retry the health check at regular intervals of the specified number of seconds for the number of retries specified by <code>retry</code>. Use the <code>no</code> form of the command to remove the tracking on a particular next-hop.</p> <p>Default values are <code>icmp</code>, 2 seconds, and 3 retries.</p> <p><b>Note:</b> Up to 4 unique next-hops can be configured for a virtual router. All 4 next-hops will be tracked.</p> <p><b>Command mode:</b> Router VRRP</p>

Table 321. VRRP Virtual Router Configuration Options (continued)

Command Syntax and Usage	
<pre>virtual-router &lt;1-128&gt; priority &lt;1-254&gt;</pre>	<p>Defines the election priority bias for this virtual server. The priority value can be any integer between 1 and 254. The default value is 100.</p> <p>During the master router election process, the routing device with the highest virtual router priority number wins. If there is a tie, the device with the highest IP interface address wins. If this virtual router's IP address is the same as the one used by the IP interface, the priority for this virtual router will automatically be set to 255 (highest).</p> <p>When priority tracking is used, this base priority value can be modified according to a number of performance and operational criteria.</p> <p><b>Command mode:</b> Router VRRP</p>
<pre>virtual-router &lt;1-128&gt; timers advertise &lt;1-255&gt;</pre>	<p>Defines the time interval between VRRP master advertisements. This can be any integer between 1 and 255 seconds. The default value is 1.</p> <p><b>Command mode:</b> Router VRRP</p>
<pre>virtual-router &lt;1-128&gt; timers preempt-delay-time &lt;0-255&gt;</pre>	<p>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.</p> <p><b>Command mode:</b> Router VRRP</p>
<pre>[no] virtual-router &lt;1-128&gt; preemption [priority-only]</pre>	<p>Enables or disables master preemption. When enabled, if this virtual router is in backup mode but has a higher priority than the current master, this virtual router will preempt the lower priority master and assume control. Note that even when <code>preemption</code> is disabled, this virtual router will always pre-empt any other master if this switch is the owner (the IP interface address and virtual router <code>addr</code> are the same). By default, this option is enabled.</p> <p>If <code>priority-only</code> is specified, preemption is based on priority and the IP address is disregarded.</p> <p><b>Command mode:</b> Router VRRP</p>
<pre>[no] virtual-router &lt;1-128&gt; fast-advertise</pre>	<p>Enables or disables Fast Advertisements. When enabled, the VRRP master advertisements interval is calculated in units of centiseconds, instead of seconds. For example, if <code>adver</code> is set to 1 and <code>fadver</code> is enabled, master advertisements are sent every .01 second.</p> <p>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.</p> <p><b>Command mode:</b> Router VRRP</p>
<pre>virtual-router &lt;1-128&gt; enable</pre>	<p>Enables this virtual router.</p> <p><b>Command mode:</b> Router VRRP</p>

Table 321. VRRP Virtual Router Configuration Options (continued)

Command Syntax and Usage
<pre>no virtual-router &lt;I-128&gt; enable</pre> <p>Disables this virtual router.</p> <p><b>Command mode:</b> Router VRRP</p>
<pre>no virtual-router &lt;I-128&gt;</pre> <p>Deletes this virtual router from the switch configuration.</p> <p><b>Command mode:</b> Router VRRP</p>
<pre>show ip vrrp virtual-router &lt;I-128&gt;</pre> <p>Displays the current configuration information for this virtual router.</p> <p><b>Command mode:</b> All except User EXEC</p>

## Virtual Router Priority Tracking Configuration

These commands are used for modifying the priority system used when electing the master router from a pool of virtual routers. Various tracking criteria can be used to bias the election results. Each time one of the tracking criteria is met, the priority level for the virtual router is increased by an amount defined through the VRRP Tracking commands.

Criteria are tracked dynamically, continuously updating virtual router priority levels when enabled. If the virtual router preemption option is enabled, this virtual router can assume master routing authority when its priority level rises above that of the current master.

Some tracking criteria apply to standard virtual routers, otherwise called “virtual interface routers.” A virtual *server* router is defined as any virtual router whose IP address is the same as any configured virtual server IP address.

Table 322. VRRP Priority Tracking Configuration Options

Command Syntax and Usage
<pre>[no] virtual-router &lt;I-128&gt; track virtual-routers</pre> <p>When enabled, the priority for this virtual router will be increased for each virtual router in master mode on this switch. This is useful for making sure that traffic for any particular client/server pairing are handled by the same switch, increasing routing and load balancing efficiency. This command is disabled by default.</p> <p><b>Command mode:</b> Router VRRP</p>
<pre>[no] virtual-router &lt;I-128&gt; track interfaces</pre> <p>When enabled, the priority for this virtual router will be increased for each other IP interface active on this switch. An IP interface is considered active when there is at least one active port on the same VLAN. This helps elect the virtual routers with the most available routes as the master. This command is disabled by default.</p> <p><b>Command mode:</b> Router VRRP</p>



Table 322. VRRP Priority Tracking Configuration Options

Command Syntax and Usage	
[no] virtual-router <I-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. <b>Command mode:</b> Router VRRP
[no] virtual-router <I-128> track next-hops <0-254>	When enabled, the priority for this virtual router will be increased for all active next hops. A next-hop is considered active if it is configured. This command is disabled by default. <b>Command mode:</b> Router VRRP
show ip vrrp virtual-router <I-128> track	Displays the current configuration for priority tracking for this virtual router. <b>Command mode:</b> 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 323. VRRP Virtual Router Group Configuration Options

Command Syntax and Usage	
group virtual-router-id <I-128>	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 128. All VRID values must be unique within the VLAN to which the virtual router’s IP interface (see <i>interface</i> ) belongs. The default virtual router ID is 1. <b>Command mode:</b> Router VRRP
group interface <interface number>	Selects a switch IP interface. The default switch IP interface number is 1. <b>Command mode:</b> Router VRRP

Table 323. VRRP Virtual Router Group Configuration Options (continued)

Command Syntax and Usage	
group interface <interface number> restricted	<p>Enables or disables restricted VRRP control traffic on an interface. When enabled, the VRRP control messages can be sent to a dedicated interface only. This helps preventing control messages from being dropped.</p> <p><b>Command mode:</b> Router VRRP</p>
group priority <1-254>	<p>Defines the election priority bias for this virtual router group. This can be any integer between 1 and 254. The default value is 100.</p> <p>During the master router election process, the routing device with the highest virtual router priority number wins. If there is a tie, the device with the highest IP interface address wins. If this virtual router's IP address (<code>addr</code>) is the same as the one used by the IP interface, the priority for this virtual router will automatically be set to 255 (highest).</p> <p>When priority tracking is used, this base priority value can be modified according to a number of performance and operational criteria.</p> <p><b>Command mode:</b> Router VRRP</p>
group advertisement <1-255>	<p>Defines the time interval between VRRP master advertisements. This can be any integer between 1 and 255 seconds. The default is 1.</p> <p><b>Command mode:</b> Router VRRP</p>
[no] group preemption [priority-only]	<p>Enables or disables master pre-emption. When enabled, if the virtual router group is in backup mode but has a higher priority than the current master, this virtual router will pre-empt the lower priority master and assume control. Note that even when <code>preemption</code> is disabled, this virtual router will always pre-empt any other master if this switch is the owner (the IP interface address and virtual router address are the same). By default, this option is <code>enabled</code>.</p> <p>If <code>priority-only</code> is specified, preemption is based on priority and the IP address is disregarded.</p> <p><b>Command mode:</b> Router VRRP</p>
[no] group fast-advertise	<p>Enables or disables Fast Advertisements. When enabled, the VRRP master advertisements interval is calculated in units of centiseconds, instead of seconds. For example, if <code>adver</code> is set to 1 and <code>fadver</code> is enabled, master advertisements are sent every .01 second.</p> <p>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.</p> <p><b>Command mode:</b> Router VRRP</p>
group enable	<p>Enables the virtual router group.</p> <p><b>Command mode:</b> Router VRRP</p>

Table 323. VRRP Virtual Router Group Configuration Options (continued)

Command Syntax and Usage
<pre>no group enable</pre> <p>Disables the virtual router group.</p> <p><b>Command mode:</b> Router VRRP</p>
<pre>no group</pre> <p>Deletes the virtual router group from the switch configuration.</p> <p><b>Command mode:</b> Router VRRP</p>
<pre>show ip vrrp group</pre> <p>Displays the current configuration information for the virtual router group.</p> <p><b>Command mode:</b> All except User EXEC</p>

## 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 324. Virtual Router Group Priority Tracking Configuration Options

Command Syntax and Usage
<pre>[no] group track interfaces</pre> <p>When enabled, the priority for this virtual router will be increased for each other IP interface active on this switch. An IP interface is considered active when there is at least one active port on the same VLAN. This helps elect the virtual routers with the most available routes as the master. This command is disabled by default.</p> <p><b>Command mode:</b> Router VRRP</p>
<pre>[no] group track ports</pre> <p>When enabled, the priority for this virtual router will be increased for each active port on the same VLAN. A port is considered “active” if it has a link and is forwarding traffic. This helps elect the virtual routers with the most available ports as the master. This command is disabled by default.</p> <p><b>Command mode:</b> Router VRRP</p>
<pre>show ip vrrp group track</pre> <p>Displays the current configuration for priority tracking for this virtual router.</p> <p><b>Command mode:</b> All except User EXEC</p>

## VRRP Interface Configuration

**Note:** The *interface* represents the IP interface on which authentication parameters must be configured.

These commands are used for configuring VRRP authentication parameters for the IP interfaces used with the virtual routers.

Table 325. VRRP Interface Options

Command Syntax and Usage	
<code>interface &lt;interface number&gt; authentication {password none}</code>	Defines the type of authentication that will be used: <code>none</code> (no authentication) or <code>password</code> (password authentication). <b>Command mode:</b> Router VRRP
<code>[no] interface &lt;interface number&gt; password &lt;password&gt;</code>	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 <code>interface authentication</code> above). <b>Command mode:</b> Router VRRP
<code>no interface &lt;interface number&gt;</code>	Clears the authentication configuration parameters for this IP interface. The IP interface itself is not deleted. <b>Command mode:</b> Router VRRP
<code>show ip vrrp interface &lt;interface number&gt;</code>	Displays the current configuration for this IP interface's authentication parameters. <b>Command mode:</b> 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 456](#)), the priority level for the virtual router is increased by a defined amount.

Table 326. VRRP Tracking Configuration Options

Command Syntax and Usage
<pre>tracking-priority-increment virtual-routers &lt;0-254&gt;</pre> <p>Defines the priority increment value (0 through 254) for virtual routers in master mode detected on this switch. The default value is 2.</p> <p><b>Command mode:</b> Router VRRP</p>
<pre>tracking-priority-increment interfaces &lt;0-254&gt;</pre> <p>Defines the priority increment value for active IP interfaces detected on this switch. The default value is 2.</p> <p><b>Command mode:</b> Router VRRP</p>
<pre>tracking-priority-increment next-hop &lt;0-254&gt;</pre> <p>Defines the priority increment value for each next-hop that is active or subtracted.</p> <p><b>Command mode:</b> Router VRRP</p>
<pre>tracking-priority-increment ports &lt;0-254&gt;</pre> <p>Defines the priority increment value for active ports on the virtual router's VLAN. The default value is 2.</p> <p><b>Command mode:</b> Router VRRP</p>
<pre>show ip vrrp tracking-priority-increment</pre> <p>Displays the current configuration of priority tracking increment values.</p> <p><b>Command mode:</b> All except User EXEC</p>

**Note:** These priority tracking options only define increment values. These options do not affect the VRRP master router election process until options under the VRRP Virtual Router Priority Tracking Commands (see [page 456](#)) are enabled.

# Protocol Independent Multicast Configuration

Table 327. PIM Configuration Options

Command Syntax and Usage
<pre>ip pim component &lt;1-2&gt;</pre> <p>Enter PIM component mode. <b>Command mode:</b> Global configuration</p>
<pre>ip pim regstop-ratelimit-period &lt;0-2147483647&gt;</pre> <p>Configures the register stop rate limit, in seconds. The default value is 5. <b>Command mode:</b> Global configuration</p>
<pre>[no] ip pim static-rp enable</pre> <p>Enables or disables static RP configuration. The default setting is disabled. <b>Command mode:</b> Global configuration</p>
<pre>[no] ip pim pmbr enable</pre> <p>Enables or disables PIM border router. The default setting is disabled. <b>Command mode:</b> Global configuration</p>
<pre>ip pim enable</pre> <p>Globally turns PIM on. <b>Command mode:</b> Global configuration</p>
<pre>no ip pim enable</pre> <p>Globally turns PIM off. <b>Command mode:</b> Global configuration</p>
<pre>clear ip pim mroute</pre> <p>Clears PIM multicast router entries. <b>Command mode:</b> Global configuration</p>

## PIM Component Configuration

Use these commands to configure PIM components.

Table 328. PIM Component Configuration Options

Command Syntax and Usage
<pre>ip pim component &lt;I-2&gt;</pre> <p>Enter PIM component mode. <b>Command mode:</b> Global configuration</p>
<pre>mode {dense sparse}</pre> <p>Configures the operational mode of the PIM router (dense or sparse). <b>Command mode:</b> PIM Component</p>
<pre>show ip pim component [&lt;I-2&gt;]</pre> <p>Displays the current PIM component configuration settings. <b>Command mode:</b> All</p>

## RP Candidate Configuration

Use these commands to configure a PIM router Rendezvous Point (RP) candidate.

Table 329. RP Candidate Configuration Options

Command Syntax and Usage
<pre>rp-candidate rp-address &lt;group multicast address&gt; &lt;group subnet mask&gt; &lt;IP address&gt;</pre> <p>Adds an RP candidate. <b>Command mode:</b> PIM Component</p>
<pre>no rp-candidate rp-address &lt;group multicast address&gt; &lt;group subnet mask&gt; &lt;IP address&gt;</pre> <p>Removes the specified RP candidate. <b>Command mode:</b> PIM Component</p>
<pre>rp-candidate holdtime &lt;0-255&gt;</pre> <p>Configures the hold time of the RP candidate, in seconds. <b>Command mode:</b> PIM Component</p>

## RP Static Configuration

Use these commands to configure a static PIM router Rendezvous Point (RP).

Table 330. RP Static Configuration Options

Command Syntax and Usage
<pre>rp-static rp-address &lt;group multicast address&gt; &lt;group subnet mask&gt; &lt;IP address&gt;</pre> <p>Adds a static RP.</p> <p><b>Command mode:</b> PIM Component</p>
<pre>no rp-static rp-address &lt;group multicast address&gt; &lt;group subnet mask&gt;</pre> <p>Removes the specified static RP.</p> <p><b>Command mode:</b> PIM Component</p>

## PIM Interface Configuration

Table 331. PIM Interface Configuration Options

Command Syntax and Usage
<pre>interface ip &lt;interface number&gt;</pre> <p>Enter Interface IP mode.</p> <p><b>Command mode:</b> Global Configuration</p>
<pre>ip pim hello-interval &lt;0-65535&gt;</pre> <p>Configures the time interval, in seconds, between PIM Hello packets. The default value is 30.</p> <p><b>Command mode:</b> Interface IP</p>
<pre>ip pim join-prune-interval &lt;0-65535&gt;</pre> <p>Configures the interval between Join Prune messages, in seconds. The default value is 60.</p> <p><b>Command mode:</b> Interface IP</p>
<pre>ip pim cbsr-preference &lt;0-255&gt;</pre> <p>Configures the candidate bootstrap router preference.</p> <p><b>Command mode:</b> Interface IP</p>
<pre>ip pim component-id &lt;1-2&gt;</pre> <p>Defines the component ID for the interface.</p> <p><b>Command mode:</b> Interface IP</p>
<pre>ip pim hello-holdtime &lt;1-65535&gt;</pre> <p>Configures the time period in seconds for which a neighbor is to consider this switch to be operative (up). The default value is 105.</p> <p><b>Command mode:</b> Interface IP</p>



Table 331. PIM Interface Configuration Options (continued)

Command Syntax and Usage	
ip pim dr-priority <0-4294967294>	Configures the designated router priority. The default value is 1. <b>Command mode:</b> Interface IP
ip pim override-interval <0-65535>	Configures the override interval for the router interface, in seconds. <b>Command mode:</b> Interface IP
ip pim lan-delay <0-32767>	Configures the LAN delay value for the router interface, in seconds. <b>Command mode:</b> Interface IP
[no] ip pim border-bit	Enables or disables the interface as a border router. The default setting is disabled. <b>Command mode:</b> Interface IP
[no] ip pim lan-prune-delay	Enables or disables LAN delay advertisements on the interface. The default setting is disabled. <b>Command mode:</b> 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. <b>Command mode:</b> Interface IP
[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> <b>Command mode:</b> Interface IP
ip pim enable	Enables PIM on the interface. <b>Command mode:</b> Interface IP
no ip pim enable	Disables PIM on the interface. <b>Command mode:</b> Interface IP

Table 331. PIM Interface Configuration Options (continued)

Command Syntax and Usage
<pre>show ip pim neighbor-filters</pre> <p>Displays the configured PIM neighbor filters.</p> <p><b>Command mode:</b> All</p>
<pre>show ip pim interface [&lt;interface number&gt; detail loopback port &lt;port number&gt;]</pre> <p>Displays the current PIM interface parameters.</p> <p><b>Command mode:</b> All</p>

## IPv6 Default Gateway Configuration

The switch supports IPv6 default gateways, as follows:

- Gateway 1: data traffic
- Gateway 4: management port

[Table 332](#) describes the IPv6 Default Gateway Configuration commands.

Table 332. IPv6 Default Gateway Configuration Options

Command Syntax and Usage
<pre>ip gateway6 {1 4} address &lt;IPv6 address&gt;</pre> <p>Configures the IPv6 address of the default gateway, in hexadecimal format with colons (such as 3001:0:0:0:0:abcd:12).</p> <p><b>Command mode:</b> Global configuration</p>
<pre>[no] ip gateway6 {1 4} enable</pre> <p>Enables or disables the default gateway.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>no ip gateway6 {1 4}</pre> <p>Deletes the default gateway.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>show ipv6 gateway6 {1 4}</pre> <p>Displays the current IPv6 default gateway configuration.</p> <p><b>Command mode:</b> All</p>

## IPv6 Static Route Configuration

Table 333 describes the IPv6 static route configuration commands.

Table 333. IPv6 Static Route Configuration Options

Command Syntax and Usage
<pre>ip route6 &lt;IPv6 address&gt; &lt;prefix length&gt; &lt;IPv6 gateway address&gt; [&lt;interface number&gt;]</pre> <p>Adds an IPv6 static route.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>no ip route6 &lt;IPv6 address&gt; &lt;prefix length&gt;</pre> <p>Removes the selected route.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>no ip route6 [destination-address &lt;IPv6 address&gt;   gateway &lt;default gateway address&gt; interface &lt;I-128&gt;  all]</pre> <p>Clears the selected IPv6 static routes.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>show ipv6 route static</pre> <p>Displays the current static route configuration.</p> <p><b>Command mode:</b> All</p>

## IPv6 Neighbor Discovery Cache Configuration

Table 334 describes the IPv6 Neighbor Discovery cache configuration commands.

Table 334. IPv6 Neighbor Discovery Cache Configuration Options

Command Syntax and Usage
<pre>ip neighbors &lt;IPv6 address&gt; &lt;MAC address&gt; vlan &lt;VLAN number&gt; port &lt;port number or alias&gt;</pre> <p>Adds a static entry to the Neighbor Discovery cache table.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>no ip neighbors {&lt;IPv6 address&gt;  all}</pre> <p>Deletes the selected entry from the static Neighbor Discovery cache table.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>no ip neighbors [all if all interface port all vlan &lt;VLAN number&gt;  all]</pre> <p>Clears the selected static entries in the Neighbor Discovery cache table.</p> <p><b>Command mode:</b> Global configuration</p>

## IPv6 Path MTU Configuration

The following table describes the configuration options for Path MTU (Maximum Transmission Unit). The Path MTU cache can consume system memory and affect performance. These commands allow you to manage the Path MTU cache.

Table 335. IPv6 Path MTU Options

Command Syntax and Usage
<pre>ip pmtu6 timeout 0 &lt;10-100&gt;</pre> <p>Sets the timeout value for Path MTU cache entries, in minutes. Enter 0 (zero) to set the timeout to infinity (no timeout). The default value is 10 minutes. <b>Command mode:</b> Global configuration</p>
<pre>clear ipv6 pmtu</pre> <p>Clears all entries in the Path MTU cache. <b>Command mode:</b> All Except User EXEC</p>
<pre>show ipv6 pmtu</pre> <p>Displays the current Path MTU configuration. <b>Command mode:</b> All</p>

## IPv6 Neighbor Discovery Prefix Configuration

The following table describes the Neighbor Discovery prefix configuration options. These commands allow you to define a list of prefixes to be placed in Prefix Information options in Router Advertisement messages sent from an interface.

Table 336. IPv6 Neighbor Discovery Prefix Options

Command Syntax and Usage	
<pre>interface ip &lt;1-127&gt;</pre>	<p>Enters Interface IP mode.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>ipv6 nd prefix {&lt;IPv6 prefix&gt; &lt;prefix length&gt;} [no-advertise]</pre>	<p>Adds a Neighbor Discovery prefix to the interface. The default setting is enabled.</p> <p>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.</p> <p>Additional prefix options are listed below.</p> <p><b>Command mode:</b> Interface IP</p>
<pre>no ipv6 nd prefix [&lt;IPv6 prefix&gt; &lt;prefix length&gt;]  interface all</pre>	<p>Removes a Neighbor Discovery prefix. If you specify an interface number, all prefixes for the interface are removed.</p> <p><b>Command mode:</b> Interface IP</p>
<pre>ipv6 nd prefix {&lt;IPv6 prefix&gt; &lt;prefix length&gt;}   valid-lifetime &lt;0-4294967295&gt; [infinite variable]   preferred-lifetime &lt;0-4294967295&gt; [infinite variable]</pre>	<p>Configures the Valid Lifetime and (optionally) the Preferred Lifetime of the prefix, in seconds.</p> <p>The Valid Lifetime is the length of time (relative to the time the packet is sent) that the prefix is valid for the purpose of on-link determination. The default value is 2592000.</p> <p>The Preferred Lifetime is the length of time (relative to the time the packet is sent) that addresses generated from the prefix via stateless address autoconfiguration remain preferred. The default value is 604800.</p> <p><b>Note:</b> The Preferred Lifetime value must not exceed the Valid Lifetime value.</p> <p><b>Command mode:</b> Interface IP</p>
<pre>ipv6 nd prefix {&lt;IPv6 prefix&gt; &lt;prefix length&gt;} off-link</pre>	<p>Disables the on-link flag. When enabled, the on-link flag indicates that this prefix can be used for on-link determination. When disabled, the advertisement makes no statement about on-link or off-link properties of the prefix. The default setting is enabled.</p> <p>To clear the off-link flag, omit the off-link parameter when you issue this command.</p> <p><b>Command mode:</b> Interface IP</p>

Table 336. IPv6 Neighbor Discovery Prefix Options (continued)

Command Syntax and Usage
<pre>ipv6 nd prefix {&lt;IPv6 prefix&gt; &lt;prefix length&gt;} no-autoconfig</pre> <p>Disables the autonomous flag. When enabled, the autonomous flag indicates that the prefix can be used for stateless address configuration. The default setting is enabled.</p> <p><b>Command mode:</b> Interface IP</p>
<pre>show ipv6 prefix {&lt;interface number&gt;}</pre> <p>Displays current Neighbor Discovery prefix parameters.</p> <p><b>Command mode:</b> All</p>

## IPv6 Prefix Policy Table Configuration

The following table describes the configuration options for the IPv6 Prefix Policy Table. The Prefix Policy Table allows you to override the default address selection criteria.

Table 337. IPv6 Prefix Policy Table Options

Command Syntax and Usage
<pre>ip prefix-policy &lt;IPv6 prefix&gt; &lt;prefix length&gt; &lt;precedence (0-100)&gt; &lt;label (0-100)&gt;</pre> <p>Adds a Prefix Policy Table entry. Enter the following parameters:</p> <ul style="list-style-type: none"> <li>– IPv6 address prefix</li> <li>– Prefix length</li> <li>– <b>Precedence:</b> The precedence is used to sort destination addresses. Prefixes with a higher precedence are sorted before those with a lower precedence.</li> <li>– <b>Label:</b> The label allows you to select prefixes based on matching labels. Source prefixes are coupled with destination prefixes if their labels match.</li> </ul> <p><b>Command mode:</b> Global configuration</p>
<pre>no ip prefix-policy &lt;IPv6 prefix&gt; &lt;prefix length&gt; &lt;precedence (0-100)&gt; &lt;label (0-100)&gt;</pre> <p>Removes a prefix policy table entry.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>show ip prefix-policy</pre> <p>Displays the current Prefix Policy Table configuration.</p> <p><b>Command mode:</b> All</p>

## IP Loopback Interface Configuration

An IP loopback interface is not connected to any physical port. A loopback interface is always accessible over the network.

Table 338. IP Loopback Interface Configuration Options

Command Syntax and Usage	
<code>interface loopback &lt;I-5&gt;</code>	Enter Interface loopback mode. <b>Command mode:</b> Global configuration
<code>no interface loopback &lt;I-5&gt;</code>	Deletes the selected loopback interface. <b>Command mode:</b> Global configuration
<code>ip address &lt;IP address&gt;</code>	Defines the loopback interface IP address. <b>Command mode:</b> Interface loopback
<code>ip netmask &lt;subnet mask&gt;</code>	Defines the loopback interface subnet mask. <b>Command mode:</b> Interface loopback
<code>ip ospf area &lt;area number&gt;</code>	Configures the OSPF area index used by the loopback interface. <b>Command mode:</b> Interface loopback
<code>[no] ip ospf enable</code>	Enables or disables OSPF for the loopback interface. <b>Command mode:</b> Interface loopback
<code>enable</code>	Enables the loopback interface. <b>Command mode:</b> Interface loopback
<code>no enable</code>	Disables the loopback interface. <b>Command mode:</b> Interface loopback
<code>show interface loopback &lt;I-5&gt;</code>	Displays the current IP loopback interface parameters. <b>Command mode:</b> All

# Flooding VLAN Configuration Menu

Table 339. Flooding VLAN Menu Options

Command Syntax and Usage
<p><code>flood</code></p> <p>Configures the switch to flood unregistered IP multicast traffic to all ports. The default setting is <code>enabled</code>.</p> <p><b>Note:</b> If none of the IGMP hosts reside on the VLAN of the streaming server for a IPMC group, you must disable IGMP flooding to ensure that multicast data is forwarded across the VLANs for that IPMC group.</p> <p><b>Command mode:</b> VLAN</p>
<p><code>cpu</code></p> <p>Configures the switch to forward unregistered IP multicast traffic to the MP, which adds an entry in the IPMC table, as follows:</p> <ul style="list-style-type: none"><li>– If no Mrouter is present, drop subsequent packets with same IPMC.</li><li>– If an Mrouter is present, forward subsequent packets to the Mrouter(s) on the ingress VLAN.</li></ul> <p>The default setting is <code>enabled</code>.</p> <p><b>Note:</b> If both <code>flood</code> and <code>cpu</code> are disabled, the switch drops all unregistered IPMC traffic.</p> <p><b>Command mode:</b> VLAN</p>
<p><code>[no] optflood</code></p> <p>Enables or disables optimized flooding. When enabled, optimized flooding avoids packet loss during the learning period. The default setting is <code>disabled</code>.</p> <p><b>Command mode:</b> VLAN</p>
<p><code>show vlan &lt;vlan number&gt; information</code></p> <p>Displays the current flooding parameters for the selected VLAN.</p> <p><b>Command mode:</b> All</p>



## DHCP Snooping

DHCP Snooping provides security by filtering untrusted DHCP packets and by maintaining a binding table of trusted interfaces.

Table 340. 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. <b>Command mode:</b> Global configuration
no ip dhcp snooping vlan <VLAN number>	Removes the selected VLAN from DHCP Snooping. <b>Command mode:</b> 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. <b>Command mode:</b> 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. <b>Command mode:</b> Global configuration
ip dhcp snooping	Turns on DHCP Snooping. <b>Command mode:</b> Global configuration
no ip dhcp snooping	Turns off DHCP Snooping. <b>Command mode:</b> Global configuration
[no] ip dhcp snooping information option-insert	Enables or disables option 82 support for DHCP Snooping. When enabled, DHCP Snooping performs the following functions: <ul style="list-style-type: none"> <li>– If a DHCP packet from a client contains option 82 information, the information is retained.</li> <li>– When DHCP Snooping forwards a DHCP packet from a client, option 82 information is added to the packet;</li> <li>– When DHCP snooping forward a DHCP packet from a server, option 82 information is removed from the packet.</li> </ul> <b>Command mode:</b> Global configuration
show ip dhcp snooping	Displays the current DHCP Snooping parameters. <b>Command mode:</b> All

---

## Converged Enhanced Ethernet Configuration

Table 341 describes the Converged Enhanced Ethernet (CEE) configuration commands.

Table 341. CEE Configuration Options

Command Syntax and Usage
<code>cee enable</code> Globally turns CEE on. <b>Command mode:</b> Global configuration
<code>no cee enable</code> Globally turns CEE off. <b>Command mode:</b> Global configuration
<code>[no] cee iscsi enable</code> Enables or disables ISCSI TLV advertisements. <b>Command mode:</b> Global configuration
<code>show cee iscsi</code> Displays the current ISCSI TLV parameters. <b>Command mode:</b> All
<code>show cee</code> Displays the current CEE parameters. <b>Command mode:</b> 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 342](#) describes the global ETS Priority Group configuration options.

Table 342. Global ETS Priority Group Options

Command Syntax and Usage
<pre>cee global ets priority-group pgid &lt;0-7, 15&gt; priority &lt;802.1p priority (0-7)&gt; bandwidth &lt;bandwidth percentage (0, 10-100)&gt;</pre> <p>Allows you to configure Priority Group parameters. You can enter the link bandwidth percentage allocated to the Priority Group, and also assign one or more 802.1p values to the Priority Group.</p> <p><b>Note:</b> Priority Group 15 is a strict priority group and does not need bandwidth assigned to it.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>[no] cee global ets priority-group pgid &lt;0-7, 15&gt; description &lt;1-31 characters&gt;</pre> <p>Enter text that describes this Priority Group.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>cee global ets priority-group pgid &lt;0-7, 15&gt; priority &lt;0-7&gt;</pre> <p>Adds one or more 802.1p priority values to the Priority Group. Enter one value per line, null to end.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>show cee global ets priority-group &lt;0-7, 15&gt;</pre> <p>Displays the current global ETS Priority Group parameters.</p> <p><b>Command mode:</b> All</p>
<pre>show cee global ets</pre> <p>Displays the current global ETS parameters.</p> <p><b>Command mode:</b> All</p>

## Priority Flow Control Configuration

Priority-based Flow Control (PFC) enhances flow control by allowing the switch to pause traffic based on its 802.1p priority value, while allowing traffic at other priority levels to continue.

### 802.1p PFC Configuration

[Table 344](#) describes the 802.1p Priority Flow Control (PFC) configuration options.

Table 343. PFC 802.1p Configuration Options

Command Syntax and Usage
<pre>cee port &lt;port alias, number, or range&gt; pfc priority &lt;0-7&gt; enable</pre> <p>Enables Priority Flow Control on the selected 802.1p priority.</p> <p><b>Note:</b> PFC can be enabled on 802.1p priority 3 and one other priority only.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>no cee port &lt;port alias, number, or range&gt; pfc priority &lt;0-7&gt; enable</pre> <p>Disables Priority Flow Control on the selected 802.1p priority.</p> <p><b>Note:</b> PFC on 802.1p priority 3 cannot be disabled.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>[no] cee port &lt;port alias, number, or range&gt; pfc priority &lt;0-7&gt; description &lt;1-31 characters&gt;</pre> <p>Enter text to describe the priority value.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>show cee port &lt;port alias, number, or range&gt; pfc</pre> <p>Displays the current 802.1p Priority Flow Control configuration on the specified port or ports.</p> <p><b>Command mode:</b> All</p>
<pre>show cee port &lt;port alias, number, or range&gt; pfc priority &lt;0-7&gt;</pre> <p>Displays the current 802.1p Priority Flow Control parameters.</p> <p><b>Command mode:</b> All</p>

## DCBX Port Configuration

Table 344 describes the port DCB Capability Exchange Protocol (DCBX) configuration options.

Table 344. Port DCBX Configuration Options

Command Syntax and Usage	
[no] cee port <port alias, number, or range> dcbx app_proto advertise	<p>Enables or disables DCBX Application Protocol advertisements of configuration data. When enabled, the Advertisement flag is set to 1 (advertise data to the peer device).</p> <p><b>Command mode:</b> Global configuration</p>
[no] cee port <port alias, number, or range> dcbx app_proto willing	<p>Enables or disables Application Protocol willingness to accept configuration data from the peer device. When enabled, the Willing flag is set to 1 (willing to accept data).</p> <p><b>Command mode:</b> Global configuration</p>
[no] cee port <port alias, number, or range> dcbx ets advertise	<p>Enables or disables DCBX ETS advertisements of configuration data. When enabled, the Advertisement flag is set to 1 (advertise data to the peer device).</p> <p><b>Command mode:</b> Global configuration</p>
[no] cee port <port alias, number, or range> dcbx ets willing	<p>Enables or disables ETS willingness to accept configuration data from the peer device. When enabled, the Willing flag is set to 1 (willing to accept data).</p> <p><b>Command mode:</b> Global configuration</p>
[no] cee port <port alias, number, or range> dcbx pfc advertise	<p>Enables or disables DCBX PFC advertisements of configuration data. When enabled, the Advertisement flag is set to 1 (advertise data to the peer device).</p> <p><b>Command mode:</b> Global configuration</p>
[no] cee port <port alias, number, or range> dcbx pfc willing	<p>Enables or disables PFC willingness to accept configuration data from the peer device. When enabled, the Willing flag is set to 1 (willing to accept data).</p> <p><b>Command mode:</b> Global configuration</p>
no cee port <port alias, number, or range> dcbx enable	<p>Disables DCBX on the port.</p> <p><b>Command mode:</b> Global configuration</p>
cee port <port alias, number, or range> dcbx enable	<p>Enables DCBX on the port.</p> <p><b>Command mode:</b> Global configuration</p>
show cee port <port alias, number, or range> dcbx	<p>Displays the current port DCBX parameters.</p> <p><b>Command mode:</b> All</p>

---

## Fibre Channel over Ethernet Configuration

Fibre Channel over Ethernet (FCoE) transports Fibre Channel frames over an Ethernet fabric. The CEE features and FCoE features allow you to create a lossless Ethernet transport mechanism.

[Table 345](#) describes the FCoE configuration options.

*Table 345. FCoE Configuration Options*

<b>Command Syntax and Usage</b>
<code>fcoe fips enable</code> Globally turns FIP Snooping on. <b>Command mode:</b> Global configuration
<code>no fcoe fips enable</code> Globally turns FIP Snooping off. <b>Command mode:</b> Global configuration
<code>[no] fcoe fips timeout-acl</code> Enables or disables ACL time-out removal. When enabled, ACLs associated with expired FCFs and FCoE connections are removed from the system. <b>Command mode:</b> Global configuration
<code>[no] fcoe fips automatic-vlan</code> Enables or disables automatic VLAN creation, based on response received from the connected device. <b>Command mode:</b> Global configuration
<code>show fcoe information</code> Displays the current FCoE parameters. <b>Command mode:</b> 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 346](#) describes the port Fibre Channel over Ethernet Initialization Protocol (FIP) Snooping configuration options.

Table 346. Port FIP Snooping Options

Command Syntax and Usage
<pre>fcoe fips port &lt;port alias or number&gt; fcf-mode [auto on off]</pre> <p>Configures FCoE Forwarding (FCF) on the port, as follows:</p> <ul style="list-style-type: none"><li>– on: Configures the port as a Fibre Channel Forwarding (FCF) port.</li><li>– off: Configures the port as an FCoE node (ENode port).</li><li>– auto: Automatically detect the configuration of the connected device, and configure this port to match.</li></ul> <p><b>Command mode:</b> Global configuration</p>
<pre>fcoe fips port &lt;port alias or number&gt; enable</pre> <p>Enables FIP Snooping on the port. The default setting is enabled.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>no fcoe fips port &lt;port alias or number&gt; enable</pre> <p>Disables FIP Snooping on the port.</p> <p><b>Command mode:</b> Global configuration</p>

---

## Remote Monitoring Configuration

Remote Monitoring (RMON) allows you to monitor traffic flowing through the switch. The RMON MIB is described in RFC 1757.

The following sections describe the Remote Monitoring (RMON) configuration options.

- [“RMON History Configuration” on page 480](#)
- [“RMON Event Configuration” on page 481](#)
- [“RMON Alarm Configuration” on page 482](#)

## RMON History Configuration

[Table 347](#) describes the RMON History commands.

*Table 347. RMON History Configuration Options*

Command Syntax and Usage
<pre>rmon history &lt;I-65535&gt; interface-oid &lt;I-127 characters&gt;</pre> <p>Configures the interface MIB Object Identifier. The IFOID must correspond to the standard interface OID, as follows:</p> <pre>1.3.6.1.2.1.2.2.1.1.x</pre> <p>where x is the ifIndex</p> <p><b>Command mode:</b> Global configuration</p>
<pre>rmon history &lt;I-65535&gt; requested-buckets &lt;I-65535&gt;</pre> <p>Configures the requested number of buckets, which is the number of discrete time intervals over which data is to be saved. The default value is 30.</p> <p>The maximum number of buckets that can be granted is 50.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>rmon history &lt;I-65535&gt; polling-interval &lt;I-3600&gt;</pre> <p>Configures the time interval over which the data is sampled for each bucket.</p> <p>The default value is 1800.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>rmon history &lt;I-65535&gt; owner &lt;I-127 characters&gt;</pre> <p>Enter a text string that identifies the person or entity that uses this History index.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>no rmon history &lt;I-65535&gt;</pre> <p>Deletes the selected History index.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>show rmon history</pre> <p>Displays the current RMON History parameters.</p> <p><b>Command mode:</b> All</p>



## RMON Event Configuration

Table 348 describes the RMON Event commands.

Table 348. RMON Event Configuration Options

Command Syntax and Usage
<pre>rmon event &lt;1-65535&gt; description &lt;1-127 characters&gt;</pre> <p>Enter a text string to describe the event. <b>Command mode:</b> Global configuration</p>
<pre>[no] rmon event &lt;1-65535&gt; type log trap both</pre> <p>Selects the type of notification provided for this event. For log events, an entry is made in the log table and sent to the configured syslog host. For trap events, an SNMP trap is sent to the management station. <b>Command mode:</b> Global configuration</p>
<pre>rmon event &lt;1-65535&gt; owner &lt;1-127 characters&gt;</pre> <p>Enter a text string that identifies the person or entity that uses this event index. <b>Command mode:</b> Global configuration</p>
<pre>no rmon event &lt;1-65535&gt;</pre> <p>Deletes the selected RMON Event index. <b>Command mode:</b> Global configuration</p>
<pre>show rmon event</pre> <p>Displays the current RMON Event parameters. <b>Command mode:</b> All</p>

## RMON Alarm Configuration

The alarm RMON group can track rising or falling values for a MIB object. The MIB object must be a counter, gauge, integer, or time interval. Each alarm index must correspond to an event index that triggers once the alarm threshold is crossed.

[Table 349](#) describes the RMON alarm commands.

Table 349. RMON Alarm Configuration Options

Command Syntax and Usage	
<code>rmon alarm &lt;1-65535&gt; oid &lt;1-127 characters&gt;</code>	Configures an alarm MIB Object Identifier. <b>Command mode:</b> Global configuration
<code>rmon alarm &lt;1-65535&gt; interval &lt;1-65535&gt;</code>	Configures the time interval over which data is sampled and compared with the rising and falling thresholds. The default value is 1800. <b>Command mode:</b> Global configuration
<code>rmon alarm &lt;1-65535&gt; sample abs delta</code>	Configures 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"> <li>– <code>abs</code>—absolute value, the value of the selected variable is compared directly with the thresholds at the end of the sampling interval.</li> <li>– <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.</li> </ul> <b>Command mode:</b> Global configuration
<code>rmon alarm &lt;1-65535&gt; alarm-type rising falling either</code>	Configures the alarm type as rising, falling, or either (rising or falling). <b>Command mode:</b> Global configuration
<code>rmon alarm &lt;1-65535&gt; rising-limit &lt;-2147483647 - 2147483647&gt;</code>	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. <b>Command mode:</b> Global configuration
<code>rmon alarm &lt;1-65535&gt; falling-limit &lt;-2147483647 - 2147483647&gt;</code>	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. <b>Command mode:</b> Global configuration

Table 349. RMON Alarm Configuration Options (continued)

Command Syntax and Usage	
<pre>rmon alarm &lt;I-65535&gt; rising-crossing-index &lt;I-65535&gt;</pre>	<p>Configures the rising alarm event index that is triggered when a rising threshold is crossed.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>rmon alarm &lt;I-65535&gt; falling-crossing-index &lt;I-65535&gt;</pre>	<p>Configures the falling alarm event index that is triggered when a falling threshold is crossed.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>rmon alarm &lt;I-65535&gt; owner &lt;I-127 characters&gt;</pre>	<p>Enter a text string that identifies the person or entity that uses this alarm index.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>no rmon alarm &lt;I-65535&gt;</pre>	<p>Deletes the selected RMON Alarm index.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>show rmon alarm</pre>	<p>Displays the current RMON Alarm parameters.</p> <p><b>Command mode:</b> All</p>

---

## Virtualization Configuration

[Table 350](#) describes the virtualization configuration options.

*Table 350. Virtualization Configuration Options*

Command Syntax and Usage
<pre>virt enable</pre> <p>Enables VMready. Before you enable VMready, you must define one or more server ports. See <a href="#">“Server Port Configuration” on page 291</a>.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>no virt enable</pre> <p>Disables VMready.</p> <p><b>Note:</b> This command deletes all configured VM groups.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>show virt</pre> <p>Displays the current virtualization parameters.</p> <p><b>Command mode:</b> All</p>

## VM Policy Bandwidth Management

**Table 351** describes the bandwidth management options for the selected VM. Use these commands to limit the bandwidth used by each VM.

Table 351. VM Bandwidth Management Options

Command Syntax and Usage
<pre>virt vmpolicy vmbwidth [&lt;MAC address&gt;   &lt;UUID&gt;   &lt;name&gt;     &lt;IP address&gt;   &lt;index number&gt;] txrate &lt;64-10000000&gt;   &lt;max. burst (32-4096)&gt; &lt;ACL number&gt;</pre> <p>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.</p> <p>The second values configures the maximum burst size, in kilobits. Enter one of the following values: 32, 64, 128, 256, 512, 1024, 2048, 4096.</p> <p>The third value represents the ACL assigned to the transmission rate. The ACL is 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.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>virt vmpolicy vmbwidth [&lt;MAC address&gt;   &lt;UUID&gt;   &lt;name&gt;     &lt;IP address&gt;   &lt;index number&gt;] rxrate &lt;64-10000000&gt;</pre> <p>The first value configures Committed Rate—the amount of bandwidth available to traffic transmitted from the switch to the VM, in kilobits per second. Enter the value in multiples of 64.</p> <p>The second values configures the maximum burst size, in Kilobits. Enter one of the following values: 32, 64, 128, 256, 512, 1024, 2048, 4096.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>[no] virt vmpolicy vmbwidth [&lt;MAC address&gt;   &lt;UUID&gt;   &lt;name&gt;     &lt;IP address&gt;   &lt;index number&gt;] bwctrl</pre> <p>Enables or disables bandwidth control on the VM policy.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>[no] virt vmpolicy vmbwidth [&lt;MAC address&gt;   &lt;UUID&gt;   &lt;name&gt;     &lt;IP address&gt;   &lt;index number&gt;]</pre> <p>Deletes the bandwidth management settings from this VM policy.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>show virt vmpolicy vmbandwidth [&lt;MAC address&gt;   &lt;UUID&gt;   &lt;name&gt;     &lt;IP address&gt;   &lt;index number&gt;]</pre> <p>Displays the current VM bandwidth management parameters.</p> <p><b>Command mode:</b> All</p>

## Virtual NIC Configuration

Table 352 describes the Virtual NIC (vNIC) configuration options.

Table 352. Virtual NIC Options

Command Syntax and Usage
<code>vnic enable</code> Globally turns vNIC on. <b>Command mode:</b> Global configuration
<code>no vnic enable</code> Globally turns vNIC off. <b>Command mode:</b> Global configuration
<code>[no] vnic uplink-share</code> Enable or disable vNIC shared mode. When enabled, multiple vNIC groups can be assigned to an uplink port. <b>Command mode:</b> Global configuration
<code>show vnic</code> Displays the current vNIC parameters. <b>Command mode:</b> Global configuration

## vNIC Port Configuration

Table 353 describes the Virtual NIC (vNIC) port configuration options.

Table 353. vNIC Port Configuration Options

Command Syntax and Usage
<code>vnic port &lt;port alias or number&gt; index &lt;1-4&gt;</code> Enters vNIC Configuration mode. <b>Note:</b> This command is valid for internal server ports only. <b>Command mode:</b> Global configuration
<code>bandwidth &lt;1-100&gt;</code> Configures the maximum bandwidth allocated to this vNIC, in increments of 100 Mbps. For example: <ul style="list-style-type: none"><li>– 1 = 100 Mbps</li><li>– 10 = 1000 Mbps</li></ul> <b>Command mode:</b> vNIC configuration

Table 353. vNIC Port Configuration Options

Command Syntax and Usage
<p>enable</p> <p>Enables the vNIC.</p> <p><b>Command mode:</b> vNIC configuration</p>
<p>no enable</p> <p>Disables the vNIC.</p> <p><b>Command mode:</b> vNIC configuration</p>

## Virtual NIC Group Configuration

Table 354 describes the Virtual NIC (vNIC) Group configuration options.

Table 354. vNIC Group Configuration Options

Command Syntax and Usage
<p>vnic vnicgroup &lt;1-32&gt;</p> <p>Enters vNIC Group Configuration mode.</p> <p><b>Command mode:</b> Global Configuration</p>
<p>vlan &lt;VLAN number&gt;</p> <p>Assigns a VLAN to the vNIC Group.</p> <p><b>Command mode:</b> vNIC Group configuration</p>
<p>[no] failover</p> <p>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.</p> <p>The default setting is disabled.</p> <p><b>Command mode:</b> vNIC Group configuration</p>
<p>member &lt;vNIC number&gt;</p> <p>Adds a vNIC to the vNIC Group. The vNIC ID is comprised of the port number and the vNIC number. For example: 1 . 1</p> <p><b>Command mode:</b> vNIC Group configuration</p>
<p>no member &lt;vNIC number&gt;</p> <p>Removes the selected vNIC from the vNIC Group.</p> <p><b>Command mode:</b> vNIC Group configuration</p>
<p>port &lt;port number or alias&gt;</p> <p>Adds the selected switch port to the vNIC Group.</p> <p><b>Command mode:</b> vNIC Group configuration</p>
<p>no port &lt;port number or alias&gt;</p> <p>Removes the selected switch port from the vNIC Group.</p> <p><b>Command mode:</b> vNIC Group configuration</p>

Table 354. vNIC Group Configuration Options (continued)

Command Syntax and Usage	
trunk <trunk number>	Adds the selected trunk group to the vNIC Group. <b>Command mode:</b> vNIC Group configuration
no trunk <trunk number>	Removes the selected trunk group from the vNIC Group. <b>Command mode:</b> vNIC Group configuration
key <trunk number>	Adds the uplink LACP trunk to the vNIC Group. <b>Command mode:</b> vNIC Group configuration
no key <trunk number>	Removes the selected uplink LACP trunk from the vNIC Group. <b>Command mode:</b> vNIC Group configuration
enable	Enables the vNIC Group. <b>Command mode:</b> vNIC Group configuration
no enable	Disables the vNIC Group. <b>Command mode:</b> vNIC Group configuration
no vnic vnicgroup <1-32>	Deletes the selected vNIC Group. <b>Command mode:</b> Global configuration
show vnicgroup	Displays the current vNIC Group parameters. <b>Command mode:</b> All



## VM Group Configuration

[Table 355](#) 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 355. VM Group Configuration Options

Command Syntax and Usage	
<pre>virt vmgroup &lt;I-4096&gt; vlan &lt;VLAN number&gt;</pre>	<p>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.</p> <p><b>Note:</b> If you add a VM profile to this group, the group will use the VLAN assigned to the profile.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>[no] virt vmgroup &lt;I-4096&gt; vmap &lt;VMAP number&gt; serverports non-serverports</pre>	<p>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.</p> <p>For more information about configuring VLAN Maps, see <a href="#">“VMAP Configuration” on page 328</a>.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>[no] virt vmgroup &lt;I-4096&gt; tag</pre>	<p>Enables or disables VLAN tagging on ports in this VM group.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>virt vmgroup &lt;I-4096&gt; vm [&lt;MAC address&gt; &lt;UUID&gt; &lt;name&gt; &lt;IP address&gt;  &lt;index number&gt;]</pre>	<p>Adds a VM to the VM group. Enter a unique identifier to select a VM. The UUID and name parameters apply only if Virtual Center information is configured (<code>virt vmware vcspec</code>). The VM index number is found in the VM information dump (<code>show virt vm</code>).</p> <p><b>Note:</b> If the VM is connected to a port that is contained within the VM group, do not add the VM to the VM group.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>no virt vmgroup &lt;I-4096&gt; vm [&lt;MAC address&gt; &lt;UUID&gt; &lt;name&gt;  &lt;IP address&gt; &lt;index number&gt;]</pre>	<p>Removes a VM from the VM group. Enter a unique identifier to select a VM. The UUID and name parameters apply only if Virtual Center information is configured (<code>virt vmware vcspec</code>). The VM index number is found in the VM information dump (<code>show virt vm</code>).</p> <p><b>Command mode:</b> Global configuration</p>

Table 355. VM Group Configuration Options (continued)

Command Syntax and Usage	
<pre>virt vmgroup &lt;1-4096&gt; profile &lt;profile name (1-39 characters)&gt;</pre>	<p>Adds the selected VM profile to the VM group.</p> <p><b>Note:</b> This command can only be used if the VM group is empty (that is, it only has a profile assigned).</p> <p><b>Command mode:</b> Global configuration</p>
<pre>no virt vmgroup &lt;1-4096&gt; profile</pre>	<p>Removes the VM profile assigned to the VM group.</p> <p><b>Note:</b> This command can only be used if the VM group is empty (only has the profile assigned).</p> <p><b>Command mode:</b> Global configuration</p>
<pre>virt vmgroup &lt;1-4096&gt; port &lt;port alias or number&gt;</pre>	<p>Adds the selected port to the VM group.</p> <p><b>Note:</b> A port can be added to a VM group only if no VMs on that port are members of the VM group.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>no virt vmgroup &lt;1-4096&gt; port &lt;port alias or number&gt;</pre>	<p>Removes the selected port from the VM group.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>virt vmgroup &lt;1-4096&gt; vport &lt;port alias or number&gt;</pre>	<p>Adds the selected virtual port to the VM group.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>no virt vmgroup &lt;1-4096&gt; vport &lt;port alias or number&gt;</pre>	<p>Removes the selected virtual port from the VM group.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>virt vmgroup &lt;1-4096&gt; portchannel &lt;trunk number&gt;</pre>	<p>Adds the selected trunk group to the VM group.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>no virt vmgroup &lt;1-4096&gt; portchannel &lt;trunk number&gt;</pre>	<p>Removes the selected trunk group from the VM group.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>virt vmgroup &lt;1-4096&gt; key &lt;1-65535&gt;</pre>	<p>Adds an LACP <i>admin key</i> to the VM group. LACP trunks formed with this <i>admin key</i> will be included in the VM group.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>no virt vmgroup &lt;1-4096&gt; key &lt;1-65535&gt;</pre>	<p>Removes an LACP <i>admin key</i> from the VM group.</p> <p><b>Command mode:</b> Global configuration</p>

Table 355. VM Group Configuration Options (continued)

Command Syntax and Usage	
<pre>virt vmgroup &lt;I-4096&gt; stg &lt;STG number&gt;</pre>	<p>Assigns the VM group to a Spanning Tree Group (STG).</p> <p><b>Command mode:</b> Global configuration</p>
<pre>virt vmgroup &lt;I-4096&gt; validate [basic advanced]</pre>	<p>Enables MAC address spoof prevention for the specified VM group. Default setting is disabled.</p> <ul style="list-style-type: none"> <li>– <code>basic</code> validation ensures lightweight port-based protection by cross-checking the VM MAC address, switch port and switch ID between the switch and the hypervisor. Applicable for “trusted” hypervisors, which are not susceptible to duplicating or reusing MAC addresses on virtual machines.</li> <li>– <code>advanced</code> validation ensures heavyweight VM-based protection by cross-checking the VM MAC address, VM UUID, switch port and switch ID between the switch and the hypervisor. Applicable for “untrusted” hypervisors, which are susceptible to duplicating or reusing MAC addresses on virtual machines.</li> </ul> <p><b>Command mode:</b> Global configuration</p>
<pre>no virt vmgroup &lt;I-4096&gt; validate</pre>	<p>Disables MAC address spoof prevention for the specified VM group.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>no virt vmgroup &lt;I-4096&gt;</pre>	<p>Deletes the VM group.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>show virt vmgroup &lt;I-4096&gt;</pre>	<p>Displays the current VM group parameters.</p> <p><b>Command mode:</b> All</p>

## VM Check Configuration

[Table 356](#) describes the VM Check validation options used for MAC address spoof prevention.

Table 356. VM Check Configuration Options

Command Syntax and Usage
<pre>virt vmcheck acls max &lt;1-256&gt;</pre> <p>Configures the maximum number of ACLs that can be set up for MAC address spoofing prevention in advanced validation mode. Default value is 50.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>no virt vmcheck acls</pre> <p>Disables ACL-based MAC address spoofing prevention in advanced validation mode.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>virt vmcheck action basic {link log}</pre> <p>Sets up action taken when detecting MAC address spoofing in basic validation mode:</p> <ul style="list-style-type: none"><li>– <code>link</code> registers a syslog entry and disables the corresponding switch port</li><li>– <code>log</code> registers a syslog entry</li></ul> <p>Default setting is <code>link</code>.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>virt vmcheck action advanced {acl link log}</pre> <p>Sets up action taken when detecting MAC address spoofing in advanced validation mode:</p> <ul style="list-style-type: none"><li>– <code>acl</code> registers a syslog entry and installs an ACL to drop traffic incoming on the corresponding switch port originating from the spoofed MAC address</li><li>– <code>link</code> registers a syslog entry and disables the corresponding switch port</li><li>– <code>log</code> registers a syslog entry</li></ul> <p>Default setting is <code>acl</code>.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>[no] virt vmcheck trust &lt;ports&gt;</pre> <p>Enables or disables trusted ports for VM communication. By default, all ports are disabled.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>show virt vmcheck</pre> <p>Displays the current VM Check settings. See <a href="#">page 123</a> for sample output.</p> <p><b>Command mode:</b> Global configuration</p>

## VM Profile Configuration

Table 357 describes the VM Profiles configuration options.

Table 357. VM Profile Configuration Options

Command Syntax and Usage
<pre>virt vmprofile &lt;profile name (1-39 characters)&gt;</pre> <p>Defines a name for the VM profile. The switch supports up to 32 VM profiles.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>no virt vmprofile &lt;profile name (1-39 characters)&gt;</pre> <p>Deletes the selected VM profile.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>virt vmprofile edit &lt;profile name (1-39 characters)&gt; vlan &lt;VLAN number&gt;</pre> <p>Assigns a VLAN to the VM profile.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>[no] virt vmprofile edit &lt;profile name (1-39 characters)&gt; shaping [&lt;average (1-1000000000)&gt; &lt;burst (1-1000000000)&gt; &lt;peak (1-1000000000)&gt;]</pre> <p>Configures traffic shaping parameters implemented in the hypervisor, as follows:</p> <ul style="list-style-type: none"> <li>– Average traffic, in Kilobits per second</li> <li>– Maximum burst size, in Kilobytes</li> <li>– Peak traffic, in Kilobits per second</li> <li>– Delete traffic shaping parameters.</li> </ul> <p><b>Command mode:</b> Global configuration</p>
<pre>[no] virt vmprofile edit &lt;profile name (1-39 characters)&gt; eshaping [&lt;average (1-1000000000)&gt; &lt;burst (1-1000000000)&gt; &lt;peak (1-1000000000)&gt;]</pre> <p>Configures traffic egress shaping parameters implemented in the hypervisor, as follows:</p> <ul style="list-style-type: none"> <li>– Average traffic, in Kilobits per second</li> <li>– Maximum burst size, in Kilobytes</li> <li>– Peak traffic, in Kilobits per second</li> <li>– Delete traffic shaping parameters.</li> </ul> <p><b>Command mode:</b> Global configuration</p>
<pre>show virt vmprofile [&lt;profile name&gt;]</pre> <p>Displays the current VM Profile parameters.</p> <p><b>Command mode:</b> All</p>

## VMWare Configuration

[Table 358](#) describes the VMware configuration options. When you configure 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 358. VM Ware Configuration Options

Command Syntax and Usage	
<pre>virt vmware hbport &lt;1-65535&gt;</pre>	<p>Configures the UDP port number used for heartbeat communication from the VM host to the Virtual Center. The default value is port 902.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>[no] virt vmware vcspec [&lt;IP address&gt;   [&lt;username&gt; noauth]</pre>	<p>Defines the Virtual Center credentials on the switch. Once you configure the Virtual Center, VM Agent functionality is enabled across the system.</p> <p>You are prompted for the following information:</p> <ul style="list-style-type: none"> <li>– IP address of the Virtual Center</li> <li>– User name and password for the Virtual Center</li> <li>– Whether to authenticate the SSL security certificate (yes or no)</li> </ul> <p><b>Command mode:</b> Global configuration</p>
<pre>virt vmware hello [enable haddr &lt;IP_address&gt; hport &lt;port_no&gt; htimer &lt;1-60&gt;]</pre>	<p>Configures CDP (Cisco Discovery Protocol) advertisements sent periodically to VMware ESX hypervisors. Exchanging CDP message with ESX hypervisors facilitates MAC address spoof prevention. Default setting is disabled.</p> <ul style="list-style-type: none"> <li>– <code>enable</code> enables CDP advertisements transmission.</li> <li>– <code>haddr</code> advertises a specific IP address instead of the default 0.0.0.0 IP.</li> <li>– <code>hport</code> enables ports on which CDP advertisements are sent.</li> <li>– <code>htimer</code> sets the number of seconds between successive CDP advertisements. Default value is 30.</li> </ul> <p><b>Command mode:</b> Global configuration</p>
<pre>no virt vmware hello [enable hport &lt;port_no&gt;]</pre>	<p>Disables CDP advertisement transmissions completely or only on specific ports.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>show virt vmware</pre>	<p>Displays the current VMware parameters.</p> <p><b>Command mode:</b> All</p>

## Miscellaneous VMready Configuration

You can pre-configure MAC addresses as VM Organization Unique Identifiers (OUIs). These configuration commands are only available using the IBM N/OS CLI and the Miscellaneous VMready Configuration Menu. [Table 358](#) describes the VMready configuration options.

Table 359. VMready Configuration Options

Command Syntax and Usage
<pre>virt vmrmisc oui &lt;3 byte VM MAC OUI&gt; &lt;Vendor Name&gt;</pre> <p>Adds a MAC OUI.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>no virt vmrmisc oui &lt;3 byte VM MAC OUI&gt;</pre> <p>Removes a MAC OUI.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>show virt oui</pre> <p>Displays all the configured MAC OUIs.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>virt vmrmisc lmac</pre> <p>Enables the switch to treat locally administered MAC addresses as VMs.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>no virt vmrmisc lmac</pre> <p>Disables the switch from treating locally administered MAC addresses as VMs.</p> <p><b>Command mode:</b> Global configuration</p>

## Edge Virtual Bridge VSI Type Database Configuration

You can configure your switch to use Edge Virtual Bridging (EVB). [Table 360](#) describes the EVB VSI Type Database configuration options.

Table 360. Edge Virtual Bridge Configuration Options

Command Syntax and Usage	
<pre>virt evb vsidb &lt;VSIDB_number&gt;</pre>	<p>Enter Virtual Station Interface Database configuration mode.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>virt evb update vsidb &lt;VSIDB_number&gt;</pre>	<p>Update VSI types from the VSI database.</p> <p><b>Command mode:</b> All</p>
<pre>clear virt evb vsidb</pre>	<p>Clears local VSI types cache.</p> <p><b>Command mode:</b> All</p>
<pre>clear virt evb vsi</pre>	<p>Clears VSI database associations.</p> <p><b>Command mode:</b> All</p>
<pre>host &lt;IP address&gt; [mgt-port data-port]</pre>	<p>Sets the Virtual Station Interface Type database manager IP address and the port used for the connection. By default, the management port is used.</p> <p><b>Command mode:</b> VSI Database</p>
<pre>port &lt;1-65534&gt;</pre>	<p>Sets the Virtual Station Interface Type database manager port.</p> <p><b>Command mode:</b> VSI Database</p>
<pre>filename &lt;file name&gt;</pre>	<p>Sets the Virtual Station Interface Type database document name.</p> <p><b>Command mode:</b> VSI Database</p>
<pre>filepath &lt;file path&gt;</pre>	<p>Sets the Virtual Station Interface Type database document path.</p> <p><b>Command mode:</b> VSI Database</p>
<pre>protocol {http   https}</pre>	<p>Sets the Virtual Station Interface Type database transport protocol. The default setting is HTTP.</p> <p><b>Command mode:</b> VSI Database</p>
<pre>update-interval &lt;5-300&gt;</pre>	<p>Sets the Virtual Station Interface Type database update interval in seconds. A value of "0" disables periodic updates.</p> <p><b>Command mode:</b> VSI Database</p>



Table 360. Edge Virtual Bridge Configuration Options (continued)

Command Syntax and Usage
<pre>show virt evb vsitypes [mgrid &lt;0-255&gt;   typeid &lt;1-16777215&gt;   version &lt;0-255&gt;]</pre> <p>Displays the current Virtual Station Interface Type database parameters.</p> <p><b>Command mode:</b> All</p>
<pre>show virt evb vsidb &lt;VSIDB_number&gt;</pre> <p>Displays the current Virtual Station Interface database information.</p> <p><b>Command mode:</b> All</p>
<pre>no virt evb vsidb &lt;VSIDB_number&gt;</pre> <p>Resets the Virtual Station Interface Type database information to the default values.</p> <p><b>Command mode:</b> Global configuration</p>

## Edge Virtual Bridge VSI Type Profile Configuration

Table 361 describes the Virtual Station Interface Type profile configuration options.

Table 361. Edge Virtual Bridge VSI Type Profile Configuration Options

Command Syntax and Usage
<pre>virt evb profile &lt;profile_number&gt;</pre> <p>Enter Virtual Station Interface type profile configuration mode.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>[no] reflective-relay</pre> <p>Enables or disables VEPA mode (Reflective Relay capability).</p> <p><b>Command mode:</b> EVB Profile</p>
<pre>[no] vsi-discovery</pre> <p>Enables or disables VSI Discovery (ECP and VDP).</p> <p><b>Command mode:</b> EVB Profile</p>
<pre>no virt evb profile &lt;profile_number&gt;</pre> <p>Deletes the specified EVB profile.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>show virt evb profile [&lt;1-16&gt;]</pre> <p>Displays the current EVB profile parameters.</p> <p><b>Command mode:</b> All</p>

Table 361. Edge Virtual Bridge VSI Type Profile Configuration Options

<b>Command Syntax and Usage</b>
<pre>evb profile &lt;1-16&gt;</pre> <p>Applies the specified EVB profile for the port. Automatically enables LLDP, EVB, and TLV on the corresponding port.</p> <p><b>Command mode:</b> Interface port</p>
<pre>no evb profile</pre> <p>Resets EVB profile for the port. Automatically disables LLDP, EVB, and TLV on the corresponding port.</p> <p><b>Command mode:</b> Interface port</p>

---

## OpenFlow Configuration

OpenFlow is an open interface used to control the forwarding plane in compatible switches and routers remotely, from an external controller. The RackSwitch G8264 can function as either a Hybrid or OpenFlow-only switch:

- In Hybrid mode (default), an OpenFlow pipeline can be set up to run in parallel to the normal Ethernet switching pipeline. The two pipelines are completely separate, each with its own dedicated ports and confined packet flows.
- In OpenFlow-only mode, the normal Ethernet switching capabilities are disabled, and the RackSwitch G8264 behaves as a pure OpenFlow switch.

Table 362 describes the OpenFlow configuration options.

Table 362. OpenFlow Configuration Options

Command Syntax and Usage
<pre>boot profile openflow</pre> <p>Starts the switch in OpenFlow-only mode on reboot.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>boot profile default</pre> <p>Starts the switch in Hybrid mode on reboot. This is the default setting.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>boot openflow {v1 v13}</pre> <p>Switches between OpenFlow version 1.0 and OpenFlow version 1.3 on reboot. The default setting is v1.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>[no] openflow enable</pre> <p>Enables or disables OpenFlow.</p> <p><b>Note:</b> The following features are not supported when OpenFlow is enabled: ACL, VNIC egress, VMready VMAP, FCOE, IPv6, IPMC, ECN, PVID and MACL.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>[no] openflow edgeport &lt;port_numbers&gt;</pre> <p>Enables or disables the selected port as an OpenFlow edge port (outside port). Edge ports are usually connected to servers. The default setting is disabled.</p> <p><b>Note:</b> Learning is turned on and flood blocking is turned on in OpenFlow edge ports.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>openflow fdb-priority &lt;1-65535&gt;</pre> <p>Configures a priority value to map flows with matching priority to FDB entries, if the flow uses destination MAC address and VLAN as the matching qualifier and single port as the action. The default value is 1000.</p> <p><b>Note:</b> When you issue this command, all registered flow entries are cleared.</p> <p><b>Command mode:</b> Global configuration</p>

Table 362. OpenFlow Configuration Options (continued)

Command Syntax and Usage	
no openflow fdb-priority	Resets priority value required for FDB flows to the default value of 1000. <b>Command mode:</b> Global configuration
openflow fdb-timeout <I-300>	Configures a time interval in seconds for periodically clearing dynamically learned FDB entries on edge ports. Default value is disabled. <b>Command mode:</b> Global configuration
no openflow fdb-timeout	Disables periodical clearing of dynamically learned FDB entries on edge ports. <b>Command mode:</b> Global configuration
[no] openflow fdb-aging	Enables or disables periodical clearing of dynamically learned FDB entries on a specific port. Default value is disabled on OpenFlow edge ports. <b>Command mode:</b> Interface port
openflow mpls-priority <I-65535>	Configures a priority value to map flows with matching priority to MPLS entries. The default value is 65535. <b>Note:</b> Supported only in OpenFlow 1.3. <b>Note:</b> When you issue this command, all the existing MPLS flows are cleared automatically. <b>Command mode:</b> Global configuration
no openflow mpls-priority	Resets the priority value required for MPLS flows to the default value of 65535. <b>Note:</b> Supported only in OpenFlow 1.3. <b>Command mode:</b> Global configuration
[no] openflow static-station-move	Enables or disables forwarding frames that have source MAC addresses conflicting with entries in the static FDB table. This enables equal cost multi-path routing and use cases where IPS and Firewall devices forward packets without changing the source MAC address. Default value is disabled. <b>Command mode:</b> Interface port
openflow instance <I-2>	Enters OpenFlow Instance command mode for the specified instance ID. <b>Command mode:</b> Global configuration, OpenFlow Instance
no openflow instance <I-2>	Deletes the instance and clears flow table and statistics for the specified instance ID. <b>Command mode:</b> Global configuration, OpenFlow Instance

Table 362. OpenFlow Configuration Options (continued)

Command Syntax and Usage
<p>[no] openflow mgmtport &lt;ports&gt;</p> <p>Enables or disables OpenFlow management for the selected port. Use OpenFlow management ports to communicate with an OpenFlow Controller. In Hybrid mode, controllers can also connect to the switch using legacy ports. The default setting is disabled.</p> <p><b>Command mode:</b> Global configuration</p>
<p>show openflow [flow-allocation   information   statistics   table]</p> <p>Displays the current OpenFlow configuration. For more information, see <a href="#">page 107</a>.</p> <ul style="list-style-type: none"> <li>– flow-allocation displays the configured, current and maximum number of flows for each OpenFlow instance. For more information, see <a href="#">page 108</a>.</li> <li>– information displays the configuration for each OpenFlow instance. For more information, see <a href="#">page 110</a>.</li> <li>– statistics displays traffic statistics for each OpenFlow instance. For more information see <a href="#">page 208</a>.</li> <li>– table displays the basic and emergency flow tables for each OpenFlow instance in OpenFlow 1.0. In OpenFlow 1.3, displays the dynamic and static flow tables. For more information, see <a href="#">page 112</a></li> </ul> <p><b>Command mode:</b> All</p>
<p>show openflow instance &lt;1-2&gt; [information   statistics   table]</p> <p>Displays OpenFlow information for the specified instance ID:</p> <ul style="list-style-type: none"> <li>– information displays the instance configuration</li> <li>– statistics displays traffic statistics</li> <li>– table displays the basic and emergency flow tables in OpenFlow 1.0. In OpenFlow 1.3, displays the dynamic and static flow tables.</li> </ul> <p><b>Command mode:</b> All</p>
<p>clear openflow {statistics   table [basic   emergency   dynamic]}</p> <p>Clears OpenFlow data for all instances:</p> <ul style="list-style-type: none"> <li>– The statistics option clears traffic statistics.</li> <li>– The table option clears all basic and emergency OpenFlow tables in OpenFlow 1.0. In OpenFlow 1.3, clears the dynamic and static flow tables. <ul style="list-style-type: none"> <li>• The basic option clears only the basic OpenFlow tables.</li> <li>• The emergency option clears only the emergency OpenFlow tables.</li> <li>• The dynamic option clears only the emergency OpenFlow tables.</li> </ul> </li> </ul> <p><b>Command mode:</b> Privileged EXEC</p>

Table 362. OpenFlow Configuration Options (continued)

Command Syntax and Usage	
<pre>clear openflow instance &lt;I-2&gt; {statistics   table [basic   emergency   dynamic]}</pre>	<p>Clears OpenFlow data for the specified instance ID:</p> <ul style="list-style-type: none"> <li>– The <code>statistics</code> option clears traffic statistics.</li> <li>– The <code>table</code> option clears all basic and emergency OpenFlow tables in OpenFlow 1.0. In OpenFlow 1.3, clears the dynamic and static flow tables. <ul style="list-style-type: none"> <li>• The <code>basic</code> option clears only the basic OpenFlow table.</li> <li>• The <code>emergency</code> option clears only the emergency OpenFlow table.</li> </ul> </li> </ul> <p>The <code>dynamic</code> option clears only the emergency OpenFlow tables.</p> <p><b>Command mode:</b> Privileged EXEC</p>
<pre>[no] buffer</pre>	<p>Enables or disables buffering support for OpenFlow packets. The default setting is disabled.</p> <p><b>Command mode:</b> OpenFlow Instance</p>
<pre>connect-retry &lt;I-8&gt;</pre>	<p>Configures the maximum number of attempts to establish connection to a controller, before assuming the controller is down. The default value is 4.</p> <p><b>Command mode:</b> OpenFlow Instance</p>
<pre>no connect-retry</pre>	<p>Resets the <code>connect-retry</code> value to 4.</p> <p><b>Command mode:</b> OpenFlow Instance</p>
<pre>controller &lt;I-4&gt; address &lt;ip_address&gt; [data-port   mgt-port]</pre>	<p>Configures the IP address of the OpenFlow Controller. You may specify the port to use for data transfer: data port (<code>data-port</code>) or management port (<code>mgt-port</code>). By default, the system uses the management port.</p> <p><b>Command mode:</b> OpenFlow Instance</p>
<pre>controller &lt;I-4&gt; port &lt;TCP port number (1-65535)&gt;</pre>	<p>Configures the TCP port used for communication with the Controller. The default port is 6633.</p> <p><b>Command mode:</b> OpenFlow Instance</p>
<pre>no controller &lt;I-4&gt;</pre>	<p>Deletes the selected controller from the specified instance ID.</p> <p><b>Command mode:</b> OpenFlow Instance</p>
<pre>dpid &lt;hex string&gt;</pre>	<p>Applies an 8 byte Datapath ID to the instance, which enables equal cost multi-path routing in an OpenFlow environment. The default value is the instance ID followed by the switch MAC.</p> <p><b>Command mode:</b> OpenFlow Instance</p>

Table 362. OpenFlow Configuration Options (continued)

Command Syntax and Usage	
no dpid	<p>Resets the instance's Datapath ID to the default value (instance ID followed by the switch MAC).</p> <p><b>Command mode:</b> OpenFlow Instance</p>
echo-reply-timeout <2-65535>	<p>Configures the duration in seconds the switch will wait to receive an echo reply from the controller, before assuming failure. The default value is 15.</p> <p><b>Note:</b> The <code>echo-reply-timeout</code> value must be lower than the <code>echo-request-interval</code> value.</p> <p><b>Command mode:</b> OpenFlow Instance</p>
no echo-reply-timeout	<p>Resets the <code>echo-reply-timeout</code> to the default value of 15.</p> <p><b>Command mode:</b> OpenFlow Instance</p>
echo-request-interval <5-65535>	<p>Configures the maximum duration in seconds the switch will keep sending echo requests to a non-responsive controller. The default value is 30.</p> <p><b>Note:</b> The <code>echo-request-interval</code> value must be higher than the <code>echo-reply-timeout</code> value.</p> <p><b>Command mode:</b> OpenFlow Instance</p>
no echo-request-interval	<p>Resets the <code>echo-request-interval</code> value to the default value of 30.</p> <p><b>Command mode:</b> OpenFlow Instance</p>
emergency [timeout <0-3600>]	<p>Forces the instance in emergency mode.</p> <p>The <code>timeout</code> parameter configures the duration in seconds after which the emergency mode expires. The default value is 30.</p> <p><b>Note:</b> Supported only in OpenFlow 1.0.</p> <p><b>Command mode:</b> OpenFlow Instance</p>
no emergency [timeout]	<p>Brings the instance out of emergency mode.</p> <p>The <code>timeout</code> parameter resets the emergency mode duration to the default value of 30.</p> <p><b>Note:</b> Supported only in OpenFlow 1.0.</p> <p><b>Command mode:</b> OpenFlow Instance</p>
[no] enable	<p>Enables or disables the instance. When disabling an instance, its flow tables and statistics are cleared.</p> <p><b>Command mode:</b> OpenFlow Instance</p>

Table 362. OpenFlow Configuration Options (continued)

Command Syntax and Usage	
<code>max-flow-acl &lt;0-750/1000&gt;</code>	<p>Enables or disables the maximum flow ACL option, which ensures a dedicated maximum number of ACL flows are available for the instance. The maximum number of entries is 750 in Hybrid mode and 1000 in OpenFlow Only mode. The total number of 750/1000 entries is shared between instances. By default, <code>max-flow-acl</code> is set to 0, allowing instances to dynamically access the available ACL flow slots until depletion. Setting <code>max-flow-acl</code> manually limits the number of ACL flow slots available for other instances by the corresponding value.</p> <p><b>Command mode:</b> OpenFlow Instance</p>
<code>max-flow-mcast-fdb &lt;0-4096&gt;</code>	<p>Enables or disables the maximum flow multicast FDB option, which ensures a dedicated maximum number of FDB multicast flows are available for the instance. The total number of entries is shared between instances. By default, <code>max-flow-mcast-fdb</code> is set to 0, allowing instances to dynamically access the available FDB multicast flow slots until depletion. Setting <code>max-flow-mcast-fdb</code> manually limits the number of FDB multicast flow slots available for other instances by the corresponding value.</p> <p><b>Command mode:</b> OpenFlow Instance</p>
<code>max-flow-mpls-pop &lt;0-1000&gt;</code>	<p>Enables or disables the maximum flow MPLS pop option, which ensures a dedicated maximum number of MPLS label pop flows are available for the instance. The total number of 1000 entries is shared between instances. By default, <code>max-flow-mpls-pop</code> is set to 0, allowing instances to dynamically access the available MPLS label pop flow slots until depletion. Setting <code>max-flow-mpls-pop</code> manually limits the number of MPLS label pop flow slots available for other instances by the corresponding value.</p> <p><b>Note:</b> Supported only in OpenFlow 1.3.</p> <p><b>Command mode:</b> OpenFlow Instance</p>
<code>max-flow-mpls-push &lt;0-1000&gt;</code>	<p>Enables or disables the maximum flow MPLS push option, which ensures a dedicated maximum number of MPLS label push flows are available for the instance. The total number of 1000 entries is shared between instances. By default, <code>max-flow-mpls-push</code> is set to 0, allowing instances to dynamically access the available MPLS label push flow slots until depletion. Setting <code>max-flow-mpls-push</code> manually limits the number of MPLS label push flow slots available for other instances by the corresponding value.</p> <p><b>Note:</b> Supported only in OpenFlow 1.3.</p> <p><b>Command mode:</b> OpenFlow Instance</p>



Table 362. OpenFlow Configuration Options (continued)

Command Syntax and Usage	
max-flow-ucast-fdb <0-123904>	<p>Enables or disables the maximum flow unicast FDB option, which ensures a dedicated maximum number of FDB unicast flows available for the instance. The total number of entries is shared between instances. By default, max-flow-ucast-fdb is set to 0, allowing instances to dynamically access the available FDB unicast flow slots until depletion. Setting max-flow-ucast-fdb manually limits the number of FDB unicast flow slots available for other instances by the corresponding value.</p> <p><b>Command mode:</b> OpenFlow Instance</p>
no max-flow-acl	<p>Sets the instance's maximum number of ACL based flows to the default value of 0 (dynamic allocation).</p> <p><b>Command mode:</b> OpenFlow Instance</p>
no max-flow-mcast-fdb	<p>Sets the instance's maximum number of FDB based multicast flows to the default value of 0 (dynamic allocation).</p> <p><b>Command mode:</b> OpenFlow Instance</p>
no max-flow-ucast-fdb	<p>Sets the instance's maximum number of FDB based unicast flows to the default value of 0 (dynamic allocation).</p> <p><b>Command mode:</b> OpenFlow Instance</p>
no max-flow-mps-pop	<p>Sets the instance's maximum number of MPLS label pop flows to the default value of 0 (dynamic allocation).</p> <p><b>Note:</b> Supported only in OpenFlow 1.3.</p> <p><b>Command mode:</b> OpenFlow Instance</p>
no max-flow-mps-push	<p>Sets the instance's maximum number of MPLS label push flows to the default value of 0 (dynamic allocation).</p> <p><b>Note:</b> Supported only in OpenFlow 1.3.</p> <p><b>Command mode:</b> OpenFlow Instance</p>
[no] member {<ports>   portchannel <1-64>}	<p>Enables or disables port or static portchannel usage by the OpenFlow instance for data traffic.</p> <p><b>Note:</b> Static portchannels are supported only in OpenFlow 1.3.</p> <p><b>Command mode:</b> OpenFlow Instance</p>

Table 362. OpenFlow Configuration Options (continued)

Command Syntax and Usage	
<code>min-flow-timeout &lt;0-300&gt;</code>	<p>Sets the minimum number of seconds after which a flow can be cleared from the instance's tables. Default value is 0, meaning controller provided values are used instead.</p> <p><b>Command mode:</b> OpenFlow Instance</p>
<code>no min-flow-timeout</code>	<p>Sets the number of seconds after which a flow can be cleared from the instance's tables to the default value of 0 (controller provided values).</p> <p><b>Command mode:</b> OpenFlow Instance</p>
<code>[no] table-miss controller</code>	<p>Sets or disables the <code>table-miss</code> flow entry to send packets unmatched by any flow entries to the controller. Default value is disabled, meaning packets unmatched by flow entries are dropped.</p> <p><b>Note:</b> Supported only in OpenFlow 1.3.</p> <p><b>Command mode:</b> OpenFlow Instance</p>
<code>table-miss cookie &lt;0x0-0xffffffff&gt;</code>	<p>Sets the flow cookie for packets sent to controller as a result of a table-miss setting (send input packets that don't match any flow entries to controller). The default value is 0xffffffff.</p> <p><b>Note:</b> Supported only in OpenFlow 1.3.</p> <p><b>Command mode:</b> OpenFlow Instance</p>
<code>no table-miss cookie</code>	<p>Resets the table-miss flow cookie to the default value of 0xffffffff.</p> <p><b>Note:</b> Supported only in OpenFlow 1.3.</p> <p><b>Command mode:</b> OpenFlow Instance</p>
<code>mirror-to-controller cookie &lt;0x0-0xffffffff&gt;</code>	<p>Sets the flow cookie for packets sent to controller as a result of a mirror-to-controller setting (flow is set to output the packet to a controller in addition to another destination). The default value is 0xffffffff.</p> <p><b>Note:</b> Supported only in OpenFlow 1.3.</p> <p><b>Command mode:</b> OpenFlow Instance</p>
<code>no mirror-to-controller cookie</code>	<p>Resets the mirror-to-controller flow cookie to the default value of 0xffffffff.</p> <p><b>Note:</b> Supported only in OpenFlow 1.3.</p> <p><b>Command mode:</b> OpenFlow Instance</p>

Table 362. OpenFlow Configuration Options (continued)

Command Syntax and Usage	
<pre>send-to-controller cookie &lt;0x0-0xffffffff&gt;</pre>	<p>Sets the flow cookie for packets sent to controller as a result of a send-to-controller setting (flow is set to output the packet only to a controller). The default value is 0xffffffff.</p> <p><b>Note:</b> Supported only in OpenFlow 1.3.</p> <p><b>Command mode:</b> OpenFlow Instance</p>
<pre>no send-to-controller cookie</pre>	<p>Resets the send-to-controller flow cookie to the default value of 0xffffffff.</p> <p><b>Note:</b> Supported only in OpenFlow 1.3.</p> <p><b>Command mode:</b> OpenFlow Instance</p>

## Static Flows Configuration

Static flows are ACL OpenFlow entries set up manually from the CLI by the administrator. Static flows cannot be deleted/modified by OpenFlow controllers and will continue to function when the switch goes into emergency mode. Even if they

qualify as FDB entries based on their settings, in version 1.0 of the OpenFlow standard, static flows are always stored as ACL entries. A total of maximum 750 static flows pool is shared between all OpenFlow instances.

Table 363 describes the static flow configuration options.

Table 363. Static Flows Configuration Options

Command Syntax and Usage
<pre>static-table add index &lt;I-750&gt; match WORD actions WORD [options WORD] priority &lt;0-65535&gt;</pre> <p>Adds a static flow entry to the instance. <b>Command mode:</b> OpenFlow Instance</p>
<pre>static-table modify index &lt;I-750&gt; match WORD actions WORD [options WORD] priority &lt;0-65535&gt;</pre> <p>Overwrites a static flow entry. <b>Command mode:</b> OpenFlow Instance</p>
<pre>static-table remove index &lt;I-750&gt;</pre> <p>Deletes a static flow entry. <b>Command mode:</b> OpenFlow Instance</p>
<pre>clear openflow table static</pre> <p>Deletes all static flow entries. <b>Command mode:</b> Global configuration</p>

The following table describes the available matching qualifiers

Table 364. Static Flow Matching Qualifiers in OpenFlow 1.0

Qualifier	Value
ingress-port	Port of instance
src-mac	Source MAC address
dst-mac	Destination MAC address
vlan-id	VLAN identifier (0-4095 + 65535 (untagged))
vlan-priority	802.1p Priority Code Point (0-7)
src-ip	Source IP address
dst-ip	Destination IP address
src-port	L4 source port (0-65536)
dst-port	L4 destination port (0-65535)
ether-type	"arp"/"0806" or "ip"/"0800" or (hex-value <= 65535)
protocol	"tcp" or "udp" or 0-255
tos	IP Type of Service (0-255)

Table 364. Static Flow Matching Qualifiers in OpenFlow 1.0 (continued)

Qualifier	Value
type	"request" or "reply" (can be set only if ether type is ARP)
all	Applicable to all traffic

OpenFlow 1.3:

Qualifier	Value
in-port	switch input port
in-portchannel	switch input portchannel
in-phy-port	switch physical input port, valid only when in-port is pecified
eth-src	source MAC address and mask
eth-dst	destination MAC address and mask
vlan-vid	VLAN identifier (0-4095 + 65535 (untagged))
vlan-pcp	802.1p(0-7)
ipv4-src	source IPv4 address and mask
ipv4-dst	destination IPv4 address and mask
tcp-src	TCP source port (0-65535)
tcp-dst	TCP destination port (0-65535)
udp-src	UDP source port (0-65535)
udp-dst	UDP destination port (0-65535)
icmpv4-type	ICMPv4 type
icmpv4-code	ICMPv4 code
eth-type	"arp"/"0806" or "ip"/"0800" or (hex-value < =65535)
ip-proto	"tcp" or "udp" or 0-255
ip-dscp	IP DSCP (6 bits in ToS field)
arp-op	"request" or "reply" (can be set only if eth-type is ARP)
mpls-label	MPLS label
all	all qualifiers or any qualifier

The following table describes the available actions

Table 365. Static Flow Actions in OpenFlow 1.0

Action	Value
out-put	"all", "in-port", "flood", "controller" or a valid port
set-src-mac	Change source MAC address
set-dst-mac	Change destination MAC address
strip-vlan-id	Remove VLAN identifier
set-vlan-priority	Set 802.1p priority code point value (0-7)
set-nw-tos	Set IP Type of Service (0-255)
drop	Drop packet
max-len	Maximum length to send to controller

Table 366. Static Flow Actions in OpenFlow 1.3

Action	Value
out-put	"all", "in-port", "flood", "controller" or a valid port
output-portchannel	output on a valid portchannel
set-eth-src	change source MAC address
set-eth-dst	change destination MAC address
push-vlan	push a new VLAN tag
pop-vlan	pop the outer VLAN tag
push-mpls	push a new MPLS tag
pop-mpls	pop the MPLS tag
set-vlan-vid	set VLAN ID
set-vlan-pcp	set 802.1p priority (0-7)
set-ip-dscp	set IP Differentiated Services Code Point (0-63)
set-mpls-label	set MPLS label <1-0xFFFFF)
set-mpls-ttl	set MPLS time-to-live
copy-ttl-out	copy time-to-live outward - from next-to-outermost to outermost
copy-ttl-in	copy time-to-live inward - from outermost to next-to-outermost
drop	drop the packet

---

## Precision Time Protocol Configuration

Precision Time Protocol (PTP) allows high accuracy clock synchronization between a networked master clock and compliant network hosts. The RackSwitch G8264 supports two PTP modes:

- Ordinary slave clock - Synchronizes the Real Time Clock (RTC) with PTP master clocks detected on the network.
- End-to-End transparent clock - Allows PTP traffic to pass through without affecting the RTC, while updating the correction fields for event packets.

Table 367. Precision Time Protocol Configuration Options

Command Syntax and Usage	
<code>[no] ptp ordinary enable</code>	<p>Enables or disables PTP ordinary slave clock mode. In this mode, if a PTP master clock is detected on the network, the RTC is synchronized with it. If no master clock is detected, the RTC is not affected. Default setting is disabled.</p> <p><b>Note:</b> Enabling PTP ordinary slave clock mode disables NTP settings and system time clock manual settings.</p> <p><b>Command mode:</b> Global configuration</p>
<code>[no] ptp transparent enable</code>	<p>Enables or disables PTP End-to-End transparent clock mode. In this mode, incoming PTP packets are forwarded based on routing rules currently in place for the PTP domain's multicast address (within the 224.0.1.129 - 224.0.1.132 range). On egress, PTP packet timestamps are updated based on the time spent between ingress and egress. Default setting is disabled.</p> <p><b>Command mode:</b> Global configuration</p>
<code>no ptp</code>	<p>Disables both PTP ordinary slave clock mode and PTP End-to-End transparent clock mode.</p> <p><b>Command mode:</b> Global configuration</p>
<code>ip ptp source-interface loopback &lt;1-5&gt;</code>	<p>Loopback interface used as source IP address for delay-request packets sent during synchronization with the master clock in ordinary slave mode. By default, the interface with the lowest index from the master clock's VLAN is used.</p> <p><b>Command mode:</b> Global configuration</p>
<code>no ip ptp source-interface loopback</code>	<p>Sets source IP address for delay-request packets sent during synchronization with the master clock in ordinary slave mode to the interface with the lowest index from the master clock's VLAN.</p> <p><b>Command mode:</b> Global configuration</p>

Table 367. Precision Time Protocol Configuration Options (continued)

Command Syntax and Usage
<pre>[no] ptp</pre> <p>Enables or disables PTP on the current port. Disabled ports will not support PTP even if PTP is globally enabled. Default setting is enabled.</p> <p><b>Note:</b> PTP is not supported on management ports.</p> <p><b>Command mode:</b> Interface port</p>
<pre>show ptp [counters]</pre> <p>Displays current PTP settings.</p> <p>The <code>counters</code> option displays PTP packet counters. See <a href="#">page 244</a> for details.</p> <p><b>Command mode:</b> All</p>
<pre>show interface port &lt;port alias or number&gt; ptp-counters</pre> <p>Displays Precision Time Protocol statistics for the port. See <a href="#">page 244</a> for details.</p> <p><b>Command mode:</b> All</p>
<pre>clear ptp counters</pre> <p>Resets PTP packet counters.</p> <p><b>Command mode:</b> Privileged EXEC</p>



---

## Microburst Detection

Microbursts are short peaks in data traffic that manifest as a sudden increase in the number of data packets transmitted over a specific millisecond-level time frame, potentially overwhelming network buffers. Microburst detection allows users to analyze and mitigate microburst-related incidents, thus preventing network congestion.

Table 368. Microburst Detection Configuration Options

Command Syntax and Usage	
<code>[no] microburst enable</code>	Enables or disables microburst detection. Default setting is disabled. <b>Command mode:</b> Global configuration
<code>microburst interval &lt;2-10000&gt;</code>	Configures microburst detection interval granularity in milliseconds. Default setting is 5. <b>Command mode:</b> Global configuration
<code>microburst port-threshold &lt;port no.&gt; &lt;1-42650&gt;</code>	Configures the number of memory cells a port is allowed to access from the shared service pool. Each port is allocated a dedicated number of 45 memory cells. If this threshold is reached, it means the port is congested and needs to access additional memory from the shared service pool. Default value is 36403. <b>Command mode:</b> Global configuration
<code>show microburst microburst-status</code>	Displays microburst state and, if applicable, bursting time for each port. <b>Command mode:</b> All
<code>show microburst pkt-stats</code>	Displays memory cell usage for egress unicast and multicast packets, broken down by port and QoS queue. <b>Command mode:</b> All
<code>show microburst port-log</code>	Displays memory cell allocation and usage for ingress packets on each port. <b>Command mode:</b> All
<code>clear microburst counters</code>	Resets microburst packet counters. <b>Command mode:</b> Privileged EXEC

---

## 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 516](#).

---

## 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|sftp} running-config` command is used, the active configuration will be replaced with the commands found in the specified configuration file. The file can contain a full switch configuration or a partial switch configuration.

To start the switch configuration download, at the prompt, enter:

```
Router(config)# copy ftp running-config  
or  
Router(config)# copy tftp running-config  
or  
Router(config)# copy sftp 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 542](#)).

### 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.

---

## Python Scripting Configuration

Python Scripting allows the user to create his own running programs on the switch. These scripts allow the switch to perform the following:

- monitoring tasks
- automatically provision itself
- automatically upgrade switch firmware/generate configuration files

**Note:** Python Scripting feature is not available in stacking mode.

The following sections describe the Python Scripting configuration options.

- [“Python Scripts Management and Execution” on page 518](#)
- [“Scheduler Jobs Management” on page 520](#)
- [“Running Job Monitor” on page 523](#)
- [“Python Script Editing” on page 528](#)

## Python Scripts Management and Execution

The user can perform various script management actions: edit or delete a script, display script content.

In addition, the switch administrator may access Python shell and directly run a script.

[Table 347](#) describes the Python Scripts Management and Execution commands.

Table 369. Python Scripts Management and Execution Commands

Command Syntax and Usage
<pre>copy tftp script address &lt;IPv4 address&gt; filename &lt;script filename&gt; [data-port   mgt-port]</pre> <p>Gets a script from a TFTP server. <b>Command mode:</b> Privileged EXEC</p>
<pre>copy script tftp address &lt;IPv4 address&gt; filename &lt;script filename&gt; [data-port   mgt-port]</pre> <p>Creates a copy of the script-log on a TFTP server. <b>Command mode:</b> Privileged EXEC</p>
<pre>no script &lt;script filename&gt;</pre> <p>Deletes a script from the system. <b>Note:</b> If the script is specified as action of a scheduled job, the corresponding scheduled job must be deleted first. <b>Command mode:</b> Privileged EXEC</p>
<pre>show script</pre> <p>Displays a list of all installed scripts. <b>Command mode:</b> All</p>

Table 369. Python Scripts Management and Execution Commands

Command Syntax and Usage	
show script <script filename>	<p>Displays the content of a specified script.</p> <p><b>Command mode:</b> All</p>
copy script-log tftp address <IPv4 address> filename <script log filename> [data-port   mgt-port]	<p>Creates a copy of the script-log on a TFTP server.</p> <p><b>Command mode:</b> Privileged EXEC</p>
show script-log	<p>Displays a list of all script log files.</p> <p><b>Note:</b> All script-log files are automatically deleted after a reboot of the switch.</p> <p><b>Command mode:</b> All</p>
show script-log <script-log filename>	<p>Displays the content of a specified script-log.</p> <p><b>Command mode:</b> All</p>
no script-log	<p>Deletes all script execution log files from the system.</p> <p><b>Command mode:</b> Privileged EXEC</p>
no script-log <script log filename>	<p>Deletes the specified script-log file.</p> <p><b>Command mode:</b> Privileged EXEC</p>
edit script <script filename>	<p>Creates or modifies a script via vi text editor.</p> <p><b>Command mode:</b> Privileged EXEC</p>
python <script filename> [<argument list>]	<p>Executes a python script directly. The optional list of arguments, if present, must be provided as a string enclosed in double quotes and the arguments must be separated by white spaces.</p> <p>The string representing the list of arguments must not exceed 199 characters.</p> <p><b>Command mode:</b> Privileged EXEC</p>
python	<p>Provides access to Python shell.</p> <p><b>Command mode:</b> Privileged EXEC</p>

Table 369. Python Scripts Management and Execution Commands

Command Syntax and Usage
<pre>[no] logging log script</pre> <p>Enables or disables scripting module syslog. The default setting is enabled.  <b>Command mode:</b> Global Configuration</p>
<pre>[no] logging log scheduler</pre> <p>Enables or disables scheduler module syslog. The default setting is enabled.  <b>Command mode:</b> Global Configuration</p>

## Scheduler Jobs Management

The user is allowed to define up to 20 scheduler jobs as a mapping of event and action. When the specified event occurs, the corresponding script is executed.

Table 370. Scheduler Jobs Management Configuration Commands

Command Syntax and Usage
<pre>[no] scheduler job name &lt;job name&gt;</pre> <p>Creates or deletes a scheduler job.  <b>Note:</b> A scheduler job can be created prior to downloading/creating an actual script.  <b>Command mode:</b> Global configuration</p>
<pre>event counter cpu ge &lt;1-99&gt;</pre> <p>Triggers a script execution when CPU usage percentage exceeds an user defined threshold. CPU usage percentage is checked every 60 seconds.  <b>Command mode:</b> Scheduler Job</p>
<pre>event counter interface port &lt;1-64&gt; {in-discard out-discard} ge &lt;1-2147483647&gt; [interval &lt;10-300&gt;]</pre> <p>Triggers a script execution when the number of discarded frames per second on a port is greater than or equal to the set up value. When an interval value is configured, the discarded frames rate is averaged over a configured period of time instead of a fixed interval 60 seconds.  <b>Command mode:</b> Scheduler Job</p>
<pre>event counter interface port &lt;1-64&gt; {in-error out-error} ge &lt;1-2147483647&gt; [interval &lt;10-300&gt;]</pre> <p>Triggers a script execution when the number of errors on a port is greater than or equal to the set up value. When an interval value is configured, the error frames rate is averaged over a configured period of time instead of a fixed interval 60 seconds.  <b>Command mode:</b> Scheduler Job</p>
<pre>event counter memory ge &lt;1-50&gt;</pre> <p>Triggers a script execution when memory usage percentage exceeds an user defined threshold. Memory usage percentage is checked every 60 seconds.  <b>Command mode:</b> Scheduler Job</p>



Table 370. Scheduler Jobs Management Configuration Commands

Command Syntax and Usage
<pre>event syslog &lt;event type&gt;</pre> <p>Configures the syslog event which triggers the scheduled job. The following syslog event types are allowed:</p> <ul style="list-style-type: none"> <li>– <b>DOT1XFAIL</b> (802.1x authentication failure event)</li> <li>– <b>LINKDOWN</b> (port link down event)</li> <li>– <b>LINKUP</b> (port link up event)</li> <li>– <b>LLDPDISCOVER</b> (lldp neighbor add or delete event)</li> </ul> <p><b>Note:</b> When a LLDP trap is detected, the scheduler automatically triggers a job.</p> <ul style="list-style-type: none"> <li>– <b>LOGINFAIL</b> (switch user login fail event)</li> <li>– <b>LOGINSUCC</b> (switch user login success event)</li> <li>– <b>MBURST</b> (microburst)</li> </ul> <p><b>Note:</b> All ports microburst state is checked every 10 seconds. When a port goes into bursting state, the scheduler automatically triggers a job.</p> <ul style="list-style-type: none"> <li>– <b>MGTGWDOWN</b> (mgmt gateway unavailable event)</li> <li>– <b>MGTGWUP</b> (mgmt gateway available event)</li> </ul> <p><b>Command mode:</b> Scheduler Job</p>
<pre>event time absolute &lt;yyyy&gt; &lt;mm&gt; &lt;dd&gt; &lt;hh&gt;:&lt;mm&gt;:&lt;ss&gt; [interval &lt;5-65535&gt;]</pre> <p>Triggers a script execution at a specific given date. The script runs only once if no time interval is configured.</p> <p><b>Note:</b> If system time zone changes, all absolute timer jobs are automatically rescheduled.</p> <p><b>Command mode:</b> Scheduler Job</p>
<pre>event time relative &lt;0-2147483647&gt; [interval &lt;5-65535&gt;]</pre> <p>Triggers a script execution at a future start time expressed in seconds. The script runs only once if no time interval is configured.</p> <p><b>Note:</b> When this command is applied, the relative time is automatically converted to absolute time. Thus, the event is visible in running configuration as an absolute time.</p> <p><b>Command mode:</b> Scheduler Job</p>

Table 370. Scheduler Jobs Management Configuration Commands

Command Syntax and Usage
<pre>action &lt;script file name&gt; [&lt;argument list&gt;]</pre> <p>Configures the script file name to be executed and an optional list of arguments that are passed to the script when executed. The list of arguments must be provided as a string enclosed in double quotes and the arguments must be separated by white spaces. The arguments string must not exceed 199 characters.</p> <p><b>Command mode:</b> Scheduler Job</p>
<pre>show scheduler job</pre> <p>Displays a list of all currently scheduled jobs. For more information, see <a href="#">page 143</a>.</p> <p><b>Command mode:</b> All</p>

## Running Job Monitor

The user is allowed to control running scripts.

[Table 349](#) describes the job monitoring commands.

*Table 371. Running Job Monitor Configuration Commands*

Command Syntax and Usage
<pre>kill scheduler job name &lt;job name&gt;</pre> <p>Terminates a running script.</p> <p><b>Command mode:</b> Privileged EXEC</p>
<pre>[no] scheduler job cpu-limit &lt;5-50&gt;</pre> <p>Enables or disables the option to terminate a running script when CPU usage percentage exceeds a globally defined threshold. CPU usage percentage is checked every 5 seconds.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>[no] scheduler job time-limit &lt;10-600&gt;</pre> <p>Enables or disables the option to terminate a running script when elapsed time exceeds a globally defined threshold (seconds).</p> <p><b>Command mode:</b> Global configuration</p>



## 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 372. General Operations Commands

Command Syntax and Usage
<pre>password &lt;1-128 characters&gt;</pre> <p>Allows the user to change the password. You must enter the current password in use for validation. The switch prompts for a new password between 1-128 characters.</p> <p><b>Command Mode:</b> Privileged EXEC</p>
<pre>access tnetsshc</pre> <p>Closes all open Telnet and SSH connections.</p> <p><b>Command Mode:</b> Global configuration</p>
<pre>console-log</pre> <p>Enables or disables session console logging.</p> <p><b>Command Mode:</b> Privileged EXEC</p>
<pre>clear logging</pre> <p>Clears all Syslog messages.</p> <p><b>Command Mode:</b> Privileged EXEC</p>
<pre>ntp send</pre> <p>Allows the user to send requests to the NTP server.</p> <p><b>Command Mode:</b> Privileged EXEC</p>
<pre>clear openflow table [basic emergency static]</pre> <p>Clears OpenFlow tables.</p> <ul style="list-style-type: none"><li>– The <code>basic</code> option clears only the basic OpenFlow table</li><li>– The <code>emergency</code> option clears only the emergency OpenFlow table</li><li>– The <code>static</code> option clears only the static Openflow table</li></ul> <p><b>Command Mode:</b> Privileged EXEC</p>

---

## Operations-Level Port Commands

Operations-level port options are used for temporarily disabling or enabling a port, and for re-setting the port.

Table 373. Port Operations

Command Syntax and Usage
<pre>interface port &lt;port number or alias&gt; dot1x init</pre> <p>Reinitializes 802.1x access control on the port.</p> <p><b>Command Mode:</b> Privileged EXEC</p>
<pre>interface port &lt;port number or alias&gt; dot1x re-authenticate</pre> <p>Immediately starts reauthentication on the port.</p> <p><b>Command Mode:</b> Privileged EXEC</p>
<pre>[no] interface port &lt;port number or alias&gt; rmon</pre> <p>Temporarily enables or disables remote monitoring of the port. The port will be returned to its configured operation mode when the switch is reset.</p> <p><b>Command Mode:</b> Privileged EXEC</p>
<pre>no interface port &lt;port number or alias&gt; shutdown</pre> <p>Temporarily enables the port. The port will be returned to its configured operation mode when the switch is reset.</p> <p><b>Command Mode:</b> Privileged EXEC</p>
<pre>interface port &lt;port number or alias&gt; shutdown</pre> <p>Temporarily disables the port. The port will be returned to its configured operation mode when the switch is reset.</p> <p><b>Command Mode:</b> Privileged EXEC</p>
<pre>interface port &lt;port number or alias&gt; learning</pre> <p>Temporarily enables FDB learning on the port.</p> <p><b>Command Mode:</b> Privileged EXEC</p>
<pre>no interface port &lt;port number or alias&gt; learning</pre> <p>Temporarily disables FDB learning on the port.</p> <p><b>Command Mode:</b> Privileged EXEC</p>
<pre>show interface port &lt;port number or alias&gt; operation</pre> <p>Displays the port interface operational state.</p> <p><b>Command Mode:</b> Privileged EXEC</p>

---

## Operations-Level FCoE Commands

Fiber Channel over Ethernet (FCoE) operations commands are listed in the following table.

Table 374. FCoE Operations

Command Syntax and Usage
<pre>no fcoe fips fcf &lt;FCF MAC address&gt; [&lt;vlan number&gt;]</pre> <p>Deletes the selected FCoE Forwarder (FCF) and any associated ACLs.</p> <p><b>Command Mode:</b> Privileged EXEC</p>

---

## Operations-Level VRRP Commands

Operations-level VRRP commands are listed in the following table.

Table 375. Virtual Router Redundancy Operations

Command Syntax and Usage
<pre>router vrrp backup {&lt;virtual router number (1-128)&gt; group}</pre> <p>Forces the specified master virtual router on this switch into backup mode. This is generally used for passing master control back to a preferred switch once the preferred switch has been returned to service after a failure. When this command is executed, the current master gives up control and initiates a new election by temporarily advertising its own priority level as 0 (lowest). After the new election, the virtual router forced into backup mode by this command will resume master control in the following cases:</p> <ul style="list-style-type: none"><li>– This switch owns the virtual router (the IP addresses of the virtual router and its IP interface are the same)</li><li>– This switch's virtual router has a higher priority and preemption is enabled.</li><li>– There are no other virtual routers available to take master control.</li></ul> <p><b>Command Mode:</b> Privileged EXEC</p>



---

## Operations-Level BGP Commands

Table 376. IP BGP Operations

Command Syntax and Usage
<pre>router bgp start &lt;peer number&gt;</pre> <p>Starts the peer session. <b>Command Mode:</b> Privileged EXEC</p>
<pre>router bgp stop &lt;peer number&gt;</pre> <p>Stops the peer session. <b>Command Mode:</b> Privileged EXEC</p>
<pre>show ip bgp state</pre> <p>Displays the current BGP operational state. <b>Command Mode:</b> Privileged EXEC</p>

---

## VMware Operations

Use these commands to perform minor adjustments to the VMware operation. Use these commands to perform Virtual Switch operations directly from the switch. Note that these commands require the configuration of Virtual Center access information (`virt vmware vcspec`).

Table 377. VMware Operations

Command Syntax and Usage
<pre>virt vmware pg [&lt;Port Group name&gt; &lt;host ID&gt; &lt;VSwitch name&gt; &lt;VLAN number&gt; &lt;shaping-enabled&gt; &lt;average-Kbps&gt; &lt;burst-KB&gt; &lt;peak-Kbps&gt;]</pre> <p>Adds a Port Group to a VMware host. You are prompted for the following information:</p> <ul style="list-style-type: none"><li>– Port Group name</li><li>– VMware host ID (Use host UUID, host IP address, or host name.)</li><li>– Virtual Switch name</li><li>– VLAN ID of the Port Group</li><li>– Whether to enable the traffic-shaping profile (1 or 0). If you choose 1 (yes), you are prompted to enter the traffic shaping parameters.</li></ul> <p><b>Command Mode:</b> All</p>
<pre>virt vmware vsw &lt;host ID&gt; &lt;Virtual Switch name&gt;</pre> <p>Adds a Virtual Switch to a VMware host. Use one of the following identifiers to specify the host:</p> <ul style="list-style-type: none"><li>– UUID</li><li>– IP address</li><li>– Host name</li></ul> <p><b>Command Mode:</b> All</p>
<pre>no virt vmware pg &lt;Port Group name&gt; &lt;host ID&gt;</pre> <p>Removes a Port Group from a VMware host. Use one of the following identifiers to specify the host:</p> <ul style="list-style-type: none"><li>– UUID</li><li>– IP address</li><li>– Host name</li></ul> <p><b>Command Mode:</b> All</p>
<pre>no virt vmware vsw &lt;host ID&gt; &lt;Virtual Switch name&gt;</pre> <p>Removes a Virtual Switch from a VMware host. Use one of the following identifiers to specify the host:</p> <ul style="list-style-type: none"><li>– UUID</li><li>– IP address</li><li>– Host name</li></ul> <p><b>Command Mode:</b> All</p>

Table 377. VMware Operations (continued)

Command Syntax and Usage	
<pre>virt vmware export &lt;VM profile name&gt; &lt;VMware host ID&gt; &lt;Virtual Switch name&gt;</pre>	<p>Exports a VM Profile to a VMware host.</p> <p>Use one of the following identifiers to specify each host:</p> <ul style="list-style-type: none"> <li>– UUID</li> <li>– IP address</li> <li>– Host name</li> </ul> <p>You may enter a Virtual Switch name, or enter a new name to create a new Virtual Switch.</p> <p><b>Command Mode:</b> All</p>
<pre>virt vmware scan</pre>	<p>Performs a scan of the VM Agent, and updates VM information.</p> <p><b>Command Mode:</b> All</p>
<pre>virt vmware vmacpg &lt;MAC address&gt; &lt;Port Group name&gt;</pre>	<p>Changes a VM NIC's configured Port Group.</p> <p><b>Command Mode:</b> All</p>
<pre>virt vmware updpkg &lt;Port Group name&gt; &lt;host ID&gt; &lt;VLAN number&gt; [&lt;shaping enabled&gt; &lt;average (1-1000000000)&gt; &lt;burst (1-1000000000)&gt; &lt;peak (1-1000000000)&gt;]</pre>	<p>Updates a VMware host's Port Group parameters. Use one of the following identifiers for the host ID:</p> <ul style="list-style-type: none"> <li>– UUID</li> <li>– IP address</li> <li>– Host name</li> </ul> <p>Enter the traffic shaping parameters as follows:</p> <ul style="list-style-type: none"> <li>– Shaping enabled</li> <li>– Average traffic, in Kilobits per second</li> <li>– Maximum burst size, in Kilobytes</li> <li>– Peak traffic, in Kilobits per second</li> </ul> <p>Delete traffic shaping parameters.</p> <p><b>Command Mode:</b> All</p>

---

## VMware Distributed Virtual Switch Operations

Use these commands to administer a VMware Distributed Virtual Switch (dvSwitch).

Table 378. VMware dvSwitch Operations (/oper/virt/vmware/dvswitch)

Command Syntax and Usage
<pre>virt vmware dvswitch add &lt;datacenter name&gt; &lt;dvSwitch name&gt; &lt;dvSwitch version&gt;</pre> <p>Adds the specified dvSwitch to the specified DataCenter.</p> <p><b>Command Mode:</b> All</p>
<pre>virt vmware dvswitch del &lt;datacenter name&gt; &lt;dvSwitch name&gt;</pre> <p>Removes the specified dvSwitch from the specified DataCenter.</p> <p><b>Command Mode:</b> All</p>
<pre>virt vmware dvswitch addhost &lt;dvSwitch name&gt; &lt;host UUID IP address host name&gt;</pre> <p>Adds the specified host to the specified dvSwitch. Use one of the following identifiers to specify the host:</p> <ul style="list-style-type: none"><li>– UUID</li><li>– IP address</li><li>– Host name</li></ul> <p><b>Command Mode:</b> All</p>
<pre>virt vmware dvswitch remhost &lt;dvSwitch name&gt; &lt;host UUID IP address host name&gt;</pre> <p>Removes the specified host from the specified dvSwitch. Use one of the following identifiers to specify the host:</p> <ul style="list-style-type: none"><li>– UUID</li><li>– IP address</li><li>– Host name</li></ul> <p><b>Command Mode:</b> All</p>
<pre>virt vmware dvswitch addUplink &lt;dvSwitch name&gt; &lt;host ID&gt; &lt;uplink name&gt;</pre> <p>Adds the specified physical NIC to the specified dvSwitch uplink ports.</p> <p><b>Command Mode:</b> All</p>
<pre>virt vmware dvswitch remUplink &lt;dvSwitch name&gt; &lt;host ID&gt; &lt;uplink name&gt;</pre> <p>Removes the specified physical NIC from the specified dvSwitch uplink ports.</p> <p><b>Command Mode:</b> All</p>

## VMware Distributed Port Group Operations

Use these commands to administer a VMware distributed port group.

Table 379. VMware Distributed Port Group Operations (/oper/virt/vmware/dpg)

Command Syntax and Usage
<pre>virt vmware dpg add &lt;port group name&gt; &lt;dvSwitch name&gt; &lt;VLAN ID&gt; [ishaping &lt;bandwidth&gt; &lt;burst size&gt; &lt;peak bandwidth&gt;] [eshaping &lt;bandwidth&gt; &lt;burst size&gt; &lt;peak bandwidth&gt;]</pre> <p>Adds the specified port group to the specified dvSwitch. You may enter the following parameters:</p> <ul style="list-style-type: none"> <li>– ishaping: Enables ingress shaping. Supply the following information: <ul style="list-style-type: none"> <li>• average bandwidth in KB per second</li> <li>• burst size in KB</li> <li>• peak bandwidth in KB per second</li> </ul> </li> <li>– eshaping: Enables egress shaping. Supply the following information: <ul style="list-style-type: none"> <li>• average bandwidth in KB per second</li> <li>• burst size in KB</li> <li>• peak bandwidth in KB per second</li> </ul> </li> </ul> <p><b>Command Mode:</b> All</p>
<pre>virt vmware dpg vmac &lt;VNIC MAC&gt; &lt;port group name&gt;</pre> <p>Adds the specified VM NIC to the specified port group.</p> <p><b>Command Mode:</b> All</p>
<pre>virt vmware dpg update &lt;port group name&gt; &lt;dvSwitch name&gt; &lt;VLAN ID (1-4094)&gt; [ishaping &lt;bandwidth&gt; &lt;burst size&gt; &lt;peak bandwidth&gt;] [eshaping &lt;bandwidth&gt; &lt;burst size&gt; &lt;peak bandwidth&gt;]</pre> <p>Updates the specified port group on the specified dvSwitch. You may enter the following parameters:</p> <ul style="list-style-type: none"> <li>– ishaping: Enables ingress shaping. Supply the following information: <ul style="list-style-type: none"> <li>• average bandwidth in KB per second</li> <li>• burst size in KB</li> <li>• peak bandwidth in KB per second</li> </ul> </li> <li>– eshaping: Enables egress shaping. Supply the following information: <ul style="list-style-type: none"> <li>• average bandwidth in KB per second</li> <li>• burst size in KB</li> <li>• peak bandwidth in KB per second</li> </ul> </li> </ul> <p><b>Command Mode:</b> All</p>
<pre>virt vmware dpg del &lt;port group name&gt; &lt;dvSwitch name&gt;</pre> <p>Removes the specified port group from the specified dvSwitch.</p> <p><b>Command Mode:</b> All</p>



## Chapter 6. Boot Options

To use the Boot Options commands, you must be logged in to the switch as the administrator. The Boot Options commands provide options for:

- Selecting a switch software image to be used when the switch is next reset
- Selecting a configuration block to be used when the switch is next reset
- Downloading or uploading a new software image to the switch via FTP/TFTP

In addition to the Boot commands, you can use a Web browser or SNMP to work with switch image and configuration files. To use SNMP, refer to “Working with Switch Images and Configuration Files” in the *Command Reference*.

The boot options are discussed in the following sections.

### Stacking Boot Options

The Stacking Boot options are used to define the role of the switch in a stack: either as the Master that controls the stack, or as a participating Member switch. Options are available for loading stack software to individual Member switches, and to configure the VLAN that is reserved for inter-switch stacking communications.

You must enable Stacking and reset the switch to enter Stacking mode. When the switch enters Stacking mode, the Stacking configuration menu appears. For more information, see “[Stacking Switch Configuration](#)” on page 303.

[Table 380](#) lists the Boot Stacking command options.

Table 380. Boot Stacking Options

Command Syntax and Usage
<pre>boot stack mode [master member]</pre> <p>Configures the Stacking mode for the selected switch.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>boot stack hlgig-trunk &lt;list of ports&gt;</pre> <p>Configures the ports used to connect the switch to the stack. Enter only 10Gb or 40Gb external ports.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>boot stack vlan &lt;VLAN number&gt; [&lt;1-16&gt; all backup master]</pre> <p>Configures the VLAN used for Stacking control communication. This can be applied for:</p> <ul style="list-style-type: none"><li>– a specific unit &lt;1-16&gt;</li><li>– all units</li><li>– backup unit</li><li>– master unit</li></ul> <p><b>Command mode:</b> Global configuration</p>

Table 380. Boot Stacking Options (continued)

Command Syntax and Usage
<pre>default boot stack [master backup &lt;csnum (1-8)&gt; all]</pre> <p>Resets the Stacking boot parameters to their default values.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>boot stack push-image {image1 image2 boot}</pre> <p>Pushes the selected software file from the master to the selected switch.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>boot stack enable</pre> <p>Enables the switch stack.</p> <p><b>Note:</b> When the switch reboots in stacking, it is reset to the factory default settings.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>no boot stack enable</pre> <p>Disables the switch stack.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>show boot stack [master backup &lt;csnum (1-8)&gt; all]</pre> <p>Displays current Stacking boot parameters.</p> <p><b>Command mode:</b> All</p>

When in stacking mode, the following stand-alone features are not supported:

- Active Multi-Path Protocol (AMP)
- SFD
- sFlow port monitoring
- Uni-Directional Link Detection (UDLD)
- Port flood blocking
- BCM rate control
- Private VLANs
- RIP
- OSPF and OSPFv3
- IPv6
- Virtual Router Redundancy Protocol (VRRP)
- Loopback Interfaces
- Router IDs
- Route maps
- Border Gateway Protocol (BGP)
- MAC address notification
- Static MAC address adding
- Static multicast
- Static routes
- MSTP and RSTP settings for CIST, Name, Rev, and Maxhop
- IGMP Relay and IGMPv3
- Microburst Detection



Switch menus and commands for unsupported features may be unavailable, or may have no effect on switch operation.

---

## 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 381. Scheduled Reboot Options

Command Syntax and Usage
<pre>boot schedule &lt;day&gt; &lt;time (hh:mm)&gt;</pre> <p>Configures the switch reset time. The following options are valid for the <code>day</code> value:</p> <ul style="list-style-type: none"><li>monday</li><li>tuesday</li><li>wednesday</li><li>thursday</li><li>friday</li><li>saturday</li><li>sunday</li></ul> <p><b>Command Mode:</b> Global configuration</p>
<pre>no boot schedule</pre> <p> Cancels the switch reset time.</p> <p><b>Command Mode:</b> Global configuration</p>
<pre>show boot</pre> <p>Displays the current switch reboot schedule.</p> <p><b>Command Mode:</b> All except User EXEC</p>

---

## Netboot Configuration

Netboot allows the switch to automatically download its configuration file over the network during switch reboot, and apply the new configuration. Upon reboot, the switch includes the following options in its DHCP requests:

- Option 66 (TFTP server address)
- Option 67 (file path)

If the DHCP server returns the information, the switch initiates a TFTP file transfer, and loads the configuration file into the active configuration block. As the switch boots up, it applies the new configuration file. Note that the option 66 TFTP server address must be specified in IP-address format (host name is not supported).

If DHCP is not enabled, or the DHCP server does not return the required information, the switch uses the manually-configured TFTP server address and file path.

Table 382. Netboot Options

Command Syntax and Usage
<pre>boot netboot enable</pre> <p>Enables Netboot. When enabled, the switch boots into factory-default configuration, and attempts to download a new configuration file.</p> <p><b>Command Mode:</b> Global configuration</p>
<pre>no boot netboot enable</pre> <p>Disables Netboot.</p> <p><b>Command Mode:</b> Global configuration</p>
<pre>[no] boot netboot tftp &lt;IP address&gt;</pre> <p>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.</p> <p><b>Command Mode:</b> Global configuration</p>
<pre>[no] boot netboot cfgfile &lt;1-31 characters&gt;</pre> <p>Defines the file path for the configuration file or script file on the TFTP server. For example:</p> <pre>/directory/sub/config.cfg /directory/sub/config.py</pre> <p><b>Command Mode:</b> Global configuration</p>
<pre>show boot</pre> <p>Displays the current Netboot parameters.</p> <p><b>Command Mode:</b> All</p>

## Forwarding Mode Configuration

This feature configures the switch Layer 2 packet forwarding methodology to either Cut-Through or Store-and-Forward.

Table 383. Forwarding Mode Options

Command Syntax and Usage
<pre>boot forwarding-mode {cut-through store-and-forward}</pre> <p>Configures the Layer 2 packet forwarding methodology:</p> <ul style="list-style-type: none"><li>– In <code>cut-through</code> mode, packets are forwarded immediately after the destination MAC address in the packet header is examined, without reading the rest of the packet. This reduces latency, but may propagate potentially corrupted packets.</li><li>– In <code>store-and-forward</code> mode, the switch examines the entire packet and compares the Cyclic-Redundancy-Check (CRC) field against its own Frame-Check-Sequence (FCS) computation. The switch then drops corrupted packets and forwards only intact packets.</li></ul> <p>The default value is <code>cut-through</code>.</p> <p>You must reboot the switch for this change to take effect.</p> <p><b>Command Mode:</b> Global configuration</p>

## Machine Type Model Configuration

This feature configures the switch Machine Type Model (MTM).

Table 384. Machine Type Model Configuration

Command Syntax and Usage
<pre>boot mtm &lt;MTM code&gt;</pre> <p>Configures the switch's machine type model (MTM) value. MTMs are applied on reset and persist over firmware upgrades:</p> <p><b>Command Mode:</b> Global configuration</p>

## QSFP Port Configuration

Table 385. QSFP Port Options

Command Syntax and Usage
<pre>boot qsfps-40gports &lt;1, 5, 9, 13&gt;</pre> <p>Enables 40GbE mode on the selected QSFP+ ports. When enabled, each QSFP+ port is set as a single 40GbE port.</p> <p>You must reboot the switch for this change to take effect.</p> <p><b>Command Mode:</b> Global configuration</p>
<pre>no boot qsfps-40gports &lt;1, 5, 9, 13&gt;</pre> <p>Disables 40GbE mode on the selected QSFP+ ports. When disabled, each QSFP+ port is configured to breakout into four 10GbE ports.</p> <p>You must reboot the switch for this change to take effect.</p> <p><b>Command Mode:</b> Global configuration</p>
<pre>show boot qsfps-port-modes</pre> <p>Displays the current QSFP parameters.</p> <p><b>Command Mode:</b> All</p>

---

## 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.

- `RSG8264_Boot.img`  
The switch replaces the current boot image with the new image, and boots with the new image.
- `RSG8264_OS.img`  
The switch boots with the new software image. The existing images are not affected.
- `RSG8264_replace1_OS.img`  
The switch replaces the current software image1 with the new image, and boots with the new image.
- `RSG8264_replace2_OS.img`  
The switch replaces the current software image2 with the new image, and boots with the new image.
- `RSG8264.cfg`  
The switch boots with the new configuration file. The existing configuration files (active and backup) are not affected.
- `RSG8264_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 517](#).

---

## 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.

Next, select a software image to run, as described in the following section.

## Selecting a Software Image to Run

You can select which software image (`image1` or `image2`) you want to run in switch memory for the next reboot.

1. In Global Configuration mode, enter:

```
Router(config)# boot image {image1|image2}
```

2. Enter the name of the image you want the switch to use upon the next boot. The system informs you of which image set to be loaded at the next reset:

```
Next boot will use switch software image1 instead of image2.
```

## Uploading a Software Image from Your Switch

You can upload a software image from the switch to a FTP or TFTP server.

1. In Privileged EXEC mode, enter:

```
Router# copy {image1|image2|boot-image} {ftp|tftp}
```

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}
```

---

## Setting an Entitlement Serial Number

To improve customer technical support, your customer support representative can assign your switch an Entitlement Serial Number (ESN) at the time you request support. The ESN can be conveniently stored on the switch using the following command:

```
RS8264(config)# boot esn <Entitlement Serial Number>
```

The ESN helps to locate your switch's identifying information when you call technical support for help in future.

---

## 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 IBM N/OS CLI

The default command-line interface for the G8264 is the ISCLI. To access the IBM N/OS CLI, enter the following command from the ISCLI:

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

To access the ISCLI, enter the following command from the IBM N/OS 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.

---

## Changing the Switch Profile

The IBM N/OS software for the G8264 can be configured to operate in different modes for different deployment scenarios. The deployment profile changes some of the basic switch behavior, shifting switch resources to optimize capacity levels to meet the needs of different types of networks. For more information about deployment profiles, see the IBM N/OS 7.6 *Application Guide*.

To change the deployment profile, select the new profile and reset the G8264. Use the following command to select a new profile:

```
Router(config)# boot profile {default | acl | ipmc-opt | openflow}
```

---

## Using the Boot Management Menu

The Boot Management menu allows you to switch the software image, reset the switch to factory defaults, or to recover from a failed software download.

You can interrupt the boot process and enter the Boot Management menu from the serial console port. When the system displays Memory Test, press **<Shift B>**. The Boot Management menu appears.

```
Resetting the System ...
Memory Test .....

Boot Management Menu
1 - Change booting image
2 - Change configuration block
3 - Xmodem download
4 - Exit

Please choose your menu option: 1
Current boot image is 1. Enter image to boot: 1 or 2: 2
Booting from image 2
```

The Boot Management menu allows you to perform the following actions:

- To change the booting image, press 1 and follow the screen prompts.
- To change the configuration block, press 2, and follow the screen prompts.
- To perform an Xmodem download, press 3 and follow the screen prompts.
- To exit the Boot Management menu, press 4. The booting process continues.

## Recovering from a Failed 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 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 386. General Maintenance Commands

Command Syntax and Usage
<pre>show flash-dump-uuencode</pre> <p>Displays dump information in uuencoded format. For details, see <a href="#">page 573</a>.</p> <p><b>Command mode:</b> All</p>
<pre>copy flash-dump {tftp ftp sftp} {data mgt}</pre> <p>Saves the system dump information via TFTP, FTP or SFTP. For details, see <a href="#">page 574</a>.</p> <p><b>Command mode:</b> Privileged EXEC</p>
<pre>copy &lt;switch filename&gt; tftp address &lt;TFTP server address&gt; filename &lt;filename on TFTP server&gt;</pre> <p>Saves a file via TFTP.sC</p> <p><b>Command mode:</b> Privileged EXEC</p>
<pre>clear flash-dump</pre> <p>Clears dump information from flash memory.</p> <p><b>Command mode:</b> Privileged EXEC</p>
<pre>copy log tftp {data mgt}</pre> <p>Saves the system log file (SYSLOG) via TFTP.</p> <p><b>Command mode:</b> Privileged EXEC</p>
<pre>clear log</pre> <p>Clears the system log file (SYSLOG).</p> <p><b>Command mode:</b> Privileged EXEC</p>

Table 386. General Maintenance Commands (continued)

Command Syntax and Usage
<pre>show tech-support [l2 l3 link port]</pre> <p>Dumps all G8264 information, statistics, and configuration. You can log the output (tsdmp) into a file. To filter the information, use the following options:</p> <ul style="list-style-type: none"><li>– l2 displays only Layer 2-related information</li><li>– l3 displays only Layer 3-related information</li><li>– link displays only link status-related information</li><li>– port displays only port-related information</li></ul> <p><b>Command mode:</b> All except User EXEC</p>
<pre>copy tech-support tftp {data mgt}</pre> <p>Redirects the technical support dump (tsdmp) to an external TFTP server.</p> <p><b>Command mode:</b> Privileged EXEC</p>
<pre>copy tech-support ftp {data mgt}</pre> <p>Redirects the technical support dump (tsdmp) to an external FTP server.</p> <p><b>Command mode:</b> Privileged EXEC</p>

---

## Forwarding Database Maintenance

The Forwarding Database commands can be used to view information and to delete a MAC address from the forwarding database or to clear the entire forwarding database. This is helpful in identifying problems associated with MAC address learning and packet forwarding decisions.

Table 387. FDB Manipulation Options

Command Syntax and Usage
<pre>show mac-address-table address &lt;MAC address&gt;</pre> <p>Displays a single database entry by its MAC address. Enter the MAC address using one of the following formats:</p> <ul style="list-style-type: none"><li>– xx:xx:xx:xx:xx:xx (such as 08:00:20:12:34:56)</li><li>– xxxxxxxxxxxx (such as 080020123456)</li></ul> <p><b>Command mode:</b> All</p>
<pre>show mac-address-table interface port &lt;port number or alias&gt;</pre> <p>Displays all FDB entries for a particular port.</p> <p><b>Command mode:</b> All</p>
<pre>show mac-address-table vlan &lt;VLAN number&gt;</pre> <p>Displays all FDB entries on a single VLAN.</p> <p><b>Command mode:</b> All</p>
<pre>show mac-address-table multicast</pre> <p>Displays all Multicast MAC entries in the FDB.</p> <p><b>Command mode:</b> All</p>
<pre>show mac-address-table static</pre> <p>Displays static entries in the FDB.</p> <p><b>Command mode:</b> All except User EXEC</p>
<pre>no mac-address-table {static multicast} {all &lt;MAC address&gt; &lt;VLAN number&gt;}</pre> <p>Removes static FDB entries.</p> <p><b>Command mode:</b> Global configuration</p>
<pre>clear mac-address-table</pre> <p>Clears the entire Forwarding Database from switch memory.</p> <p><b>Command mode:</b> Privileged EXEC</p>

---

## Debugging Commands

The Miscellaneous Debug Commands display trace buffer information about events that can be helpful in understanding switch operation. You can view the following information using the debug commands:

- Events traced by the Management Processor (MP)
- Events traced to a buffer area when a reset occurs

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 388. Miscellaneous Debug Options

Command Syntax and Usage	
<code>debug debug-flags</code>	This command sets the flags that are used for debugging purposes. <b>Command mode:</b> Privileged EXEC
<code>debug mp-trace</code>	Displays the Management Processor trace buffer. Header information similar to the following is shown:  MP trace buffer at 13:28:15 Fri May 25, 2001; mask: 0x2ffdf748  The buffer information is displayed after the header. <b>Command mode:</b> Privileged EXEC
<code>debug dumpbt</code>	Displays the backtrace log. <b>Command mode:</b> Privileged EXEC
<code>debug mp-snap</code>	Displays the Management Processor snap (or post-mortem) trace buffer. This buffer contains information traced at the time that a reset occurred. <b>Command mode:</b> Privileged EXEC
<code>clear flash-config</code>	Deletes all flash configuration blocks. <b>Command mode:</b> Privileged EXEC
<code>debug pstat &lt;port alias or number&gt;</code>	Displays all port statistics for the selected port. <b>Command mode:</b> Privileged EXEC

Table 388. Miscellaneous Debug Options

Command Syntax and Usage
<p>[no] debug lacp packet [receive transmit both] [port &lt;port numbers&gt;]</p> <p>Enables/disables debugging for Link Aggregation Control Protocol (LACP) packets on all ports running LACP.</p> <p>The following parameters are available:</p> <ul style="list-style-type: none"><li>– receive filters only LACP packets received</li><li>– transmit filters only LACP packets sent</li><li>– both filters LACP packets either sent or received</li><li>– port filters LACP packets sent/received on specific ports</li></ul> <p>By default, LACP debugging is disabled.</p> <p><b>Command mode:</b> Privileged EXEC</p>
<p>[no] debug spanning-tree bpdu [receive transmit]</p> <p>Enables/disables debugging for Spanning Tree Protocol (STP) Bridge Protocol Data Unit (BPDU) frames sent or received.</p> <p>The following parameters are available:</p> <ul style="list-style-type: none"><li>– receive filters only BPDU frames received</li><li>– transmit filters only BPDU frames sent</li></ul> <p>By default, STP BPDU debugging is disabled.</p> <p><b>Command mode:</b> Privileged EXEC</p>

---

## IPsec Debugging

Tablx describes the IPsec debugging commands.

Table 389. IPsec Debugging Options

Command Syntax and Usage
[no] debug sec all Enables or disables all IP security debug messages. <b>Command mode:</b> Privileged EXEC
[no] debug sec crypto Enables or disables all IP security cryptographic debug messages. <b>Command mode:</b> Privileged EXEC
[no] debug sec ike Enables or disables all IP security IKEv2 debug messages. <b>Command mode:</b> Privileged EXEC
[no] debug sec ipsec Enables or disables all IPsec debug messages. <b>Command mode:</b> Privileged EXEC
[no] debug sec info Displays the current security debug flag. <b>Command mode:</b> Privileged EXEC



---

## BGP Debugging

Table 390 describes the IPsec debugging commands.

Table 390. BGP Debugging Options

Command Syntax and Usage	
[no] debug bgp	Enables or disables all BGP debug messages for all existing peers. <b>Command mode:</b> Privileged EXEC
[no] debug bgp <IP address>	Enables or disables all BGP debug messages for the specified BGP neighbor. <b>Command mode:</b> Privileged EXEC
[no] debug bgp in out	Enables or disables all inbound or outbound BGP debug messages. <b>Command mode:</b> Privileged EXEC
[no] debug bgp <IP address> in out	Enables or disables all inbound or outbound BGP debug messages for the specified BGP neighbor. <b>Command mode:</b> Privileged EXEC
show debug bgp	Displays the current BGP debug setting. <b>Command mode:</b> All

---

## DCBX Maintenance

Table 391 describes the DCBX maintenance commands.

Table 391. DCBX Maintenance Commands

Command Syntax and Usage
<pre>show cee information dcbx port &lt;port alias or number&gt;</pre> <p>Displays DCBX feature information for the selected port.</p> <p><b>Command mode:</b> All</p>
<pre>show cee information dcbx port &lt;port alias or number&gt; app_proto</pre> <p>Displays DCBX application protocol state-machine information.</p> <p><b>Command mode:</b> All</p>
<pre>show cee information dcbx port &lt;port alias or number&gt; ets</pre> <p>Displays DCBX ETS state-machine information.</p> <p><b>Command mode:</b> All</p>
<pre>show cee information dcbx port &lt;port alias or number&gt; pfc</pre> <p>Displays DCBX PFC state-machine information.</p> <p><b>Command mode:</b> All</p>
<pre>show cee information dcbx port &lt;port alias or number&gt; control</pre> <p>Displays information about the Control state machine for the selected port.</p> <p><b>Command mode:</b> All</p>
<pre>show cee information dcbx port &lt;port alias or number&gt; feature</pre> <p>Displays information about the Feature state machine for the selected port.</p> <p><b>Command mode:</b> All</p>
<pre>show dcbx transmit</pre> <p>Displays the Type-Length-Value (TLV) list transmitted in the DCBX TLV for the selected port.</p> <p><b>Command mode:</b> All</p>
<pre>show dcbx receive</pre> <p>Displays the Type-Length-Value (TLV) list received in the DCBX TLV for the selected port.</p> <p><b>Command mode:</b> All</p>

---

## LLDP Cache Manipulation

[Table 392](#) describes the LLDP cache manipulation commands.

*Table 392. LLDP Cache Manipulation Options*

<b>Command Syntax and Usage</b>
<pre>show lldp port &lt;port alias or number&gt;</pre> <p>Displays Link Layer Discovery Protocol (LLDP) port information.</p> <p><b>Command mode:</b> All</p>
<pre>show lldp receive</pre> <p>Displays information about the LLDP receive state machine.</p> <p><b>Command mode:</b> All</p>
<pre>show lldp transmit</pre> <p>Displays information about the LLDP transmit state machine.</p> <p><b>Command mode:</b> All</p>
<pre>show lldp remote-device [&lt;1-256&gt; detail]</pre> <p>Displays information received from LLDP -capable devices. For more information, see <a href="#">page 42</a>.</p> <p><b>Command mode:</b> All</p>
<pre>show lldp</pre> <p>Displays all LLDP information.</p> <p><b>Command mode:</b> All</p>
<pre>clear lldp</pre> <p>Clears the LLDP cache.</p> <p><b>Command mode:</b> Privileged EXEC</p>

---

## ARP Cache Maintenance

[Table 393](#) describes the ARP cache maintenance commands.

*Table 393. Address Resolution Protocol Maintenance Options*

Command Syntax and Usage
<pre>show ip arp find &lt;IP address&gt;</pre> <p>Shows a single ARP entry by IP address.</p> <p><b>Command mode:</b> All</p>
<pre>show ip arp interface port &lt;port number or alias&gt;</pre> <p>Shows ARP entries on selected ports.</p> <p><b>Command mode:</b> All</p>
<pre>show ip arp vlan &lt;VLAN number&gt;</pre> <p>Shows ARP entries on a single VLAN.</p> <p><b>Command mode:</b> All</p>
<pre>show ip arp reply</pre> <p>Shows the list of IP addresses which the switch will respond to for ARP requests.</p> <p><b>Command mode:</b> All</p>
<pre>show ip arp</pre> <p>Shows all ARP entries.</p> <p><b>Command mode:</b> All</p>
<pre>clear arp</pre> <p>Clears the entire ARP list from switch memory.</p> <p><b>Command mode:</b> Privileged EXEC</p>

**Note:** To display all or a portion of ARP entries currently held in the switch, you can also refer to “ARP Information” on [page 62](#).

---

## BGP Maintenance

Table 393 describes the BGP information commands.

Table 394. Border Gateway Protocol Maintenance Options

Command Syntax and Usage
<pre>show ip bgp debugging in out</pre> <p>Displays inbound or outbound BGP debugging updates.</p> <p><b>Command mode:</b> All</p>
<pre>show ip bgp debugging &lt;IP address&gt; in out [last]</pre> <p>Displays inbound or outbound BGP debugging updates for the specified neighbor. If <code>last</code> is specified, displays the results starting with the last entry first.</p> <p><b>Command mode:</b> All</p>
<pre>show ip bgp debugging ignored</pre> <p>Shows all BGP information for routers that have been ignored.</p> <p><b>Command mode:</b> All</p>
<pre>show ip bgp debugging &lt;IP address&gt; ignored [last]</pre> <p>Displays BGP information for routers that have been ignored by the specified neighbor. If <code>last</code> is specified, displays the results starting with the last entry first.</p> <p><b>Command mode:</b> All</p>
<pre>show ip bgp debugging &lt;IP address&gt; [last]</pre> <p>Displays all BGP debugging entries for the specified neighbor. If <code>last</code> is specified, displays the results starting with the last entry first.</p> <p><b>Command mode:</b> All</p>
<pre>show ip bgp debugging [last]</pre> <p>Displays all BGP debugging entries. If <code>last</code> is specified, displays the results starting with the last entry first.</p> <p><b>Command mode:</b> All</p>
<pre>show ip bgp information</pre> <p>Displays the BGP routing table.</p> <p><b>Command mode:</b> All</p>
<pre>show ip bgp information &lt;IP address&gt;</pre> <p>Displays the BGP routing table for the specified neighbor.</p> <p><b>Command mode:</b> All</p>
<pre>clear ip bgp debug-log</pre> <p>Clears the entire BGP debug log from switch memory.</p> <p><b>Command mode:</b> Privileged EXEC</p>

---

## IP Route Manipulation

Table 395 describes the IP route manipulation commands.

Table 395. IP Route Manipulation Options

Command Syntax and Usage
<pre>debug route-map pbr</pre> <p>Enables policy-based routing debugging.</p> <p><b>Command mode:</b> Privileged EXEC</p>
<pre>show ip route address &lt;IP address&gt;</pre> <p>Shows a single route by destination IP address.</p> <p><b>Command mode:</b> All</p>
<pre>show ip route gateway &lt;IP address&gt;</pre> <p>Shows routes to a default gateway.</p> <p><b>Command mode:</b> All</p>
<pre>show ip route type {indirect direct local broadcast  martian multicast}</pre> <p>Shows routes of a single type. For a description of IP routing types, see <a href="#">Table 42 on page 61</a></p> <p><b>Command mode:</b> All</p>
<pre>show ip route tag {fixed static address rip ospf broadcast  martian multicast}</pre> <p>Shows routes of a single tag. For a description of IP routing tags, see <a href="#">Table 43 on page 61</a></p> <p><b>Command mode:</b> All</p>
<pre>show ip route interface &lt;IP interface&gt;</pre> <p>Shows routes on a single interface.</p> <p><b>Command mode:</b> All</p>
<pre>show ip route</pre> <p>Shows all routes.</p> <p><b>Command mode:</b> All</p>
<pre>clear ip route</pre> <p>Clears the route table from switch memory.</p> <p><b>Command mode:</b> Privileged EXEC</p>

**Note:** To display all routes, you can also refer to “IP Routing Information” on [page 60](#).

---

## IGMP Snooping Maintenance

Table 396 describes the IGMP Snooping maintenance commands.

Table 396. IGMP Multicast Group Maintenance Options

Command Syntax and Usage
<pre>show ip igmp groups address &lt;IP address&gt;</pre> <p>Displays a single IGMP multicast group by its IP address.</p> <p><b>Command mode:</b> All</p>
<pre>show ip igmp groups vlan &lt;VLAN number&gt;</pre> <p>Displays all IGMP multicast groups on a single VLAN.</p> <p><b>Command mode:</b> All</p>
<pre>show ip igmp groups interface port &lt;port number or alias&gt;</pre> <p>Displays all IGMP multicast groups on selected ports.</p> <p><b>Command mode:</b> All</p>
<pre>show ip igmp groups portchannel &lt;trunk number&gt;</pre> <p>Displays all IGMP multicast groups on a single trunk group.</p> <p><b>Command mode:</b> All</p>
<pre>show ip igmp groups detail &lt;IP address&gt;</pre> <p>Displays detailed information about a single IGMP multicast group.</p> <p><b>Command mode:</b> All</p>
<pre>show ip igmp groups</pre> <p>Displays information for all multicast groups.</p> <p><b>Command mode:</b> All</p>
<pre>clear ip igmp groups</pre> <p>Clears the IGMP group table.</p> <p><b>Command mode:</b> Privileged EXEC</p>

---

## IGMP Multicast Routers Maintenance

Table 397 describes the maintenance commands for IGMP multicast routers (Mrouters).

Table 397. IGMP Multicast Router Maintenance Commands

Command Syntax and Usage
<pre>show ip igmp mrouter vlan &lt;VLAN number&gt;</pre> <p>Displays IGMP Mrouter information for a single VLAN.</p> <p><b>Command mode:</b> All</p>
<pre>show ip igmp mrouter</pre> <p>Displays information for all Mrouters.</p> <p><b>Command mode:</b> All</p>
<pre>show ip igmp mrouter information</pre> <p>Displays IGMP snooping information for all Mrouters.</p> <p><b>Command mode:</b> All</p>
<pre>show ip igmp snoop igmpv3</pre> <p>Displays IGMPv3 snooping information.</p> <p><b>Command mode:</b> All</p>
<pre>show ip igmp relay</pre> <p>Displays IGMP relay information.</p> <p><b>Command mode:</b> All</p>
<pre>show ip igmp querier vlan &lt;VLAN number&gt;</pre> <p>Displays IGMP querier information for a single VLAN.</p> <p><b>Command mode:</b> All</p>
<pre>clear ip igmp mrouter</pre> <p>Clears the IGMP Mrouter port table.</p> <p><b>Command mode:</b> Privileged EXEC</p>



## MLD Multicast Group Maintenance

Table 398 describes the maintenance commands for MLD multicast group maintenance.

Table 398. MLD Multicast Group Maintenance Commands

Command Syntax and Usage	
groups	Displays all MLD groups.
find <IPv6 address>	Shows a single MLD group by its IP address.
vlan <VLAN number>	Shows all MLD groups on a single VLAN.
port <port alias or number>	Shows all MLD groups on a single port.
trunk <trunk number>	Displays all MLD groups on a single trunk group.
if <interface number>	Shows MLD interface information.
mrclear	Clears dynamic MLD multicast router group tables from switch memory.
grclear	Clears dynamic MLD registered group tables from switch memory.
clear	Clears dynamic MLD group tables from switch memory.
show ip igmp mrouter vlan <VLAN number>	Displays IGMP Mrouter information for a single VLAN. <b>Command mode:</b> All
show ip igmp mrouter	Displays information for all Mrouters. <b>Command mode:</b> All
clear ip igmp mrouter	Clears the IGMP Mrouter port table. <b>Command mode:</b> Privileged EXEC

---

## LACP Maintenance

[Table 399](#) describes the maintenance commands for LACP.

*Table 399. LACP Maintenance Commands*

<b>Command Syntax and Usage</b>
<pre>qos protocol-packet-control packet-queue-map &lt;packet queue number&gt; lacp</pre> <p>Send an LACP Marker packet (for debugging only).</p> <p><b>Command mode:</b> All</p>

---

## IPv6 Neighbor Discovery Cache Manipulation

Table 400 describes the IPv6 Neighbor Discovery cache manipulation commands.

Table 400. IPv6 Neighbor Discovery Cache Manipulation Options

Command Syntax and Usage
<pre>show ipv6 neighbors find &lt;IPv6 address&gt;</pre> <p>Shows a single IPv6 Neighbor Discovery cache entry by IP address. <b>Command mode:</b> All</p>
<pre>show ipv6 neighbors interface port &lt;port number or alias&gt;</pre> <p>Shows IPv6 Neighbor Discovery cache entries on a single port. <b>Command mode:</b> All</p>
<pre>show ipv6 neighbors vlan &lt;VLAN number&gt;</pre> <p>Shows IPv6 Neighbor Discovery cache entries on a single VLAN. <b>Command mode:</b> All</p>
<pre>show ipv6 neighbors static</pre> <p>Shows static IPv6 Neighbor Discovery cache entries. <b>Command mode:</b> All</p>
<pre>show ipv6 neighbors</pre> <p>Shows all IPv6 Neighbor Discovery cache entries. <b>Command mode:</b> All</p>
<pre>clear ipv6 neighbors</pre> <p>Clears all IPv6 Neighbor Discovery cache entries from switch memory. <b>Command mode:</b> Privileged EXEC</p>

---

## IPv6 Route Maintenance

Table 401 describes the IPv6 route maintenance commands.

Table 401. IPv6 Route Maintenance Options

Command Syntax and Usage
<pre>show ipv6 route address &lt;IPv6 address&gt;</pre> <p>Show a single route by destination IP address.</p> <p><b>Command mode:</b> All</p>
<pre>show ipv6 route gateway &lt;IPv6 gateway number&gt;</pre> <p>Show routes to a single gateway.</p> <p><b>Command mode:</b> All</p>
<pre>show ipv6 route interface &lt;interface number&gt;</pre> <p>Show routes on a single IP interface.</p> <p><b>Command mode:</b> All</p>
<pre>show ipv6 route type {connected static ospf}</pre> <p>Show routes of a single type.</p> <p><b>Command mode:</b> All</p>
<pre>show ipv6 route static</pre> <p>Show static IPv6 routes.</p> <p><b>Command mode:</b> All</p>
<pre>show ipv6 route summary</pre> <p>Shows a summary of IPv6 route information.</p> <p><b>Command mode:</b> All</p>
<pre>show ipv6 route</pre> <p>Shows all IPv6 routes.</p> <p><b>Command mode:</b> All</p>
<pre>clear ipv6 route</pre> <p>Clears all IPv6 routes.</p> <p><b>Command mode:</b> Privileged EXEC</p>

---

## Uencode Flash Dump

Using this command, dump information is presented in uuencoded format. This format makes it easy to capture the dump information as a file or a string of characters.

If you want to capture dump information to a file, set your communication software on your workstation to capture session data prior to issuing the `show flash-dump-uuencode` command. This will ensure that you do not lose any information. Once entered, the `show flash-dump-uuencode` command will cause approximately 23,300 lines of data to be displayed on your screen and copied into the file.

Using the `show flash-dump-uuencode` command, dump information can be read multiple times. The command does not cause the information to be updated or cleared from flash memory.

**Note:** Dump information is not cleared automatically. In order for any subsequent dump information to be written to flash memory, you must manually clear the dump region. For more information on clearing the dump region, see [page 575](#).

To access dump information, enter:

```
Router# show flash-dump-uuencode
```

The dump information is displayed on your screen and, if you have configured your communication software to do so, captured to a file. If the dump region is empty, the following appears:

```
No FLASH dump available.
```

---

## TFTP, SFTP or FTP System Dump Put

Use these commands to `put` (save) the system dump to a TFTP or FTP server.

**Note:** If the TFTP/FTP server is running SunOS or the Solaris operating system, the specified `copy flash-dump tftp` (or `ftp`) file must exist *prior* to executing the `copy flash-dump tftp` command (or `copy flash-dump ftp`), and must be writable (set with proper permission, and not locked by any application). The contents of the specified file will be replaced with the current dump data.

To save dump information via TFTP, enter:

```
Router# copy flash-dump tftp <server filename>
```

You are prompted for the TFTP server IP address or hostname, and the *filename* of the target dump file.

To save dump information via SFTP, enter:

```
Router# copy flash-dump sftp <server filename>
```

You are prompted for the SFTP 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. IBM N/OS System Log Messages

The RackSwitch G8264 (G8264) uses the following syntax when outputting system log (syslog) messages:

*<Time stamp><IP/Hostname><Log Label>IBMOS<Thread ID> : <Message>*

The following parameters are used:

- *<Timestamp>*

The time of the message event is displayed in the following format:

*<month (3 characters)> <day> <hour (1-24)> : <minute> : <second>*

For example: Aug 19 14 : 20 : 30

- *<IP/Hostname>*

The hostname is displayed when configured.

For example: 1 . 1 . 1 . 1

- *<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: <table border="0" style="width: 100%; border-collapse: collapse;"> <tr> <td style="vertical-align: top; width: 50%;"> <ul style="list-style-type: none"> <li>• Connect Retry Expire</li> <li>• Holdtime Expire</li> <li>• Invalid</li> <li>• Keepalive Expire</li> <li>• Receive KEEPALIVE</li> <li>• Receive NOTIFICATION</li> <li>• Receive OPEN</li> </ul> </td> <td style="vertical-align: top; width: 50%; border-left: 1px solid black; padding-left: 10px;"> <ul style="list-style-type: none"> <li>• Receive UPDATE</li> <li>• Start</li> <li>• Stop</li> <li>• Transport Conn Closed</li> <li>• Transport Conn Failed</li> <li>• Transport Conn Open</li> <li>• Transport Fatal Error</li> </ul> </td> </tr> </table>	<ul style="list-style-type: none"> <li>• Connect Retry Expire</li> <li>• Holdtime Expire</li> <li>• Invalid</li> <li>• Keepalive Expire</li> <li>• Receive KEEPALIVE</li> <li>• Receive NOTIFICATION</li> <li>• Receive OPEN</li> </ul>	<ul style="list-style-type: none"> <li>• Receive UPDATE</li> <li>• Start</li> <li>• Stop</li> <li>• Transport Conn Closed</li> <li>• Transport Conn Failed</li> <li>• Transport Conn Open</li> <li>• Transport Fatal Error</li> </ul>		
<ul style="list-style-type: none"> <li>• Connect Retry Expire</li> <li>• Holdtime Expire</li> <li>• Invalid</li> <li>• Keepalive Expire</li> <li>• Receive KEEPALIVE</li> <li>• Receive NOTIFICATION</li> <li>• Receive OPEN</li> </ul>	<ul style="list-style-type: none"> <li>• Receive UPDATE</li> <li>• Start</li> <li>• Stop</li> <li>• Transport Conn Closed</li> <li>• Transport Conn Failed</li> <li>• Transport Conn Open</li> <li>• Transport Fatal Error</li> </ul>				
BGP	session with <IP address> failed <reason type> : <reason>  Reason Types: <table border="0" style="width: 100%; border-collapse: collapse;"> <tr> <td style="vertical-align: top; width: 50%;"> <ul style="list-style-type: none"> <li>• FSM Error</li> <li>• Hold Timer Expired</li> <li>• Message Header Error</li> </ul> </td> <td style="vertical-align: top; width: 50%; border-left: 1px solid black; padding-left: 10px;"> <ul style="list-style-type: none"> <li>• OPEN Message Error</li> <li>• UPDATE Message Error</li> </ul> </td> </tr> </table> Reasons: <table border="0" style="width: 100%; border-collapse: collapse;"> <tr> <td style="vertical-align: top; width: 50%;"> <ul style="list-style-type: none"> <li>• AS Routing Loop</li> <li>• Attr Flags Error</li> <li>• Attr Length Error</li> <li>• Auth Failure</li> <li>• Bad BGP Identifier</li> <li>• Bad HoldTime</li> <li>• Bad Length</li> <li>• Bad Peer AS</li> <li>• Bad Type</li> <li>• Conn Not Synced</li> <li>• Invalid Network Field</li> </ul> </td> <td style="vertical-align: top; width: 50%; border-left: 1px solid black; padding-left: 10px;"> <ul style="list-style-type: none"> <li>• Invalid NEXTHOP Attr</li> <li>• Invalid ORIGIN Attr</li> <li>• Malformed AS_PATH</li> <li>• Malformed Attr List</li> <li>• Missing Well Known Attr</li> <li>• None</li> <li>• Optional Attr Error</li> <li>• Unrecognized Well Known Attr</li> <li>• Unsupported Opt Param</li> <li>• Unsupported Version</li> </ul> </td> </tr> </table>	<ul style="list-style-type: none"> <li>• FSM Error</li> <li>• Hold Timer Expired</li> <li>• Message Header Error</li> </ul>	<ul style="list-style-type: none"> <li>• OPEN Message Error</li> <li>• UPDATE Message Error</li> </ul>	<ul style="list-style-type: none"> <li>• AS Routing Loop</li> <li>• Attr Flags Error</li> <li>• Attr Length Error</li> <li>• Auth Failure</li> <li>• Bad BGP Identifier</li> <li>• Bad HoldTime</li> <li>• Bad Length</li> <li>• Bad Peer AS</li> <li>• Bad Type</li> <li>• Conn Not Synced</li> <li>• Invalid Network Field</li> </ul>	<ul style="list-style-type: none"> <li>• Invalid NEXTHOP Attr</li> <li>• Invalid ORIGIN Attr</li> <li>• Malformed AS_PATH</li> <li>• Malformed Attr List</li> <li>• Missing Well Known Attr</li> <li>• None</li> <li>• Optional Attr Error</li> <li>• Unrecognized Well Known Attr</li> <li>• Unsupported Opt Param</li> <li>• Unsupported Version</li> </ul>
<ul style="list-style-type: none"> <li>• FSM Error</li> <li>• Hold Timer Expired</li> <li>• Message Header Error</li> </ul>	<ul style="list-style-type: none"> <li>• OPEN Message Error</li> <li>• UPDATE Message Error</li> </ul>				
<ul style="list-style-type: none"> <li>• AS Routing Loop</li> <li>• Attr Flags Error</li> <li>• Attr Length Error</li> <li>• Auth Failure</li> <li>• Bad BGP Identifier</li> <li>• Bad HoldTime</li> <li>• Bad Length</li> <li>• Bad Peer AS</li> <li>• Bad Type</li> <li>• Conn Not Synced</li> <li>• Invalid Network Field</li> </ul>	<ul style="list-style-type: none"> <li>• Invalid NEXTHOP Attr</li> <li>• Invalid ORIGIN Attr</li> <li>• Malformed AS_PATH</li> <li>• Malformed Attr List</li> <li>• Missing Well Known Attr</li> <li>• None</li> <li>• Optional Attr Error</li> <li>• Unrecognized Well Known Attr</li> <li>• Unsupported Opt Param</li> <li>• Unsupported Version</li> </ul>				
HOTLINKS	LACP trunk <trunk ID> and <trunk ID> formed with admin key <key>				
IP	cannot contact default gateway <IP address>				
IP	cannot contact gateway <IP address>				
IP	Dynamic Routing table is full				
IP	Route table full				

Thread	LOG_ALERT Message (continued)
MGMT	Maximum number of login failures (<threshold>) has been exceeded.
oflow	Switch is configured to function in Openflow Mode
oflow	Switch is configured to function in Normal Mode
oflow	WARNING! With Openflow enabled, Switch legacy features are restricted on Openflow ports
oflow	WARNING! Under Hybrid Mode, functionality of the following features are not supported - ACL, VNIC, VMREADY, FCOE, IPv6, IPMC-OPT, ECN
oflow	WARNING! with Openflow enabled, Switch legacy features are not supported
oflow	Openflow Instance <x> disabled
oflow	Openflow Instance <x> deleted
oflow	Openflow Instance <x>: No Controller Available for Connection
oflow	Openflow Instance <x>: Failed to receive Hello Message from Controller <y> A.B.C.D
oflow	Openflow Instance <x>: Connection stopped with Controller <y> A.B.C.D
oflow	Openflow Instance <x>: Version Negotiation Failed with Controller <y> A.B.C.D
oflow	Openflow Instance <x>: Connection established with Controller <y> A.B.C.D
oflow	Openflow Instance <x>: port <z> administratively disabled by controller
oflow	Openflow Instance <x>: port <z> administratively enabled by controller
oflow	ACL table full. Could not add MPLS pop ACL entry for Openflow Flow Table
oflow	ACL table full. Could not add MPLS push ACL entry for Openflow Flow Table
oflow	Openflow Instance <x> Maximum permitted multicast FDB flows reached
oflow	Openflow Instance <x> Maximum permitted unicast FDB flows reached
oflow	Openflow Instance <x> Maximum permitted ACL flows reached
oflow	Openflow Instance <x> Maximum permitted MPLS PUSH flows reached

Thread	LOG_ALERT Message (continued)
oflow	Openflow Instance <x> Maximum permitted MPLS POP flows reached
oflow	FDB table full. Could not add FDB entry to Openflow Flow Table
oflow	ACL table full. Could not add ACL entry for Openflow Flow Table
oflow	Openflow statistics cleared for all instances
oflow	Openflow instance <x> Openflow statistics cleared
oflow	Openflow instance <x> Memory not available. Could not modify flow entry in Openflow Flow Table
oflow	Openflow instance <x> Flow Limit reached. Could not perform Flow mod request
oflow	Openflow Instance <x>, change DPID from <0xAAAAA> to <0xBBBBB>
oflow	Memory not available. Could not add flow entry
oflow	Flow Limit reached. Could not add Flow entry to Flow Table
oflow	Openflow dynamic table cleared for all instances
oflow	Openflow dynamic table cleared for instance <x>
oflow	Openflow static table cleared for all instances
oflow	Openflow static table cleared for instance <x>
oflow	Openflow all tables cleared for all instances
oflow	Openflow all tables cleared for instance <x>
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

Thread	LOG_ALERT Message (continued)
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 is 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 <i>&lt;port&gt;</i>
CFG	ERROR: More than <i>&lt;maximum&gt;</i> 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 <i>&lt;VLAN&gt;</i> Protocol <i>&lt;protocol&gt;</i> !
DCBX	Duplicate DCBX Application Protocol Sub-TLV detected on port <i>&lt;port&gt;</i>
DCBX	Duplicate DCBX Control Sub-TLV detected on port <i>&lt;port&gt;</i>
DCBX	Duplicate DCBX PFC Sub-TLV detected on port <i>&lt;port&gt;</i>
DCBX	Duplicate DCBX PG Sub-TLV detected on port <i>&lt;port&gt;</i>
DCBX	Duplicate DCBX VNIC Sub-TLV detected on port <i>&lt;port&gt;</i>
ETS	The internal COS7 is used for stack communication; hence the ETS priority group 7 is not available.
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 Erro. 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	Invalide CRC value. Boot image rejected
MGMT	Revert Apply is issued by another user. Try later
MGMT	Revert is issued by another user. Try later.



Thread	LOG_ERR Message (continued)
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
PFC	PFC can be enabled on 2 priorities only - priority 3 and one other priority.
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.
VRP	Virtual Router Group is disabled due to no enabled virtual routers.

## LOG\_INFO

Thread	LOG_INFO Message
	System log cleared by user <i>&lt;username&gt;</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	/* Config changes at <i>&lt;time&gt;</i> by <i>&lt;username&gt;</i> */ <i>&lt;config diff&gt;</i> /* Done */
MGMT	<i>&lt;username&gt;</i> ejected from BBI
MGMT	<i>&lt;username&gt;</i> ( <i>&lt;user type&gt;</i> ) {logout   ejected   idle timeout   connection closed} from {Console   Telnet/SSH}
MGMT	<i>&lt;username&gt;</i> ( <i>&lt;user type&gt;</i> ) login {on Console   from host <i>&lt;IP address&gt;</i> }
MGMT	boot image changed
MGMT	boot kernel download completed. Now writing to flash.
MGMT	boot kernel downloaded {from host <i>&lt;hostname&gt;</i>   via browser}, filename too long to be displayed, software version <i>&lt;version&gt;</i>
MGMT	boot kernel downloaded from host <i>&lt;hostname&gt;</i> , file' <i>&lt;filename&gt;</i> ', software version <i>&lt;version&gt;</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.
MGMT	Firmware download failed to {invalid image   image1   image2   boot kernel   undefined   SP boot kernel}
MGMT	Firmware downloaded to {invalid image   image1   image2   boot kernel   undefined   SP boot kernel}.
MGMT	Flash dump successfully tftp'd to <i>&lt;hostname&gt;</i> : <i>&lt;filename&gt;</i>

Thread	LOG_INFO Message (continued)
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
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>

Thread	LOG_INFO Message (continued)
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 IBMOS 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]
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>
oflow	OpenFlow <OpenFlow ID>: Connection established with controller <1-4> <IP address>
oflow	Openflow Statistics Cleared
oflow	Openflow Flowtable Cleared
oflow	OpenFlow <OpenFlow ID>: Connection lost with controller <1-4> <IP address>
RMON	RMON {alarm   event   history} index <ID> was deleted via SNMP

Thread	LOG_INFO Message (continued)
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 adress>

## 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>
8021X	RADIUS server <IP address> auth response has an invalid VLAN id (<VLAN>) and cannot be assigned to port <port>

Thread	LOG_NOTICE Message (continued)
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"
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!

Thread	LOG_NOTICE Message (continued)
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}
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



Thread	LOG_NOTICE Message (continued)
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
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

Thread	LOG_NOTICE Message (continued)
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
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

Thread	LOG_NOTICE Message (continued)
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>
SYSTEM	BOOTP Offer (continue): Primary DNS: <IP address>, Secondary DNS: <IP address>
SYSTEM	Change fibre GIG port <port> mode to full duplex
SYSTEM	Change fibre 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

Thread	LOG_NOTICE Message (continued)
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
SYSTEM	rebooted (<reason>)[, administrator logged in]  Reason: <ul style="list-style-type: none"> <li>• Boot watchdog reset</li> <li>• console PANIC command</li> <li>• console RESET KEY</li> <li>• hard reset by SNMP</li> <li>• hard reset by WEB-UI</li> <li>• hard reset from console</li> <li>• hard reset from Telnet</li> <li>• low memory</li> <li>• MM Cycled Power Domain</li> <li>• power cycle</li> <li>• Reset Button was pushed</li> <li>• reset by SNMP</li> <li>• reset by WEB-UI</li> <li>• reset from console</li> <li>• reset from EM</li> <li>• reset from Telnet/SSH</li> <li>• scheduled reboot</li> <li>• SMS-64 found an over-voltage</li> <li>• SMS-64 found an under-voltage</li> <li>• software ASSERT</li> <li>• software PANIC</li> <li>• software VERIFY</li> <li>• Telnet PANIC command</li> <li>• unknown reason</li> <li>• watchdog timer</li> </ul>
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).
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.

Thread	LOG_NOTICE Message (continued)
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   tcpl4   udpl4   port   dport} hashing without tcpl4 or udpl4. {sip   dip   protocol   tcpl4   udpl4   port   dport} hashing will be ignored!
CFG	Configured {sip   dip   protocol   tcpl4   udpl4   port   dport} hashing without sport or dport. {sip   dip   protocol   tcpl4   udpl4   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>
ETS	ETS prohibits a PG comprising of PFC and non-PFC traffic. Mixing in the same PG different PFC settings may affect the switch functionality.
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
TEAMING	is down, but teardown is blocked



Thread	LOG_WARNING Message (continued)
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>



---

## **Appendix B. Getting help and technical assistance**

If you need help, service, or technical assistance or just want more information about IBM products, you will find a wide variety of sources available from IBM to assist you. This section contains information about where to go for additional information about IBM and IBM products, what to do if you experience a problem with your system, and whom to call for service, if it is necessary.

---

## Before you call

Before you call, make sure that you have taken these steps to try to solve the problem yourself:

- Check all cables to make sure that they are connected.
- Check the power switches to make sure that the system and any optional devices are turned on.
- Use the troubleshooting information in your system documentation, and use the diagnostic tools that come with your system. Information about diagnostic tools is in the *Problem Determination and Service Guide* on the *IBM Documentation CD* that comes with your system.
- Go to the IBM support website at <http://www.ibm.com/systems/support/> to check for technical information, hints, tips, and new device drivers or to submit a request for information.

You can solve many problems without outside assistance by following the troubleshooting procedures that IBM provides in the online help or in the documentation that is provided with your IBM product. The documentation that comes with IBM systems also describes the diagnostic tests that you can perform. Most systems, operating systems, and programs come with documentation that contains troubleshooting procedures and explanations of error messages and error codes. If you suspect a software problem, see the documentation for the operating system or program.

---

## Using the documentation

Information about your IBM system and pre-installed software, if any, or optional device is available in the documentation that comes with the product. That documentation can include printed documents, online documents, ReadMe files, and Help files. See the troubleshooting information in your system documentation for instructions for using the diagnostic programs. The troubleshooting information or the diagnostic programs might tell you that you need additional or updated device drivers or other software. IBM maintains pages on the World Wide Web where you can get the latest technical information and download device drivers and updates. To access these pages, go to <http://www.ibm.com/systems/support/> and follow the instructions. Also, some documents are available through the IBM Publications Center at <http://www.ibm.com/shop/publications/order/>.

---

## Getting help and information on the World Wide Web

On the World Wide Web, the IBM website has up-to-date information about IBM systems, optional devices, services, and support. The address for IBM System x<sup>®</sup> and xSeries<sup>®</sup> information is <http://www.ibm.com/systems/x/>. The address for IBM BladeCenter information is <http://www.ibm.com/systems/bladecenter/>. The address for IBM IntelliStation<sup>®</sup> information is <http://www.ibm.com/intellistation/>.

You can find service information for IBM systems and optional devices at <http://www.ibm.com/systems/support/>.

---

## Software service and support

Through IBM Support Line, you can get telephone assistance, for a fee, with usage, configuration, and software problems with System x and x Series servers, BladeCenter products, IntelliStation workstations, and appliances. For information about which products are supported by Support Line in your country or region, see <http://www.ibm.com/services/sl/products/>.

For more information about Support Line and other IBM services, see <http://www.ibm.com/services/>, or see <http://www.ibm.com/planetwide/> for support telephone numbers. In the U.S. and Canada, call 1-800-IBM-SERV (1-800-426-7378).

---

## Hardware service and support

You can receive hardware service through your IBM reseller or IBM Services. To locate a reseller authorized by IBM to provide warranty service, go to <http://www.ibm.com/partnerworld/> and click **Find Business Partners** on the right side of the page. For IBM support telephone numbers, see <http://www.ibm.com/planetwide/>. In the U.S. and Canada, call 1-800-IBM-SERV (1-800-426-7378).

In the U.S. and Canada, hardware service and support is available 24 hours a day, 7 days a week. In the U.K., these services are available Monday through Friday, from 9 a.m. to 6 p.m.



---

## IBM Taiwan product service

台灣 IBM 產品服務聯絡方式：  
台灣國際商業機器股份有限公司  
台北市松仁路7號3樓  
電話：0800-016-888

IBM Taiwan product service contact information:

IBM Taiwan Corporation  
3F, No 7, Song Ren Rd.  
Taipei, Taiwan  
Telephone: 0800-016-888



---

# Index

## Numerics

- 802.1p
  - ACL and TOS mapping 318
  - configuration 305
  - DSCP configuration 306
  - ETS configuration 475
  - information 103
  - priority flow control configuration 476
  - priority level 292, 312
    - IPv6 319
    - MACL 325
    - VMAP 328
  - priority value 305
  - re-marking the value 318
  - re-marking the value (IPv6) 322
- 802.1x
  - configuration 333
  - control plane protection 307
  - guest VLAN configuration 335
  - information 33
  - port configuration 336
  - RADIUS server timeout 334
  - Spanning Tree information 47

## A

- abbreviating commands (CLI) 9
- access control
  - user 284
- ACL
  - IPv6 319
  - log configuration 324
  - meter configuration 317
  - port commands 300
  - port metering 317
  - port mirroring 313
  - port re-mark configuration 318
  - re-marking (IPv6) 322, 323
  - statistics 236
- active configuration block 249, 546
- active IP interface 459
- active port
  - LACP 359
  - VLAN 459
- active switch configuration
  - gtcfg 516
  - ptcfg 515
  - restoring 516
  - saving and loading 516
- addr (IP route tag) 61
- administrator account 10
- aging (STP information) 48, 50
- asnum (attached switch number) 303
- autonomous system filter
  - action 389

- configuration 385
- configuration (display) 389
- delete 389
- disable 389
- enable 389
- path (as-path-list) 389
- path number 389

## B

- backup configuration block 546
- bandwidth allocation, Priority Groups 475
- BGP 61
  - aggregation configuration 424, 427
  - configuration 419
  - configuration mode 4
  - control plane protection 307
  - eBGP 419
  - filters, aggregation configuration 428
  - group in route 426
  - group keep-alive time 425
  - iBGP 419
  - in route 422
  - IP address, border router 421
  - keep-alive time 421
  - operations-level options 529
  - peer 419
  - peer configuration 421
  - remote autonomous system 421
  - route reflector client 421, 424
  - router hops 422, 425
  - TTL security hops 422, 425
- bgp (IP route tag) 61
- Boot Management menu 551
- Boot options 535 to 553
- bootstrap protocol 450
- Border Gateway Protocol (see BGP) 419
- bridge priority 47, 51, 53
- Bridge Protocol Data Unit (BPDU) 47, 51, 52, 53, 344
- Bridge Spanning-Tree parameters 344
- broadcast (IP route tag) 62
- broadcast (IP route type) 61

## C

- capture dump information to a file 573
- CEE configuration 474
- Cisco Ether Channel 353
- CIST information 52
- clear
  - counters for all interfaces and queues 148
  - CPU use statistics 145
  - dump information 575
  - FDB statistics 167
  - hot links statistics 167
  - IPv4 statistics 174
  - IPv6 statistics 174
  - LACP statistics 167

- MP-related statistics 145
- port statistics 145, 148
- statistics for all ports 148
- trunk group statistics 166
- vLAG statistics 171
- CLI Display 15
- command (help) 7
- commands
  - abbreviations 9
  - conventions used in this manual xiv
  - modes 3
  - shortcuts 9
  - tab completion 9
- configuration
  - commands 247 to 518
  - default gateway interval, for health checks 377
  - default gateway IP address 377
  - dump command 514
  - failover 360
  - global 3
  - IP static route 378
  - LACP 358
  - port mirroring 332
  - port trunking 353
  - RIP 391
  - save changes 249
  - switch IP address 373
  - virtualization 484
  - VLAN default (PVID) 293
  - VLAN IP interface 373
  - VLAN tagging 293
- configuration block
  - active 546
  - backup 546
  - factory 546
  - selection 546
- control plane protection (CoPP) 307
- Converged Enhanced Ethernet 474
- COS, queue information Class of Service (see COS) 103
- cost (STP information) 48, 50, 53
- CPU
  - statistics 231
  - statistics history 233
  - use 231
  - use history 233
- csnum (configured switch number) 303

## D

- daylight savings time 250
- DCB Capability Exchange Protocol 477
- DCBX
  - configuration 477
  - information 129
- debugging 555
- default gateway
  - information 58
- default gateway, interval (for health checks) 377

- default password 10
- delete
  - counters for all interfaces and queues 148
  - CPU use statistics 145
  - FDB entry 557
  - FDB statistics 167
  - hot links statistics 167
  - IPv4 statistics 174
  - IPv6 statistics 174
  - LACP statistics 167
  - MP-related statistics 145
  - port statistics 145, 148
  - statistics for all ports 148
  - trunk group statistics 166
  - vLAG statistics 171
- DHCP
  - control plane protection 307, 521
  - Snooping 473
- direct (IP route type) 61
- directed broadcasts 383
- DISC (port state) 47, 48, 50
- disconnect idle timeout 11
- downloading software 543
- DSB (port state) 50
- dump
  - configuration command 514
  - maintenance 555
- duplex mode, link status 13, 119
- dynamic routes 566

## E

- ECMP
  - hashing configuration 378
  - route information 80
- ECN (Explicit Congestion Notification) 309
- Edge Virtual Bridging, configuration 496
- Enhanced Transmission Selection (see ETS) 475
- ENode 479
- error disable and recovery
  - port 296
  - system 253
- EtherChannel, with port trunking 353
- ETS
  - configuration 475
  - Priority Group configuration 475
- EVB
  - configuration mode 6
- Explicit Congestion Notification (ECN) 309

## F

- factory configuration block 546
- failover
  - configuration 360
  - manual monitor control configuration 362
  - manual monitor port configuration 361
  - trigger configuration 361

- FCF port 479
- FCoE
  - configuration 478
  - forwarding 479
  - Initialization Protocol Snooping (see FIPS) 479
  - statistics 237
- FDB
  - delete entry 557
  - maintenance 557
  - managing information 555
  - statistics 168
- Fiber Channel over Ethernet (see FCoE) 237
- FIPS 479
- fixed (IP route tag) 61
- flag field 63
- flow control 13, 119
  - CBP discards 159
  - IBP discards 159
  - pause packets 157, 158
  - Priority-based Flow Control (PFC) 476
  - setting 297
- forwarding
  - database (see FDB) 168
  - database, delete entry 557
  - FDB maintenance 557
  - IP forwarding configuration 382
  - state (FWD) 37, 55
- Forwarding Database (see FDB) 35
- forwarding mode 540
- forwarding state
  - (FWD) 51, 52, 53
- FWD (port state) 47, 48, 50
- fwd (STP bridge option) 345
- FwdDel (forward delay), bridge port 47, 50, 51, 52, 53

## G

- gateway
  - clearing routes that use 378
  - default gateway configuration (IPv4) 377
  - IPv6 466
- getting help 603
- gtcfg (TFTP load command) 516

## H

- hardware service and support 608
- health checks
  - default gateway interval, retries 377
  - retry, number of failed health checks 377
- hello (STP information) 47, 49, 51, 52, 53
- help
  - getting 603
  - online 7
- Hot Links configuration 363
- hot-standby failover 457
- HTTPS 287

## I

- IBM support line 607
- ICMP
  - control plane protection 307, 521
  - statistics 187
- idle timeout, setting 11
- IEEE standards
  - 802.1d 338
  - 802.1x 33, 47
- IGMP
  - advanced parameters 439
  - configuration 431
  - control plane protection 307
  - information 81
  - multicast router information 84
  - querier 440
  - querier information 83
  - relay 434
  - snooping 432
  - statistics 191
- IKEv2
  - configuration mode 5
  - configuring 441
  - identification, configuring 443
  - information 94
  - preshare keys 442
  - proposal 442
- image
  - downloading 543
  - software, selecting 544
- indirect (IP route type) 61
- information commands 13 to 141
- interface change statistics 199, 203
- IP address
  - ARP information 62
  - invalid 160
  - invalid (IPv4) 178
  - invalid (IPv6) 181
- IP forwarding
  - directed broadcasts 383
  - information 58
- IP information 58, 92
- IP interface 61
  - active 459
  - address of default gateway 377
  - configuration mode 3
  - configuring address 373
  - configuring VLANs 373
  - information 58
  - IP route tag 61
  - network filter configuration 384
  - priority increment value (ifs) for VRRP 461
- IP routing
  - configuration 382
  - information 60
  - information (IPv6) 78
  - manipulation 566
  - tag parameters 61

- tags 61
- types 61
- IP Static Route commands 378
- IPMC
  - display all groups registered 175
  - group information 85
- IPsec
  - configuring 443
  - information 95
  - Layer 3 configuration 413
  - traffic selector, configuring 445
  - transform set, configuring 444
- IPv4
  - clear statistics 174
  - route statistics 184
  - statistics 178
- IPv6
  - ACL configuration 319
  - clear statistics 174
  - default gateway configuration 466
  - ND prefix configuration 469
  - Neighbor Discovery cache configuration 467
  - Neighbor Discovery configuration 375
  - Path MTU configuration 468
  - Path MTU information 91
  - re-mark configuration 322, 323
  - route information 78
  - route statistics 185
  - static route 467
  - statistics 180
- ISCLI commands
  - basics 1 to 11
  - modes 3

**L**

- LACP
  - clear statistics 167
  - configuration 358
  - control plane protection 307
  - information 38
  - interface portchannel mode 292
  - logged packet statistics 226
  - statistics 167, 168
  - vLAG information 46
- Layer 2 commands 30
- Layer 3 commands 57
- LDAP
  - configuration 264
  - server address 264
- LED, Service Required 252
- Lightweight Directory Access Protocol (see LDAP) 264
- Link Aggregation Control Protocol (see LACP) 167
- Link Flap Dampening (LFD) 254
- Link Layer Detection Protocol (see LLDP) 167
- link status 13
  - command 119
  - duplex mode 13, 119

- information 119
- port speed 13, 119
- linkt (SNMP option) 269
- LLDP
  - configuration 349
  - information 41
  - statistics 167, 170
- local (IP route type) 61
- logs
  - ACL 324
  - syslog messages 256
- loopback
  - BGP peering group 424
  - configuration mode 3
  - information 68
  - interface configuration 471
  - NTP source interface 267
  - OSPF, information 70
  - PIM interface information 98
  - RADIUS source interface, setting 258
  - setting interface number for syslogs 255
  - SNMP traps source interface 269
  - TACACS+ source interface 261
- LRN (port state) 47, 48, 50, 51, 52, 53

## M

- MAC address 14, 26, 35, 62, 557
  - multicast configuration 347
- MAC address spoof prevention 492
- Maintenance commands 555 to 576
- manual style conventions xiv
- martian
  - IP route tag (filtered) 62
  - IP route type (filtered out) 61
- MaxAge (STP information) 47, 50, 51, 52, 53
- MD5
  - cryptographic authentication 396
  - key 400
- Media Access Control address (see MAC) 35
- Miscellaneous Debug commands 558
- MLD
  - configuration mode 5
  - global configuration 429
  - global statistics 194
  - information 58, 86
  - interface configuration 430
  - Mrouter information 87
  - statistics commands 193
- monitor port 332
- MP
  - clear statistics 145
  - debug commands 558
  - display MAC address 14, 26
  - packet 223
  - packet statistics 221
  - processor statistics 221
- MST 5

- configuration mode 5
- multicast
  - MAC 347
  - router information 84
- multicast (IP route type) 61
- Multicast Listener Discovery Protocol (see MLD) 5
- mxage (STP bridge option) 344

## N

- nbr change statistics 198, 203
- Neighbor Discovery
  - cache configuration 467
  - cache manipulation (IPv6) 571
  - IPv6 375
  - prefix 469
- Network Configuration Protocol (NETCONF) 283
- notice 251
- NTP synchronization 267

## O

- OAM Discovery
  - information 45
  - statistics 171
- online help 7
- OpenFlow
  - configuration 499
  - configuration mode 5
  - information 107
    - flow allocation 108
    - flow configuration 110
    - flow tables 112
    - global configuration 107
  - static flows 507
    - actions 510
    - qualifiers 508
  - statistics 208
- Operations commands 525 to 533
- operations-level
  - BGP options 529
  - port options 526
  - VRRP options 528

## OSPF

- area index 396
- authentication key 399
- control plane protection 307
- cost of the selected path 399
- cost value of the host 403
- database information 70
- dead, declaring a silent router to be down 399
- dead, health parameter of a hello packet 401
- export 404
- fixed routes 419
- hello, authentication parameter of a hello packet 401
- host entry configuration 403
- host routes 394
- information 68, 69

- interface 394
- interface configuration 399
- link state database 394
- loopback information 70
- Not-So-Stubby Area 396
- priority value of the switch interface 399
- range number 394
- route information 72
- route redistribution configuration 404
- SPF, shortest path first 396
- stub area 396
- summary range configuration 398
- transit area 396
- transit delay 399
- type 396
- virtual link 394
- virtual link configuration 401
- virtual neighbor, router ID 401
- ospf (IP route tag) 61
- OSPFv3
  - configuration 405
  - configuration mode 4
  - dead, declaring a silent router to be down 412
  - dead, health parameter of a hello packet 415
  - hello, authentication parameter of a hello packet 415
  - interface configuration 411
  - link state database 405
  - Not-So-Stubby Area 407
  - stub area 407
  - transit area 407
  - type 407
  - virtual neighbor, router ID 415

## P

- parameters
  - tag 61
  - type 61
- passwords 10
  - administrator account 10
  - default 10
  - user access control 284
  - user account 10
- Path MTU 468
- path-cost (STP port option) 345
- PFC configuration 476
- PIM
  - component configuration 462
  - component configuration mode 5
  - component information 99
  - configuration 462
  - information 98
  - interface configuration 464
  - interface information 100
  - Mroute information 101
  - neighbor information 100
  - operational mode 463
  - statistics 206

- ping 7
- poisoned reverse, as used with split horizon 391
- port
  - 802.1x configuration 336
  - ACL meter 317
  - configuration 292
  - configuration mode 4
  - disabling (temporarily) 298
  - ECN configuration 301
  - Error Disable and Recovery 296
  - information 119
  - link configuration 297
  - membership of the VLAN 31, 56
  - mirroring
    - ACLs 313
    - configuration 332
  - number 119
  - operations-level options 526
  - priority 48, 53
  - speed 13, 119
  - states 37
  - trunking
    - configuration 353
    - description 353
  - VLAN ID 13, 119
  - WRED configuration 301
- preemption
  - assuming VRRP master routing authority 456
  - delay interval 455
  - hot links 364
  - virtual router 455
  - virtual router group 458
- Priority Flow Control 476
- Priority Groups configuration, ETS 475
- Private VLAN 370
- Protocol Independent Multicast (see PIM) 5
- protocol-based VLAN configuration 368
- ptcfg (TFTP save command) 515
- PTP
  - configuration 511
  - statistics 244
- push status, Stacking 28
- PVID (port VLAN ID) 13, 119

## R

- RADIUS
  - 802.1x server timeout 334
  - server configuration 258
  - statistics 228
  - vs TACACS+ 260
- Rapid Spanning Tree information 49
- read community string (SNMP option) 268
- receive flow control 297
- reference ports 37
- re-mark
  - ACL port re-mark menu 318
  - IPv6 ACL 322, 323

- Remonte Monitoring (see RMON) 147
- Rendezvous Point (RP) 463
- retry
  - health checks for default gateway 377
  - RADIUS server 258
- RIP 390
  - configuration 390, 391
  - control plane protection 307
  - information 61, 77
  - poisoned reverse 391
  - split horizon 391
  - version 1 parameters 391
- rip (IP route tag) 61
- RMON
  - alarm configuration 482, 523
  - alarm information 117
  - configuration 480, 518
  - event configuration 481, 520
  - event information 118
  - history 116, 143
  - history configuration 480, 518
  - information 114
  - port information 119
  - statistics 147, 161
- route map
  - autonomous system filter path configuration 389
  - configuration 385
  - configuration mode 5, 371
  - information 58, 92
  - IP access list configuration 387
  - policy-based, configuration 388
  - RIP route redistribution list 393
- route statistics
  - IPv4 184
  - IPv6 185
- router hops 422
  - BGP groups 425
- Routing Information Protocol (see RIP) 391
- RSTP informationMSTP informationRapid Spanning Tree informationMultiple Spanning Tree information 49
- Rx/Tx statistics 197, 202

## S

- save (global command) 249
- secret
  - RADIUS server 258
- Secure Shell 257
- service and support 608
- Service Required LED 252
- shortcuts (CLI) 9
- snap traces
  - buffer 558
- SNMP
  - configuration 268
  - display packets logged 228
  - options 268



- parameters, modifying 268
- statistics 145, 238
- SNMPv3
  - community table configuration 276
  - community table information 21
  - configuration 270
  - group configuration 275
  - information 17
  - notify table configuration 279
  - target address table configuration 277
  - target address table information 22
  - target parameters table configuration 278
  - view configuration 273
- software
  - image 543
  - image file and version 14, 26
  - service and support 607
- software upgrade, recovery 551
- Spanning Tree Protocol (see STP) 9
- SPAR. See Switch Partition.
- split horizon 391
- Stacking
  - boot options 535
  - configuration 303
  - information 28
  - push status 28
  - switch information 28
- state (STP information) 48, 50, 53
- static
  - IP route tag 61
  - multicast MAC configuration 347
- static route
  - add 378
  - IPv6 467
  - rem 378
- Statistics commands 145 to 245
- STG
  - root bridge 47
  - Topology Change Count 48
- STP 55
  - blocked ports information 30
  - bridge parameters 344
  - bridge priority 47, 51, 53
  - configuration 338
  - information 30, 339
  - link type 48
  - path-cost option 345
  - root bridge 51, 53, 344
  - root information 30
  - RSTP/PVRST 343
  - switch reset effect 548
- subnet
  - IP interface 373
  - performance 153
- support line 607
- support Web site 607
- switch
  - name and location 14, 26

- resetting 548
- Switch Partition (SPAR)
  - configuration 510
- system
  - contact (SNMP option) 268
  - date and time 14, 26
  - information 26
  - location (SNMP option) 268
- System Error Disable and Recovery 253
- System Information 14, 142
- System Log Messages 577 to 601
- system options
  - tnport 281

## T

- tab completion (CLI) 9
- TACACS+ 260
- TCP
  - DCBX information 134
  - ECN 301
  - header parameters 105
  - statistics 175, 189, 230
  - statistics, clearing 176
  - TACACS+ 260
  - WRED thresholds 301
- technical assistance 603
- telephone assistance 607
- telephone numbers 609
- telnet
  - configuring switches using 514
  - radius server 259, 264
- text conventions xiv
- TFTP 543
  - PUT and GET commands 515
  - server 515
- timeout
  - idle connection 11
  - radius server 258
- timers kickoff 200, 204
- trace buffer 558
- traceroute 8
- transceiver status 122
- transmit flow control 297
- trunk group information 55
- TTL security hops 422, 425
- type of area
  - OSPF 396
  - OSPFv3 407
- type parameters 61
- typographic conventions, manual xiv

## U

- UCB statistics 231
- UDLD
  - configuration 298
  - information 43

- UDP
  - statistics 190
- UniDirectional Link Detection 298
- unknown (UNK) port state 37
- Unscheduled System Dump 576
- upgrade
  - recover from failure 551
  - switch software 543
- USB Boot 542
- USB Copy 517
- USB drive 517, 542
- user access control configuration 284
- user account 10
- uuencode flash dump 573

## V

- Virtual Link Aggregation Control Protocol (see vLAG) 30
- virtual router
  - description 454
  - group configuration 457
  - group priority tracking 459
  - increasing priority level of 456
  - priority increment values for VRRP 461
  - tracking criteria 456
- Virtual Router Redundancy Protocol (see VRRP) 5
- virtualization
  - configuration options 484
  - information 122
- vLAG
  - clear statistics 171
  - configuration 356
  - control plane protection 307
  - information 30
- VLAN
  - active port 459
  - ARP entry information 62
  - configuration 366
  - configuration mode 4
  - information 56
  - name 31, 56
  - port membership 31, 56
  - protocol-based, configuration 368
  - setting access VLAN 293
  - setting default number (PVID) 293
  - tagging 13, 119
    - port configuration 293
    - port restrictions 367
  - VLAN Number 56
- VM
  - bandwidth management 485
  - Distributed Virtual Switch 532
  - Edge Virtual Bridge configuration 496
  - group configuration 489
  - information 122
  - policy configuration 485
  - profile configuration 493
  - VMready configuration 495

- VMware
  - configuration 494
  - dvSwitch operations 532, 533
  - information 123
  - operations 530
- vNIC
  - configuration 486
  - group configuration 487
  - information 126
- VRRP 88
  - authentication parameters for IP interfaces 460
  - configuration 453
  - configuration mode 5
  - control plane protection 307
  - information 88
  - interface configuration 460
  - master advertisements 455
  - master advertisements, time interval 458
  - operations-level options 528
  - priority tracking options 421, 428, 456
  - statistics 205
  - tracking configuration 461
  - weights for priority levels 461
- VSI
  - configuration mode 6

## W

- watchdog timer 555
- Web site
  - ordering publications 605
  - support 607
  - telephone support numbers 608
- Weighted Random Early Detection (see WRED) 309
- WRED
  - configuration 309
  - transmit queue configuration 301, 310
- write community string (SNMP option) 269