

BLADEOS™

ISCLI Reference

1/10Gb Uplink Ethernet Switch Module for IBM BladeCenter®

Version 6.3

Part Number: BMD00176, April 2010

BLADE
NETWORK TECHNOLOGIES

2350 Mission College Blvd.
Suite 600
Santa Clara, CA 95054
www.bladenetwork.net

Copyright © 2010 BLADE Network Technologies, Inc., 2350 Mission College Blvd., Suite 600, Santa Clara, California, 95054, USA. All rights reserved. Part Number: BMD00176.

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

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

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

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

Originated in the USA.

Contents

Preface ■ 13

- Who Should Use This Book ■ 13
- How This Book Is Organized ■ 13
- Typographic Conventions ■ 14
- How to Get Help ■ 16

Chapter 1: ISCLI Basics ■ 17

- Accessing the ISCLI ■ 17
- ISCLI Command Modes ■ 18
- Global Commands ■ 21
- Command Line Interface Shortcuts ■ 23
 - CLI List and Range Inputs ■ 23
 - Command Abbreviation ■ 24
 - Tab Completion ■ 24
- User Access Levels ■ 24
- Idle Timeout ■ 25

Chapter 2: Information Commands ■ 27

- System Information ■ 29
 - SNMPv3 System Information ■ 31
 - SNMPv3 USM User Table Information ■ 33
 - SNMPv3 View Table Information ■ 34
 - SNMPv3 Access Table Information ■ 35
 - SNMPv3 Group Table Information ■ 36
 - SNMPv3 Community Table Information ■ 37
 - SNMPv3 Target Address Table Information ■ 38
 - SNMPv3 Target Parameters Table Information ■ 39
 - SNMPv3 Notify Table Information ■ 40
 - SNMPv3 Dump Information ■ 41
 - General System Information ■ 42

Show Recent Syslog Messages	■	44
User Status	■	45
Stacking Information	■	46
Stacking Switch Information	■	48
Layer 2 Information	■	49
AMP Information	■	51
Show AMP Global Information	■	52
Show AMP Group Information	■	53
FDB Information	■	54
Show All FDB Information	■	55
Clearing Entries from the Forwarding Database	■	55
Link Aggregation Control Protocol Information	■	56
Link Aggregation Control Protocol	■	57
Layer 2 Failover Information	■	58
Layer 2 Failover Information	■	59
Hot Links Information	■	60
LLDP Information	■	61
LLDP Remote Device Information	■	62
Unidirectional Link Detection Information	■	63
UDLD Port Information	■	63
OAM Discovery Information	■	64
OAM Port Information	■	64
802.1X Information	■	65
Spanning Tree Information	■	67
RSTP/MSTP/PVRST Information	■	70
Common Internal Spanning Tree Information	■	73
Trunk Group Information	■	75
VLAN Information	■	76
Layer 3 Information	■	78
IP Routing Information	■	80
Show All IP Route Information	■	81
ARP Information	■	83
Show All ARP Entry Information	■	84
ARP Address List Information	■	84
BGP Information	■	85
BGP Peer information	■	86
BGP Summary information	■	86
Dump BGP Information	■	87

OSPF Information	■ 87
OSPF General Information	■ 89
OSPF Interface Information	■ 90
OSPF Database Information	■ 90
OSPF Information Route Codes	■ 92
OSPFv3 Information	■ 93
OSPFv3 Information Dump	■ 95
OSPFv3 Interface Information	■ 96
OSPFv3 Database Information	■ 97
OSPFv3 Route Codes Information	■ 98
Routing Information Protocol	■ 99
RIP Routes Information	■ 99
RIP Interface Information	■ 100
IPv6 Routing Information	■ 101
IPv6 Routing Table	■ 101
IPv6 Neighbor Discovery Cache Information	■ 102
IPv6 Neighbor Discovery Cache Information	■ 102
Interface Information	■ 103
IP Information	■ 104
IGMP Multicast Group Information	■ 105
IGMP Group Information	■ 107
IGMP Multicast Router Information	■ 108
VRRP Information	■ 109
Quality of Service Information	■ 110
802.1p Information	■ 111
Access Control List Information Commands	■ 112
Access Control List Information	■ 113
RMON Information Commands	■ 114
RMON History Information	■ 115
RMON Alarm Information	■ 116
RMON Event Information	■ 118
Link Status Information	■ 119
Port Information	■ 120
Port Transceiver Status	■ 121
Virtual Machines Information	■ 122
VM Information	■ 122
VMware Information	■ 123
VMware Host Information	■ 124
Information Dump	■ 124

Chapter 3: Statistics Commands ■ 125**Port Statistics ■ 126**

802.1X Authenticator Statistics ■ 128

802.1X Authenticator Diagnostics ■ 129

Active MultiPath Statistics ■ 132

Bridging Statistics ■ 133

Ethernet Statistics ■ 134

Interface Statistics ■ 137

Interface Protocol Statistics ■ 140

Link Statistics ■ 140

RMON Statistics ■ 141

Layer 2 Statistics ■ 144

Active MultiPath Statistics ■ 145

Active MultiPath Group Statistics ■ 146

FDB Statistics ■ 147

LACP Statistics ■ 148

Hotlinks Statistics ■ 149

LLDP Port Statistics ■ 150

OAM Statistics ■ 151

Layer 3 Statistics ■ 152

IPv4 Statistics ■ 156

IPv6 Statistics ■ 159

Route Statistics ■ 164

ARP statistics ■ 164

DNS Statistics ■ 165

ICMP Statistics ■ 166

TCP Statistics ■ 168

UDP Statistics ■ 170

IGMP Statistics ■ 171

OSPF Statistics ■ 172

OSPF Global Statistics ■ 173

OSPFv3 Statistics ■ 178

OSPFv3 Global Statistics ■ 179

VRRP Statistics ■ 183

Routing Information Protocol Statistics ■ 184

Management Processor Statistics ■ 185

MP Packet Statistics ■ 186

TCP Statistics ■ 188

UDP Statistics ■ 188

CPU Statistics	■	189
Access Control List Statistics	■	190
ACL Statistics	■	190
VMAP Statistics	■	191
SNMP Statistics	■	192
NTP Statistics	■	196
Statistics Dump	■	197
Chapter 4: Configuration Commands	■	199
Viewing and Saving Changes	■	200
System Configuration	■	201
System Error Disable and Recovery Configuration	■	203
System Host Log Configuration	■	204
SSH Server Configuration	■	205
RADIUS Server Configuration	■	207
TACACS+ Server Configuration	■	209
LDAP Server Configuration	■	213
NTP Server Configuration	■	215
System SNMP Configuration	■	217
SNMPv3 Configuration	■	219
User Security Model Configuration	■	221
SNMPv3 View Configuration	■	222
View-based Access Control Model Configuration	■	224
SNMPv3 Group Configuration	■	226
SNMPv3 Community Table Configuration	■	227
SNMPv3 Target Address Table Configuration	■	228
SNMPv3 Target Parameters Table Configuration	■	229
SNMPv3 Notify Table Configuration	■	231
System Access Configuration	■	232
Management Network Configuration	■	233
User Access Control Configuration	■	234
System User ID Configuration	■	235
Strong Password Configuration	■	236
HTTPS Access Configuration	■	238
Custom Daylight Savings Time Configuration	■	239
sFlow Configuration	■	240
sFlow Port Configuration	■	241

Port Configuration	242
Port Error Disable and Recovery Configuration	245
Port Link Configuration	245
Temporarily Disabling a Port	247
UniDirectional Link Detection Configuration	247
Port OAM Configuration	248
Port ACL Configuration	248
Port Spanning Tree Configuration	250
Stacking Configuration	251
Stacking Switch Configuration	252
Quality of Service Configuration	253
802.1p Configuration	253
DSCP Configuration	254
Access Control Configuration	255
Access Control List Configuration	256
Ethernet Filtering Configuration	257
IPv4 Filtering Configuration	258
TCP/UDP Filtering Configuration	260
Packet Format Filtering Configuration	261
VMAP Configuration	263
ACL Group Configuration	264
ACL Metering Configuration	264
ACL Re-Mark Configuration	266
Re-marking In-Profile Configuration	267
Re-Marking Out-of-Profile Configuration	267
Port Mirroring	268
Port-Mirroring Configuration	269
Layer 2 Configuration	270
802.1X Configuration	271
802.1X Global Configuration	272
802.1X Guest VLAN Configuration	274
802.1X Port Configuration	275
Active MultiPath Protocol Configuration	277
RSTP/MSTP/PVRST Configuration	281
Common Internal Spanning Tree Configuration	282
CIST Bridge Configuration	283
CIST Port Configuration	284
Spanning Tree Configuration	286
Bridge Spanning Tree Configuration	287
Spanning Tree Port Configuration	288

Forwarding Database Configuration	■	290
Static FDB Configuration	■	291
Static Multicast MAC Configuration	■	292
LLDP Configuration	■	293
LLDP Port Configuration	■	295
LLDP Optional TLV configuration	■	295
Trunk Configuration	■	297
IP Trunk Hash Configuration	■	299
IP Trunk Hash Parameters	■	299
Link Aggregation Control Protocol Configuration	■	301
LACP Port Configuration	■	302
Layer 2 Failover Configuration	■	303
Failover Trigger Configuration	■	304
Auto Monitor Configuration	■	305
Failover Manual Monitor Port Configuration	■	305
Failover Manual Monitor Control Configuration	■	307
Hot Links Configuration	■	308
Hot Links Trigger Configuration	■	309
Hot Links Master Configuration	■	310
Hot Links Backup Configuration	■	311
VLAN Configuration	■	312
Protocol-Based VLAN Configuration	■	314
Private VLAN Configuration	■	316
Layer 3 Configuration	■	318
IP Interface Configuration	■	320
IPv6 Neighbor Discovery Configuration	■	322
Default Gateway Configuration	■	324
IPv4 Static Route Configuration	■	325
IP Multicast Route Configuration	■	326
ARP Configuration	■	328
ARP Static Configuration	■	328
IP Forwarding Configuration	■	329
Network Filter Configuration	■	330
Routing Map Configuration	■	331
IP Access List Configuration	■	333
Autonomous System Filter Path Configuration	■	334
Routing Information Protocol Configuration	■	335
Routing Information Protocol Interface Configuration	■	336
RIP Route Redistribution Configuration	■	338

Open Shortest Path First Configuration	339
Area Index Configuration	341
OSPF Summary Range Configuration	343
OSPF Interface Configuration	344
OSPF Virtual Link Configuration	346
OSPF Host Entry Configuration	348
OSPF Route Redistribution Configuration.	349
OSPF MD5 Key Configuration	350
Border Gateway Protocol Configuration	351
BGP Peer Configuration	352
BGP Redistribution Configuration	355
BGP Aggregation Configuration	356
IGMP Configuration	357
IGMP Snooping Configuration	358
IGMPv3 Configuration	359
IGMP Relay Configuration	360
IGMP Relay Multicast Router Configuration	361
IGMP Static Multicast Router Configuration	362
IGMP Filtering Configuration	363
IGMP Filter Definition	364
IGMP Filtering Port Configuration	365
IGMP Advanced Configuration	365
Domain Name System Configuration	367
Bootstrap Protocol Relay Configuration	368
VRRP Configuration	369
Virtual Router Configuration	370
Virtual Router Priority Tracking Configuration	372
Virtual Router Group Configuration	374
Virtual Router Group Priority Tracking Configuration	376
VRRP Interface Configuration	377
VRRP Tracking Configuration	378
IPv6 Default Gateway Configuration	379
IPv6 Static Route Configuration	380
IPv6 Neighbor Discovery Cache Configuration	381
Open Shortest Path First Version 3 Configuration	382
OSPFv3 Area Index Configuration	384
OSPFv3 Summary Range Configuration	386
OSPFv3 AS-External Range Configuration	387
OSPFv3 Interface Configuration	388
OSPFv3 Virtual Link Configuration	390

OSPFv3 Host Entry Configuration	■ 392
IP Loopback Interface Configuration	■ 394
RMON History Configuration	■ 396
RMON Event Configuration	■ 397
RMON Alarm Configuration	■ 398
Virtualization Configuration	■ 400
VM Group Configuration	■ 402
VM Profile Configuration	■ 404
VM Ware Configuration	■ 406
Configuration Dump	■ 407
Saving the Active Switch Configuration	■ 407
Restoring the Active Switch Configuration	■ 408

Chapter 5: Operations Commands ■ 409

Operations-Level Port Commands	■ 410
Operations-Level Port 802.1X Commands	■ 411
Operations-Level VRRP Commands	■ 412
Operations-Level BGP Commands	■ 412
Protected Mode Options	■ 413
VMware Operations	■ 414

Chapter 6: Boot Options ■ 417

Stacking Boot Options	■ 417
Scheduled Reboot	■ 420
Netboot Configuration	■ 420
Updating the Switch Software Image	■ 422
Loading New Software to Your Switch	■ 422
Selecting a Software Image to Run	■ 423
Uploading a Software Image from Your Switch	■ 424
Selecting a Configuration Block	■ 425
Resetting the Switch	■ 425
Accessing the BLADEOS CLI	■ 426
Using the Boot Management Menu	■ 427
Recovering from a Failed Upgrade	■ 427

Chapter 7: Maintenance Commands ■ 431

Forwarding Database Maintenance	■ 432
Debugging Commands	■ 433
ARP Cache Maintenance	■ 435

IP Route Manipulation	■	436
LLDP Cache Manipulation	■	437
IGMP Groups Maintenance	■	438
IGMP Multicast Routers Maintenance	■	439
IPv6 Neighbor Discovery Cache Manipulation	■	440
IPv6 Route Maintenance	■	441
Uuencode Flash Dump	■	441
TFTP or FTP System Dump Put	■	442
Clearing Dump Information	■	442
Unscheduled System Dumps	■	443
Index	■	445

Preface

The *BLADEOS 6.3 ISCLI Reference* describes how to configure and use the BLADE OS 6.3 software with your 1/10Gb Uplink Ethernet Switch Module. 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 GbESM. For details about the configuration and operation of the GbESM, see the *BLADE OS 6.3 Application Guide*.

Who Should Use This Book

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

How This Book Is Organized

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

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

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

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

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

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

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

“[Index](#)” includes pointers to the description of the key words used throughout the book.

Typographic Conventions

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

Table 1 Typographic Conventions

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

Table 1 Typographic Conventions

Typeface or Symbol	Meaning
braces { }	<p>Indicate required elements in syntax descriptions where there is more than one option. You must choose only one of the options. Do not type the braces when entering the command.</p> <p>Example: If the command syntax is show portchannel {<I-16> hash information}</p> <p>you enter:</p> <p>show portchannel <I-16></p> <p>or</p> <p>show portchannel hash</p> <p>or</p> <p>show portchannel information</p>
brackets []	<p>Indicate optional elements in syntax descriptions. Do not type the brackets when entering the command.</p> <p>Example: If the command syntax is show ip interface [<I-128>]</p> <p>you enter</p> <p>show ip interface</p> <p>or</p> <p>show ip interface <I-128></p>

Table 1 Typographic Conventions

Typeface or Symbol	Meaning
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</p> <pre>show portchannel {<1-16> hash information}</pre> <p>you must enter:</p> <pre>show portchannel <1-16></pre> <p>or</p> <pre>show portchannel hash</pre> <p>or</p> <pre>show portchannel information</pre>

How to Get Help

If you need help, service, or technical assistance, see the “Getting help and technical assistance” appendix in the *1/10Gb Uplink Ethernet Switch Module Installation Guide*.

CHAPTER 1

ISCLI Basics

Your 1/10Gb Uplink ESM (GbESM) 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 GbESM.

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

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

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

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

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

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

ISCLI Command Modes

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

- **User EXEC mode**
This is the initial mode of access. By default, password checking is disabled for this mode, on console.
- **Privileged EXEC mode**
This mode is accessed from User EXEC mode. This mode can be accessed using the following command: **enable**
- **Global Configuration mode**
This mode allows you to make changes to the running configuration. If you save the configuration, the settings survive a reload of the GbESM. Several sub-modes can be accessed from the Global Configuration mode. For more details, see [Table 2](#).

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

[Table 2](#) lists the ISCLI command modes.

Table 2 ISCLI Command Modes

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

Table 2 ISCLI Command Modes

Command Mode/Prompt	Command used to enter or exit
Interface Loopback Router (config-ip-loopback) #	Enter Interface Loopback Configuration mode, from Global Configuration mode: interface ip loopback <1-5> Exit to Global Configuration mode: exit Exit to Privileged EXEC mode: end
Interface Port Router (config-if) #	Enter Port Configuration mode, from Global Configuration mode: interface port <port number or alias> Exit to Privileged EXEC mode: exit Exit to Global Configuration mode: end
VLAN Router (config-vlan) #	Enter VLAN Configuration mode, from Global Configuration mode: vlan <VLAN number> Exit to Global Configuration mode: exit Exit to Privileged EXEC mode: end
Router OSPF Router (config-router-ospf) #	Enter OSPF Configuration mode, from Global Configuration mode: router ospf Exit to Global Configuration mode: exit Exit to Privileged EXEC mode: end
Router OSPFv3 Router (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 Router (config-router-bgp) #	Enter BGP Configuration mode, from Global Configuration mode: router bgp Exit to Global Configuration mode: exit Exit to Privileged EXEC mode: end
Router RIP Router (config-router-rip) #	Enter RIP Configuration mode, from Global Configuration mode: router rip Exit to Global Configuration mode: exit Exit to Privileged EXEC mode: end

Table 2 ISCLI Command Modes

Command Mode/Prompt	Command used to enter or exit
Route Map Router (config-route-map) #	Enter Route Map Configuration mode, from Global Configuration mode: route-map <1-32> Exit to Global Configuration mode: exit Exit to Privileged EXEC mode: end
Router VRRP Router (config-vrrp) #	Enter VRRP Configuration mode, from Global Configuration mode: router vrrp Exit to Global Configuration mode: exit Exit to Privileged EXEC mode: end

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.

Table 3 Description of Global Commands

Command	Action
ping	<p>Use this command to verify station-to-station connectivity across the network. The format is as follows:</p> <pre>ping <host name> <IP address> [-n <tries (0-4294967295)>] [-w <msec delay (0-4294967295)>] [-l <length (0/32-65500/2080)>] [-s <IP source>] [-v <tos (0-255)>] [-f] [-t]</pre> <p>Where:</p> <ul style="list-style-type: none"> □ -n: Sets the number of attempts (optional). □ -w: Sets the number of milliseconds between attempts (optional). □ -l: Sets the ping request payload size (optional). □ -s: Sets the IP source address for the IP packet (optional). □ -v: Sets the Type Of Service bits in the IP header. □ -f: Sets the <i>don't fragment</i> bit in the IP header (only for IPv4 addresses). □ -t: Pings continuously (same as -n 0). <p>Where the <i>IP address</i> or <i>hostname</i> specify the target device. Use of a hostname requires DNS parameters to be configured on the switch.</p> <p><i>Tries</i> (optional) is the number of attempts (1-32), and <i>msec delay</i> (optional) is the number of milliseconds between attempts.</p>
tracert	<p>Use this command to identify the route used for station-to-station connectivity across the network. The format is as follows:</p> <pre>tracert {<hostname> <IP address>} [<max-hops (1-32)>] [<msec delay>]</pre> <pre>tracert <hostname> <IP address> [<max-hops (1-32)>] [<msec-delay (1-4294967295)>]</pre> <p>Where <i>hostname/IP address</i> is the hostname or IP address of the target station, <i>max-hops</i> (optional) is the maximum distance to trace (1-32 devices), and <i>msec-delay</i> (optional) is the number of milliseconds to wait for the response.</p> <p>As with ping, the DNS parameters must be configured if specifying hostnames.</p>

Table 3 Description of Global Commands

Command	Action
telnet	<p>This command is used to form a Telnet session between the switch and another network device. The format is as follows:</p> <pre>telnet {<hostname> <IP address>} [<port>]</pre> <p>Where <i>IP address</i> or <i>hostname</i> specifies the target station. Use of a hostname requires DNS parameters to be configured on the switch.</p> <p><i>Port</i> is the logical Telnet port or service number.</p>
show history	This command displays the last ten issued commands.
show who	Displays a list of users who are currently logged in.

Command Line Interface Shortcuts

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

CLI List and Range Inputs

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

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

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

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

Do not use spaces within list and range specifications.

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

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

Note – Port ranges accept only port numbers, not aliases such as INT1 or EXT1.

Command Abbreviation

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

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

Tab Completion

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

User Access Levels

To enable better switch management and user accountability, three levels or *classes* of user access have been implemented on the GbESM. 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 GbESM. 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 GbESM. 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 GbESM. 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 1/10Gb Uplink ESM, including the ability to change both the user and administrator passwords.	admin

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

Idle Timeout

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

system idle <1-60>

Command mode: Global Configuration

CHAPTER 2

Information Commands

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

Table 5 Information Commands

Command Syntax and Usage

show interface link

Displays configuration information about each port, including:

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

Command mode: All

For details, see [page 119](#).

Table 5 Information Commands (continued)

Command Syntax and Usage

show interface information

Displays port status information, including:

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

Command mode: All

For details, see [page 120](#).

show transceiver

Displays the status of the port transceiver module on each external port.

Command mode: All

For details, see [page 121](#).

show information-dump

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

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

Command mode: All

System Information

The information provided by each command option is briefly described in [Table 6 on page 29](#), with pointers to where detailed information can be found.

Table 6 System Information Commands

Command Syntax and Usage

show sys-info

Displays system information, including:

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

Command mode: All

For details, see [page 42](#).

show logging messages

Displays most recent syslog messages.

Command mode: All

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

show access user

Displays configured user names and their status.

Command mode: All except User EXEC

Error Disable and Recovery Information

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

Table 7 Error Disable Information Options

Command Syntax and Usage	
show errdisable recovery	Displays a list ports with their Error Recovery status.
show errdisable timers	Displays a list of active recovery timers, if applicable.
show errdisable information	Displays all Error Disable and Recovery information.

SNMPv3 System Information

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

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

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

Table 8 SNMPv3 commands

Command Syntax and Usage

show snmp-server v3 user

Displays User Security Model (USM) table information.

Command mode: All

To view the table, see [page 33](#).

show snmp-server v3 view

Displays information about view, subtrees, mask and type of view.

Command mode: All

To view a sample, see [page 34](#).

show snmp-server v3 access

Displays View-based Access Control information.

Command mode: All

To view a sample, see [page 35](#).

show snmp-server v3 group

Displays information about the group, including the security model, user name, and group name.

Command mode: All

To view a sample, see [page 36](#).

Table 8 SNMPv3 commands (continued)

Command Syntax and Usage

show snmp-server v3 community

Displays information about the community table information.

Command mode: All

To view a sample, see [page 37](#).

show snmp-server v3 target-address

Displays the Target Address table information.

Command mode: All

To view a sample, see [page 38](#).

show snmp-server v3 target-parameters

Displays the Target parameters table information.

Command mode: All

To view a sample, see [page 39](#).

show snmp-server v3 notify

Displays the Notify table information.

Command mode: All

To view a sample, see [page 40](#).

show snmp-server v3

Displays all the SNMPv3 information.

Command mode: All

To view a sample, see [page 41](#).

SNMPv3 USM User Table Information

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

show snmp-server v3 user

Command mode: All

The USM user table contains the following information:

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

usmUser Table:

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

Table 9 USM User Table Information Parameters

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

SNMPv3 View Table Information

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

The following command displays the SNMPv3 View Table:

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

Command mode: All

View Name	Subtree	Mask	Type
-----	-----	-----	-----
iso	1.3		included
v1v2only	1.3		included
v1v2only	1.3.6.1.6.3.15		excluded
v1v2only	1.3.6.1.6.3.16		excluded
v1v2only	1.3.6.1.6.3.18		excluded

Table 10 SNMPv3 View Table Information Parameters

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

SNMPv3 Access Table Information

The access control sub system provides authorization services.

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

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

The following command displays SNMPv3 access information:

show snmp-server v3 access

Command mode: All

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

Table 11 SNMPv3 Access Table Information

Field	Description
Group Name	Displays the name of group.
Prefix	Displays the prefix that is configured to match the values.
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, noAuthNoPriv, authNoPriv, or authPriv.
Match	Displays the match for the contextName. The options are: exact and prefix.
ReadV	Displays the MIB view to which this entry authorizes the read access.
WriteV	Displays the MIB view to which this entry authorizes the write access.
NotifyV	Displays the Notify view to which this entry authorizes the notify access.

SNMPv3 Group Table Information

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

The following command displays SNMPv3 group information:

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

Command mode: All

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

Table 12 SNMPv3 Group Table Information Parameters

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

SNMPv3 Community Table Information

This command displays the community table information stored in the SNMP engine.

The following command displays SNMPv3 community information:

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

Command mode: All

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

Table 13 SNMPv3 Community Table Information Parameters

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

SNMPv3 Target Address Table Information

The following command displays SNMPv3 target address information:

show snmp-server v3 target-address

Command mode: All

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

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

Table 14 SNMPv3 Target Address Table Information Parameters

Field	Description
Name	Displays the locally arbitrary, but unique identifier associated with this snmpTargetAddrEntry.
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 snmpTargetParamsTable. The identified entry contains SNMP parameters to be used when generating messages to be sent to this transport address.

SNMPv3 Target Parameters Table Information

The following command displays SNMPv3 target parameters information:

show snmp-server v3 target-parameters

Command mode: All

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

Table 15 SNMPv3 Target Parameters Table Information

Field	Description
Name	Displays the locally arbitrary, but unique identifier associated with this snmpTargeParamsEntry.
MP Model	Displays the Message Processing Model used when generating SNMP messages using this entry.
User Name	Displays the securityName, 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 inconsistentValue error if an attempt is made to set this variable to a value for a security model which the system does not support.
Sec Level	Displays the level of security used when generating SNMP messages using this entry.

SNMPv3 Notify Table Information

The following command displays the SNMPv3 Notify Table:

show snmp-server v3 notify

Command mode: All

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

Table 16 SNMPv3 Notify Table Information

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

SNMPv3 Dump Information

The following command displays SNMPv3 information:

show snmp-server v3

Command mode: All

```

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

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

vacmViewTreeFamily Table:
View Name Subtree Mask Type
-----
iso        1.3 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        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 0:16:42 Wed Jan 3, 2010
Time zone: America/US/Pacific
Daylight Savings Time Status: Disabled

1/10Gb Uplink Ethernet Switch Module

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

MAC address: 00:11:58:ad:a3:00 Management IP Address (if 128):
10.90.90.97
Software Version 6.3.0 (FLASH image1), factory default configuration.

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

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

Switch is in I/O Module Bay 1
```

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

System information includes:

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

Show Recent Syslog Messages

The following command displays system log messages:

show logging messages

Command mode: All

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

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

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

User Status

The following command displays user status information:

show access user

Command mode: All except User EXEC

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

This command displays the status of the configured usernames.

Stacking Information

Table 17 lists the Stacking information options.

Table 17 Stacking information Options

Command Syntax and Usage

show stack switch

Displays information about each switch in the stack, including:

- ☐ Configured Switch Number (csnum)
- ☐ Attached Switch Number (asnum)
- ☐ MAC address
- ☐ Stacking state

Command mode: All

show stack link

Displays link information for each switch in the stack, listed by assigned switch number.

Command mode: All

show stack name

Displays the name of the stack.

Command mode: All

show stack backup

Displays the unit number of the backup switch.

Command mode: All

show stack version

Displays the firmware version number for the selected switch.

Command mode: All

show stack path-map

Displays the Stacking packet path map that shows how the stack switches are connected.

Command mode: All

Table 17 Stacking information Options

Command Syntax and Usage

show stack push-status

Displays the status of the most recent firmware and configuration file push from the master to member switches.

Command mode: All

show stack dynamic

Displays all stacking information.

Command mode: All

Stacking Switch Information

The following command displays Stacking switch information:

show stack switch

Command mode: All

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

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

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

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

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

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

Stack switch information includes the following:

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

Layer 2 Information

Table 18 Layer 2 Information Commands

Command Syntax and Usage

show dot1x information

Displays 802.1X Information.

Command mode: All

For details, see [page 65](#).

show spanning-tree

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

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

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

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

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

Command mode: All

show spanning-tree stp <1-128> information

Displays information about a specific Spanning Tree Group.

Command mode: All

For details, see [page 67](#).

Table 18 Layer 2 Information Commands (continued)

Command Syntax and Usage

show spanning-tree mstp cist information

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

CIST bridge information includes:

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

CIST port information includes:

- ☐ Port number and priority
- ☐ Cost
- ☐ State

Command mode: All

For details, see [page 73](#).

show portchannel information

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

Command mode: All

For details, see [page 75](#).

show vlan

Displays VLAN configuration information for all configured VLANs, including:

- ☐ VLAN Number
- ☐ VLAN Name
- ☐ Status
- ☐ Port membership of the VLAN
- ☐ VLAN management status

Command mode: All

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

Table 18 Layer 2 Information Commands (continued)

Command Syntax and Usage

show failover trigger <1-8>

Displays Layer 2 Failover information.

Command mode: AllFor details, see [page 58](#).

show hotlinks information

Displays Hot Links information.

Command mode: AllFor details, see [page 60](#).

show layer2 information

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

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

Command mode: All

AMP Information

Use these commands to display Active MultiPath Protocol (AMP) information for the switch.

Table 19 AMP Information Commands

Command Syntax and Usage

show active-multipath information

Displays global Active MultiPath (AMP) information.

Command mode: All

show active-multipath group [*<AMP group number>*] **information**

Displays AMP group information.

Command mode: All

Show AMP Global Information

The following command displays global Active MultiPath (AMP) information:

show active-multipath information

Command mode: All

```
Active Multipath Protocol: enabled
  Protocol version      : 2
  Switch id             : 00:22:00:ee:cd:00
  Switch type           : aggregator
  Switch priority       : 100
  Packet interval       : 50 centiseconds
  Timeout count         : 4
  Aggr. precedence     : 1
  Aggr. link            : PoCh 2 (Ports 12 13)
  No. of groups         : 3

Group  State  Ports
-----
1      up    PoCh 1
2      up    PoCh 13 [LACP 100]
3      up    21

Port   State  PoCh
-----
1      fwd   1
2      fwd   1
12     fwd   2
13     fwd   2
17     fwd   13
18     fwd   13
21     fwd
```

This displays show global AMP information for an AMP aggregator switch. AMP global information includes the following:

- Active MultiPath Protocol information:
 - ☐ AMP status (enabled or disabled)
 - ☐ Protocol version
 - ☐ Switch ID (MAC address)
 - ☐ Switch type (access or aggregator)
 - ☐ Priority
 - ☐ Interval between AMP keep-alive packets
 - ☐ Timeout count
 - ☐ Aggregator precedence (1 or 2)

- ❑ Aggregator links
- ❑ Number of active (enabled) AMP groups
- Group information
 - ❑ Group number
 - ❑ Group state (up or DOWN)
 - ❑ Ports/portchannels in the group
- Link information
 - ❑ Port number
 - ❑ State (fwd, BLOCK, or DOWN)
 - ❑ Portchannel (trunk) number

Show AMP Group Information

The following command displays Active MultiPath (AMP) Group information:

show active-multipath group [*<AMP group number>*] **information**

Command mode: All

```
Group 3: enabled, topology UP
  Port 10: access
    State : forwarding
    Peer  : 00:22:00:ac:d7:00
            aggregator, priority 100
  Port 11: access
    State : forwarding
    Peer  : 00:25:03:49:82:00
            aggregator, priority 1
```

This display shows AMP group information for an AMP access switch. AMP group information includes the following:

- AMP group number and topology status (UP or DOWN)
- AMP link 1:
 - ❑ Switch type (access/aggregator)
 - ❑ State (forwarding, BLOCKING, or DOWN)
 - ❑ Peer information (MAC address, switch type, AMP priority)
- AMP link 2:
 - ❑ Switch type (access/aggregator)
 - ❑ State (forwarding, BLOCKING, or DOWN)
 - ❑ Peer information (MAC address, switch type, AMP priority)

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 16K MAC address entries on the MP per switch.

Table 20 FDB Information Commands

Command Syntax and Usage

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

Displays a single database entry by its MAC address. You are prompted to enter the MAC address of the device. Enter the MAC address using the format, `xx:xx:xx:xx:xx:xx`. For example, `08:00:20:12:34:56`

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

Command mode: All

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

Displays all FDB entries for a particular port.

Command mode: All

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

Displays all FDB entries on a single VLAN.

Command mode: All

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

Displays all FDB entries for a particular state.

Command mode: All

Table 20 FDB Information Commands (continued)**Command Syntax and Usage****show mac-address-table multicast**

Displays all Multicast MAC entries in the FDB.

Command mode: All

show mac-address-table

Displays all entries in the Forwarding Database.

Command mode: All

For more information, see [page 55](#).

Show All FDB Information

The following command displays Forwarding Database information:

show mac-address-table

Command mode: All

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

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

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

Clearing Entries from the Forwarding Database

To clear the entire FDB, refer to “[Forwarding Database Maintenance](#)” on [page 432](#).

Link Aggregation Control Protocol Information

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

Table 21 LACP Information Commands

Command Syntax and Usage
show lacp aggregator <i><port alias or number></i>
Displays detailed information about the LACP aggregator used by the selected port.
Command mode: All
show interface port <i><port alias or number></i> lacp information
Displays LACP information about the selected port.
Command mode: All
show lacp information
Displays a summary of LACP information.
Command mode: All
For details, see page 57 .

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
INT1	active	30	30	yes	32768	17	19	up
INT2	active	30	30	yes	32768	17	19	up
INT3	off	3	3	no	32768	--	--	--
INT4	off	4	4	no	32768	--	--	--
...								

LACP dump includes the following information for each external port in the GbESM:

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

Layer 2 Failover Information

Table 22 Layer 2 Failover Information commands

Command Syntax and Usage

show failover trigger <1-8>

Displays detailed information about the selected Layer 2 Failover trigger.

Command mode: All

show failover trigger

Displays a summary of Layer 2 Failover information. For details, see [page 59](#).

Command mode: All

Layer 2 Failover Information

The following command displays Layer 2 Failover information:

show failover trigger

Command mode: All

```
Trigger 1 Auto Monitor: Enabled
Trigger 1 limit: 0
Monitor State: Up
Member      Status
-----
trunk 1
  EXT2      Operational
  EXT3      Operational

Control State: Auto Disabled
Member      Status
-----
  INT1      Operational
  INT2      Operational
  INT3      Operational
  INT4      Operational
...
```

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

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

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

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

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

Hot Links Information

The following command displays Hot Links information:

show hotlinks information

Command mode: All

```
Hot Links Info: Trigger

Current global Hot Links setting: ON
bpdu disabled
sndfdb disabled

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

Active state: None

Master settings:
port EXT1
Backup settings:
port EXT2
```

Hot Links information includes the following:

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

LLDP Information

Table 23 LLDP Information commands

Command Syntax and Usage

show lldp port

Displays Link Layer Discovery Protocol (LLDP) port information.

Command mode: All

show lldp receive

Displays information about the LLDP receive state machine.

Command mode: All

show lldp transmit

Displays information about the LLDP transmit state machine.

Command mode: All

show lldp remote-device

Displays information received from LLDP -capable devices. To view a sample display, see [page 62](#).

show lldp information

Displays all LLDP information.

Command mode: All

LLDP Remote Device Information

The following command displays LLDP remote device information:

show lldp remote-device

Command mode: All

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

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

Local Port Alias: EXT1	
Remote Device Index	: 15
Remote Device TTL	: 99
Remote Device RxChanges	: false
Chassis Type	: Mac Address
Chassis Id	: 00-18-b1-33-1d-00
Port Type	: Locally Assigned
Port Id	: 23
Port Description	: EXT1
System Name :	
System Description :	
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 24 UDLD Information commands

Command Syntax and Usage

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

Displays UDLD information about the selected port.

Command mode: All

show udld

Displays all UDLD information.

Command mode: All

UDLD Port Information

The following command displays UDLD information for the selected port:

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

Command mode: All

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

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

UDLD information includes the following:

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

OAM Discovery Information

Table 25 OAM Discovery Information commands

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

OAM Port Information

The following command displays OAM information for the selected port:

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

Command mode: All

```
OAM information on port EXT1
State enabled
Mode active
Link up
Satisfied Yes
Evaluating No

Remote port information:
Mode active
MAC address 00:da:c0:00:04:00
Stable Yes
State valid Yes
Evaluating No
```

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

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
```

Port	Auth Mode	Auth Status	Authenticator PAE State	Backend Auth State
-----	-----	-----	-----	-----
INT1	force-auth	authorized	initialize	initialize
*INT2	force-auth	authorized	initialize	initialize
*INT3	force-auth	authorized	initialize	initialize
*INT4	force-auth	authorized	initialize	initialize
*INT5	force-auth	authorized	initialize	initialize
*INT6	force-auth	authorized	initialize	initialize
*INT7	force-auth	authorized	initialize	initialize
*INT8	force-auth	authorized	initialize	initialize
INT9	force-auth	authorized	initialize	initialize
INT10	force-auth	authorized	initialize	initialize
*INT11	force-auth	authorized	initialize	initialize
*INT12	force-auth	authorized	initialize	initialize
*INT13	force-auth	authorized	initialize	initialize
*INT14	force-auth	authorized	initialize	initialize
*MGT1	force-auth	authorized	initialize	initialize
*MGT2	force-auth	authorized	initialize	initialize
*EXT1	force-auth	unauthorized	initialize	initialize
*EXT2	force-auth	unauthorized	initialize	initialize
*EXT3	force-auth	unauthorized	initialize	initialize
*EXT4	force-auth	unauthorized	initialize	initialize
...				
-----	-----	-----	-----	-----

* - Port down or disabled

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

The following table describes the IEEE 802.1X parameters.

Table 26 802.1X Parameter Descriptions

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

Spanning Tree Information

The following command displays Spanning Tree information:

show spanning-tree stp <1-128> information

Command mode: All

```

-----
upfast disabled, update 40
Pvst+ compatibility mode enabled
-----

Spanning Tree Group 1: On (STP/PVST+)
VLANs: 1

Current Root:          Path-Cost  Port Hello MaxAge FwdDel
ffff 00:13:0a:4f:7d:d0      0    EXT2    2    20    15

Parameters:  Priority  Hello  MaxAge  FwdDel  Aging
              65535    2      20      15     300

Port Priority Cost FastFwd  State           Designated Bridge  Des Port
-----
INT1      0    0    n  FORWARDING  *
INT2      0    0    n  FORWARDING  *
INT3      0    0    n  FORWARDING  *
INT4      0    0    n  FORWARDING  *
INT5      0    0    n  FORWARDING  *
INT6      0    0    n  FORWARDING  *
INT7      0    0    n  FORWARDING  *
INT8      0    0    n  FORWARDING  *
INT9      0    0    n  DISABLED    *
INT10     0    0    n  FORWARDING  *
INT11     0    0    n  FORWARDING  *
INT12     0    0    n  FORWARDING  *
INT13     0    0    n  FORWARDING  *
INT14     0    0    n  FORWARDING  *
EXT1     128    2    n  DISABLED
EXT2     128    2    n  DISABLED
EXT3     128    2    n  FORWARDING  ffff-00:13:0a:4f:7d:d0  8011
EXT4     128    4!   n  FORWARDING  ffff-00:22:00:7d:71:00  8017
...
* = STP turned off for this port.
! = Automatic path cost.

```

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

The switch software uses the IEEE 802.1D Spanning Tree Protocol (STP). If IEEE 802.1w Rapid Spanning Tree Protocol (RSTP), the IEEE 802.1s Multiple Spanning Tree Protocol (MSTP), or Per VLAN Rapid Spanning Tree Protocol (PVRST) are turned on, see [“RSTP/MSTP/PVRST Information” on page 70](#).

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

Table 27 Spanning Tree Bridge Parameter Descriptions

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

The following port-specific information is also displayed:

Table 28 Spanning Tree Port Parameter Descriptions

Parameter	Description
Priority (port)	The Port Priority parameter helps determine which bridge port becomes the designated port. In a network topology that has multiple bridge ports connected to a single segment, the port with the lowest port priority becomes the designated port for the segment.
Cost	The Port Path cost parameter is used to help determine the designated port for a segment. Generally speaking, the faster the port, the lower the path cost. A setting of 0 indicates that the cost will be set to the appropriate default after the link speed has been auto negotiated.
FastFwd	The Fast Forward field shows whether the port is in Fast Forwarding mode or not, which permits the port that participates in Spanning Tree to bypass the Listening and Learning states and enter directly into the Forwarding state.
State	The State field shows the current state of the port. The state field can be BLOCKING, LISTENING, LEARNING, FORWARDING, or DISABLED.
Designated Bridge	The Designated Bridge shows information about the bridge connected to each port, if applicable. Information includes the priority (in hexadecimal notation) and MAC address of the Designated Bridge.
Designated Port	The Designated Port field shows the port on the Designated Bridge to which this port is connected.

RSTP/MSTP/PVRST Information

The following command displays RSTP/MSTP/PVRST information:

show spanning-tree stp <1-128> information

Command mode: All

Spanning Tree Group 1: On (RSTP)									
VLANs: 1									
Current Root:									
ffff 00:13:0a:4f:7d:d0		Path-Cost		Port		Hello		MaxAge	
		0		EXT4		2		20	
								15	
Parameters:									
Priority		Hello		MaxAge		FwdDel		Aging	
61440		2		20		15		300	
Port	Prio	Cost	State	Role	Designated	Bridge	Des	Port	Type
-----	----	-----	-----	----	-----	-----	-----	-----	-----
INT1	0	0	DSB	*					
INT2	0	0	DSB	*					
INT3	0	0	FWD	*					
INT4	0	0	DSB	*					
INT5	0	0	DSB	*					
INT6	0	0	DSB	*					
INT7	0	0	DSB	*					
INT8	0	0	DSB	*					
INT9	0	0	DSB	*					
INT10	0	0	DSB	*					
INT11	0	0	DSB	*					
INT12	0	0	DSB	*					
INT13	0	0	DSB	*					
INT14	0	0	DSB	*					
EXT1	128	2000	FWD	DESG	8000-00:11:58:ae:39:00		8011		P2P
EXT2	128	2000	DISC	BKUP	8000-00:11:58:ae:39:00		8011		P2P
EXT3	128	2000	FWD	DESG	8000-00:11:58:ae:39:00		8013		P2P
EXT4	128	20000	DISC	BKUP	8000-00:11:58:ae:39:00		8013		Shared
...									
* = STP turned off for this port.									

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

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

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

Table 29 RSTP/MSTP/PVRST Bridge Parameter Descriptions

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

The following port-specific information is also displayed:

Table 30 RSTP/MSTP/PVRST Port Parameter Descriptions

Parameter	Description
Prio (port)	The Port Priority parameter helps determine which bridge port becomes the designated port. In a network topology that has multiple bridge ports connected to a single segment, the port with the lowest port priority becomes the designated port for the segment.
Cost	The port Path Cost parameter is used to help determine the designated port for a segment. Generally speaking, the faster the port, the lower the path cost. A setting of 0 indicates that the cost will be set to the appropriate default after the link speed has been auto negotiated.

Table 30 RSTP/MSTP/PVRST Port Parameter Descriptions (continued)

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

Common Internal Spanning Tree Information

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

show spanning-tree mstp cist information

Command mode: All

```
Common Internal Spanning Tree: on
VLANs: 2-4094

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

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

Parameters:  Priority  MaxAge  FwdDel  Hops
              61440    20      15     20

Port  Prio  Cost    State  Role  Designated Bridge  Des Port  Hello  Type
-----
INT1   0      0      DSB  *
INT2   0      0      DSB  *
INT3   0      0      FWD  *
INT4   0      0      DSB  *
INT5   0      0      DSB  *
INT6   0      0      DSB  *
INT7   0      0      DSB  *
INT8   0      0      DSB  *
INT9   0      0      DSB  *
INT10  0      0      DSB  *
INT11  0      0      DSB  *
INT12  0      0      DSB  *
INT13  0      0      DSB  *
INT14  0      0      DSB  *
MGT1   0      0      FWD  *
MGT2   0      0      FWD
*EXT1  128    20000  FWD  DESG 8000-00:11:58:ae:39:00  8011  2    P2P
EXT2   128    20000  DISC BKUP 8000-00:11:58:ae:39:00  8011  2    P2P
EXT3   128    20000  FWD  DESG 8000-00:11:58:ae:39:00  8013  2    P2P
EXT4   128    20000  DISC BKUP 8000-00:11:58:ae:39:00  8013  2    Shared
...
* = STP turned off for this port.
```

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

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

Table 31 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 32 CIST Parameter Descriptions

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

Table 32 CIST Parameter Descriptions (continued)

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

Trunk Group Information

The following command displays Trunk Group information:

show portchannel information

Command mode: All

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

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

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

VLAN Information

Table 33 VLAN Information commands

Command Syntax and Usage

show vlan *<VLAN number>*

Displays general VLAN information.

show protocol-vlan *<protocol number>*

Displays protocol VLAN information.

Command mode: All

show private-vlan *<VLAN number>*

Displays private VLAN information.

Command mode: All

show vlan information

Displays information about all VLANs, including:

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

The following command displays VLAN information:

show vlan

Command mode: All

VLAN	Name	Status	MGT	Ports
1	Default VLAN	ena	dis	INT1-INT14 EXT1-EXT9
10	VLAN 10	ena	dis	INT1
11	VLAN 11	ena	dis	EXT3
30	VLAN 30	ena	dis	EXT4
4095	Mgmt VLAN	ena	ena	INT1-INT14 MGT1 MGT2

Private-VLAN	Type	Mapped-To	Status	Ports
1000	primary	1001-1014	ena	EXT1 EXT2
1001	isolated	1000	ena	INT1
1002	community	1000	ena	INT2
1003	community	1000	ena	INT3

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

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

VLAN information includes:

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

Layer 3 Information

Table 34 Layer 3 Information Commands

Command Syntax and Usage

show ip route

Displays all routes configured on the switch.

Command mode: All

For details, see [page 81](#).

show ip arp

Displays Address Resolution Protocol (ARP) information.

Command mode: All

For details, see [page 83](#).

show ip bgp information

Displays Border Gateway Protocol (BGP) information.

Command mode: All

For details, see [page 87](#).

show ip ospf information

Displays the OSPF information.

Command mode: All

For more OSPF information options, see [page 87](#).

show ipv6 ospf information

Displays OSPFv3 information.

Command mode: All

For more OSPFv3 information options, see [page 93](#).

show interface ip rip

Displays RIP user's configuration.

Command mode: All

For details, see [page 99](#).

Table 34 Layer 3 Information Commands (continued)

Command Syntax and Usage

show ip information

Displays IP Information. For details, see [page 80](#).

IP information, includes:

- ❑ IP interface information: Interface number, IP address, subnet mask, VLAN number, and operational status.
- ❑ Default gateway information: Metric for selecting which configured gateway to use, gateway number, IP address, and health status
- ❑ IP forwarding settings, network filter settings, route map settings

Command mode: All

show ip igmp groups

Displays IGMP Information.

Command mode: All

show ip vrrp information

Displays VRRP information.

Command mode: All

For details, see [page 109](#).

show layer3

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

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

Command mode: All

IP Routing Information

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

Table 35 Route Information Commands

Command Syntax and Usage
show ip route address <i><IP address></i> Displays a single route by destination IP address. Command mode: All
show ip route gateway <i><IP address></i> Displays routes to a single gateway. Command mode: All
show ip route type {indirect direct local broadcast martian multicast} Displays routes of a single type. For a description of IP routing types, see Table 36 on page 81 . Command mode: All
show ip route tag {fixed static addr rip ospf bgp broadcast martian multicast} Displays routes of a single tag. For a description of IP routing tags, see Table 37 on page 82 . Command mode: All
show ip route interface <i><interface number></i> Displays routes on a single interface. Command mode: All
show ip route static Displays static routes configured on the switch. Command mode: All
show ip route Displays all routes configured in the switch. Command mode: All For more information, see page 81 .

Show All IP Route Information

The following command displays IP route information:

show ip route

Command mode: All

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

The following table describes the Type parameters.

Table 36 IP Routing Type Parameters

Parameter	Description
indirect	The next hop to the host or subnet destination will be forwarded through a router at the Gateway address.
direct	Packets will be delivered to a destination host or subnet attached to the switch.
local	Indicates a route to one of the switch's IP interfaces.
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 37 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 1/10Gb Uplink ESM.
addr	The address belongs to one of the switch's IP interfaces.
rip	The address was learned by the Routing Information Protocol (RIP).
ospf	The address was learned by Open Shortest Path First (OSPF).
bgp	The address was learned via Border Gateway Protocol (BGP).
broadcast	Indicates a broadcast address.
martian	The address belongs to a filtered group.
multicast	Indicates a multicast address.

ARP Information

The ARP information includes IP address and MAC address of each entry, address status flags (see [Table 39 on page 84](#)), VLAN and port for the address, and port referencing information.

Table 38 ARP Information Commands

Command Syntax and Usage

show ip arp find *<IP address>*

Displays a single ARP entry by IP address.

Command mode: All

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

Displays the ARP entries on a single port.

Command mode: All

show ip arp vlan *<VLAN number>*

Displays the ARP entries on a single VLAN.

Command mode: All

show ip arp

Displays all ARP entries. including:

- ☐ IP address and MAC address of each entry
- ☐ Address status flag (see below)
- ☐ The VLAN and port to which the address belongs
- ☐ The ports which have referenced the address (empty if no port has routed traffic to the IP address shown)

Command mode: All

For more information, see [page 84](#).

show ip arp reply

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

Command mode: All

Show All ARP Entry Information

The following command displays ARP information:

show ip arp

Command mode: All

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

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

The **Flags** field is interpreted as follows:

Table 39 ARP Dump Flag Parameters

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

ARP Address List Information

The following command displays owned ARP address list information:

show ip arp reply

Command mode: All

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

BGP Information

Table 40 BGP Peer Information Commands

Command Syntax and Usage

show ip bgp neighbor information

Displays BGP peer information.

Command mode: All

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

show ip bgp neighbor summary

Displays peer summary information such as AS, message received, message sent, up/down, state.

Command mode: All

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

show ip bgp information

Displays the BGP routing table.

Command mode: All

See [page 87](#) for a sample output.

BGP Peer information

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

show ip bgp neighbor information

Command mode: All

```
BGP Peer Information:

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

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

BGP Summary information

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

show ip bgp neighbor summary

Command mode: All

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

Dump BGP Information

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

show ip bgp information

Command mode: All

Status codes: * valid, > best, i - internal						
Origin codes: i - IGP, e - EGP, ? - incomplete						
Network	Mask	Next Hop	Metr	LcPrf	Wght	Path
-----	-----	-----	-----	-----	-----	-----
*> 1.1.1.0	255.255.255.0	0.0.0.0			0	?
*> 10.100.100.0	255.255.255.0	0.0.0.0			0	?
*> 10.100.120.0	255.255.255.0	0.0.0.0			0	?
The 13.0.0.0 is filtered out by rrmapp; or, a loop detected.						

OSPF Information

Table 41 OSPF Information Commands

Command Syntax and Usage

show ip ospf general-information

Displays general OSPF information.

Command mode: All

See [page 89](#) for a sample output.

show ip ospf area information

Displays area information for all areas.

Command mode: All

show ip ospf area <0-2>

Displays area information for a particular area index.

Command mode: All

show interface ip {<interface number>} ospf

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

Command mode: All

See [page 90](#) for a sample output.

Table 41 OSPF Information Commands (continued)

Command Syntax and Usage

show ip ospf area-virtual-link information

Displays information about all the configured virtual links.

Command mode: All

show ip ospf neighbor

Displays the status of all the current neighbors.

Command mode: All

show ip ospf summary-range <0-2>

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

Command mode: All

show ip ospf summary-range-nssa <0-2>

Displays the list of summary ranges belonging to NSSA areas.

Command mode: All

show ip ospf routes

Displays OSPF routing table.

Command mode: All

See [page 92](#) for a sample output.

show ip ospf information

Displays the OSPF information.

Command mode: All

OSPF General Information

The following command displays general OSPF information:

show ip ospf general-information

Command mode: All

```

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

```

OSPF Interface Information

The following command displays OSPF interface information:

show ip ospf interface <interface number>

Command mode: All

```
Ip Address 10.10.12.1, Area 0.0.0.1, Admin Status UP
Router ID 10.10.10.1, State DR, Priority 1
Designated Router (ID) 10.10.10.1, Ip Address 10.10.12.1
Backup Designated Router (ID) 10.10.14.1, Ip Address 10.10.12.2
Timer intervals, Hello 10, Dead 40, Wait 1663, Retransmit 5,
      Poll interval 0, Transit delay 1
Neighbor count is 1   If Events 4, Authentication type none
```

OSPF Database Information

Table 42 OSPF Database Information Commands

Command Syntax and Usage

show ip ospf database advertising-router <router ID>

Takes advertising router as a parameter. Displays all the Link State Advertisements (LSAs) in the LS database that have the advertising router with the specified router ID, for example: 20.1.1.1.

Command mode: All

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

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

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

Command mode: All

Table 42 OSPF Database Information Commands (continued)

Command Syntax and Usage

show ip ospf database database-summary

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

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

No parameters are required.

Command mode: All

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

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

Command mode: All

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

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

Command mode: All

show ip ospf database nssa

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

Command mode: All

show ip ospf database router

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

Command mode: All

show ip ospf database self

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

Command mode: All

Table 42 OSPF Database Information Commands (continued)

Command Syntax and Usage

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

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

Command mode: All

show ip ospf database

Displays all the LSAs.

Command mode: All

OSPF Information Route Codes

The following command displays OSPF route information:

show ip ospf routes

Command mode: All

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

OSPFv3 Information

Table 43 OSPFv3 Information Options

Command Syntax and Usage

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

Displays the area information.

Command mode: All

show ipv6 ospf areas

Displays the OSPFv3 Area Table.

Command mode: All

show ipv6 ospf interface *<interface number>*

Displays interface information for a particular interface. If no parameter is supplied, it displays information for all the interfaces. To view a sample display, see [page 96](#).

Command mode: All

show ipv6 ospf area-virtual-link

Displays information about all the configured virtual links.

Command mode: All

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

Displays the status of a neighbor with a particular router ID. If no router ID is supplied, it displays the information about all the current neighbors.

Command mode: All

show ipv6 ospf host

Displays OSPFv3 host configuration information.

Command mode: All

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

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

Command mode: All

Table 43 OSPFv3 Information Options

Command Syntax and Usage

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

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

Command mode: All

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

Displays the OSPFv3 external summary-address configuration information.

Command mode: All

show ipv6 ospf redistrib-config

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

Command mode: All

show ipv6 ospf area-range information

Displays OSPFv3 summary ranges.

Command mode: All

show ipv6 ospf routes

Displays OSPFv3 routing table. To view a sample display, see [page 98](#).

Command mode: All

show ipv6 ospf border-routers

Displays OSPFv3 routes to an ABR or ASBR.

Command mode: All

show ipv6 ospf information

Displays all OSPFv3 information. To view a sample display, see [page 95](#).

Command mode: All

OSPFv3 Information Dump

```

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

```

OSPFv3 Interface Information

The following command displays OSPFv3 interface information:

show ipv6 ospf interface

Command mode: All

```
Ospf3 Interface Information

Interface Id: 1      Instance Id: 0      Area Id: 0.0.0.0
Local Address: fe80::222:ff:fe7d:5d00    Router Id: 1.0.0.1
Network Type: BROADCAST  Cost: 1        State: BACKUP

Designated Router Id: 2.0.0.2      local address:
fe80::218:b1ff:feal:6c01

Backup Designated Router Id: 1.0.0.1      local address:
fe80::222:ff:fe7d:5d00

Transmit Delay: 1 sec    Priority: 1      IfOptions: 0x0
Timer intervals configured:
Hello: 10,  Dead: 40,  Retransmit: 5
Hello due in 6 sec
Neighbor Count is: 1,  Adjacent neighbor count is: 1
Adjacent with neighbor 2.0.0.2
```


OSPFv3 Database Information

Table 44 OSPFv3 Database Information Options

Command Syntax and Usage

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

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

Command mode: All

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

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

Command mode: All

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

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

Command mode: All

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

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

Command mode: All

show ipv6 ospf database link [detail|hex]

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

Command mode: All

show ipv6 ospf database network [detail|hex]

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

Command mode: All

show ipv6 ospf database router [detail|hex]

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

Command mode: All

Table 44 OSPFv3 Database Information Options

Command Syntax and Usage

show ipv6 ospf database nssa [detail|hex]

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

Command mode: All

show ipv6 ospf database [detail|hex]

Displays all the LSAs.

Command mode: All

OSPFv3 Route Codes Information

The following command displays OSPFv3 route information:

show ipv6 ospf database routes

Command mode: All

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

Routing Information Protocol

Table 45 Routing Information Protocol Commands

Command Syntax and Usage

show ip rip routes

Displays RIP routes.

Command mode: All

For more information, see [page 99](#).

show interface ip <interface number> rip

Displays RIP user’s configuration.

Command mode: All

For more information, see [page 100](#).

RIP Routes Information

The following command displays RIP route information:

show ip rip routes

Command mode: All

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

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

RIP Interface Information

The following command displays RIP user information:

show interface ip *<interface number>* **rip**

Command mode: All

```
RIP USER CONFIGURATION :  
  RIP on update 30  
  RIP Interface 1 : 10.4.4.2,          enabled  
  version 2, listen enabled, supply enabled, default none  
  poison disabled, split horizon enabled, trigg enabled,  
  mcast enabled, metric 1  
  auth none, key none
```

IPv6 Routing Information

Table 46 IPv6 Routing information commands

Command Syntax and Usage

show ipv6 route summary

Displays a summary of IPv6 routing information.

Command mode: All

show ipv6 route

Displays all IPv6 routing information.

Command mode: All

IPv6 Routing Table

The following command displays IPv6 routing information:

show ipv6 route

Command mode: All

```
IPv6 Routing Table - 3 entries
Codes : C - Connected, S - Static

S   ::/0 [1/20]
      via 2001:2:3:4::1, Interface 2
C   2001:2:3:4::/64 [1/1]
      via ::, Interface 2
C   fe80::20f:6aff:feec:f701/128 [1/1]
      via ::, Interface 2
```

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

IPv6 Neighbor Discovery Cache Information

Table 47 IPv6 Neighbor Discovery Cache information commands

Command Syntax and Usage

show ipv6 neighbors find *<IPv6 address>*

Shows a single IPv6 Neighbor cache entry by IP address.

Command mode: All

show ipv6 neighbors interface port *<port alias or number>*

Shows IPv6 Neighbor cache entries on a single port.

Command mode: All

show ipv6 neighbors vlan *<VLAN number>*

Shows IPv6 Neighbor cache entries on a single VLAN.

Command mode: All

show ipv6 neighbors

Shows all IPv6 Neighbor cache entries.

Command mode: All

For more information, see [page 102](#).

IPv6 Neighbor Discovery Cache Information

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

show ipv6 neighbors

Command mode: All

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

Interface Information

The following command displays interface information:

show interface ip

Command mode: All

```
Interface information:
  1: IP4 172.31.35.5      255.255.0.0 172.31.255.255,  vlan 1, up
  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
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)

IP Information

The following command displays Layer 3 information:

show layer3 information

Command mode: All

```
IP information:
  AS number 0

Interface information:
  1: 10.200.30.3      255.255.0.0      10.200.255.255,  vlan 1, up
  127: IP6 10:90:90:0:0:0:0:91/64      , vlan 4095, up
      fe80::222:ff:fe7d:717e
  128: IP4 172.31.30.128  255.255.0.0      172.31.255.255,  vlan 4095, up

Loopback interface information:
  2: 2.2.2.2          255.255.255.0    2.2.2.255,      enabled

Default gateway information: metric strict
  1: 10.200.1.1,      vlan any, up
  132: 172.31.1.1,    vlan 4095, up  active

Default IP6 gateway information:

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

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

Current network filter settings:
  none

Current route map settings:
```

IP information includes:

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

IGMP Multicast Group Information

Table 48 IGMP Multicast Group Information Commands

Command Syntax and Usage

show ip igmp snoop

Displays IGMP Snooping information.

Command mode: All

show ip igmp relay

Displays IGMP Relay information.

Command mode: All

show ip igmp mrouter information

Displays IGMP Multicast Router information.

Command mode: All

show ip igmp mrouter vlan <VLAN number>

Displays IGMP Multicast Router information for the specified VLAN.

Command mode: All

show ip igmp filtering

Displays current IGMP Filtering parameters.

Command mode: All

show ip igmp profile <1-16>

Displays information about the current IGMP filter.

Command mode: All

show ip igmp groups address <IP address>

Displays a single IGMP multicast group by its IP address.

Command mode: All

show ip igmp groups vlan <VLAN number>

Displays all IGMP multicast groups on a single VLAN.

Command mode: All

Table 48 IGMP Multicast Group Information Commands (continued)

Command Syntax and Usage

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

Displays all IGMP multicast groups on a single port.

Command mode: All

show ip igmp groups portchannel *<trunk number>*

Displays all IGMP multicast groups on a single trunk group.

Command mode: All

show ip igmp groups detail *<IP address>*

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

Command mode: All

show ip igmp groups

Displays information for all multicast groups.

Command mode: All

IGMP Group Information

The following command displays IGMP Group information:

show ip igmp groups

Command mode: All

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

IGMP Group information includes:

- IGMP source address
- IGMP Group address
- VLAN and port
- IGMP version
- IGMPv3 filter mode
- Expiration timer value
- IGMP multicast forwarding state

IGMP Multicast Router Information

The following command displays Mrouter information:

show ip igmp mrouter information

Command mode: All

SrcIP	VLAN	Port	Version	Expires	MRT	QRV	QQIC
-----	-----	-----	-----	-----	-----	-----	-----
10.1.1.1	2	21	V3	4:09	128	2	125
10.1.1.5	2	23	V2	4:09	125	-	-
10.10.10.43	9	24	V2	static	unknown	-	-

IGMP Mrouter information includes:

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

VRRP Information

Virtual Router Redundancy Protocol (VRRP) support on 1/10Gb Uplink ESM 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.

Quality of Service Information

Table 49 QoS information commands

Command Syntax and Usage

show qos transmit-queue

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

Command mode: All

show qos transmit-queue information

Displays all 802.1p information.

Command mode: All

For details, see [page 111](#).

802.1p Information

The following command displays 802.1p information:

show qos transmit-queue information

Command mode: All

Current priority to COS queue information:			
Priority	COSq	Weight	
-----	----	-----	
0	0	1	
1	1	2	
2	2	3	
3	3	4	
4	4	5	
5	5	7	
6	6	15	
7	7	0	
Current port priority information:			
Port	Priority	COSq	Weight
-----	-----	----	-----
INT1	0	0	1
INT2	0	0	1
...			
MGT1	0	0	1
MGT2	0	0	1
EXT1	0	0	1
EXT2	0	0	1
EXT3	0	0	1
EXT4	0	0	1
...			

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

Table 50 802.1p 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 51 802.1p Port Priority Parameter Descriptions

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

Access Control List Information Commands

Table 52 ACL information commands

Command Syntax and Usage
show access-control list <i><ACL number></i> Displays ACL list information. For details, see page 113 . Command mode: All
show access-control group <i><ACL group number></i> Displays ACL group information. Command mode: All

Access Control List Information

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

show access-control list <ACL number>

Command mode: All

```
Current ACL information:
-----
Filter 2 profile:
  Ethernet
    - VID          : 2/0xffff
  Meter
    - Set to disabled
    - Set committed rate : 64
    - Set max burst size : 32
  Re-Mark
    - Set use of TOS precedence to disabled
  Actions          : Permit
  Statistics        : enabled

No ACL groups configured.
No VMAP configured.
```

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

Table 53 ACL Parameter Descriptions

Parameter	Description
Filter <i>x</i> profile	Indicates the ACL number.
Meter	Displays the ACL meter parameters.
Re-Mark	Displays the ACL re-mark parameters.
Actions	Displays the configured action for the ACL.
Statistics	Displays the status of ACL statistics configuration (enabled or disabled).

RMON Information Commands

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

Table 54 RMON Information commands

Command Syntax and Usage	
show rmon history	Displays RMON History information. For details, see page 115 .
Command mode: All	
show rmon alarm	Displays RMON Alarm information. For details, see page 116 .
Command mode: All	
show rmon event	Displays RMON Event information. For details, see page 118 .
Command mode: All	
show rmon	Displays all RMON information.
Command mode: All	

RMON History Information

The following command displays RMON History information:

show rmon history

Command mode: All

RMON History group configuration:				
Index	IFOID	Interval	Rbnum	Gbnum
-----	-----	-----	-----	-----
1	1.3.6.1.2.1.2.2.1.1.24	30	5	5
2	1.3.6.1.2.1.2.2.1.1.22	30	5	5
3	1.3.6.1.2.1.2.2.1.1.20	30	5	5
4	1.3.6.1.2.1.2.2.1.1.19	30	5	5
5	1.3.6.1.2.1.2.2.1.1.24	1800	5	5
Index	Owner			
-----	-----			
1	dan			

The following table describes the RMON History Information parameters.

Table 55 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 56 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: <div><div><input type="checkbox"/> abs—absolute value, the value of the selected variable is compared directly with the thresholds at the end of the sampling interval.</div><div><input type="checkbox"/> delta—delta value, the value of the selected variable at the last sample is subtracted from the current value, and the difference compared with the thresholds.</div></div>
Type	Displays the type of alarm, as follows: <div><div><input type="checkbox"/> falling—alarm is triggered when a falling threshold is crossed.</div><div><input type="checkbox"/> rising—alarm is triggered when a rising threshold is crossed.</div><div><input type="checkbox"/> either—alarm is triggered when either a rising or falling threshold is crossed.</div></div>

Table 56 RMON Alarm Parameter Descriptions (continued)

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

RMON Event Information

The following command displays RMON Alarm information:

show rmon event

Command mode: All

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

The following table describes the RMON Event Information parameters.

Table 57 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 link

Command mode: All

Alias	Port	Speed	Duplex	Flow Ctrl		Link
----	-----	-----	-----	--TX--	--RX--	-----
INT1	1	1000	full	yes	yes	up
INT2	2	1000	full	yes	yes	up
INT3	3	1000	full	yes	yes	up
INT4	4	1000	full	yes	yes	up
INT5	5	1000	full	yes	yes	down
INT6	6	1000	full	yes	yes	up
INT7	7	1000	full	yes	yes	up
INT8	8	1000	full	yes	yes	up
INT9	9	1000	full	yes	yes	up
INT10	10	1000	full	yes	yes	up
INT11	11	1000	full	yes	yes	up
INT12	12	1000	full	yes	yes	up
INT13	13	1000	full	yes	yes	up
INT14	14	1000	full	yes	yes	up
MGT1	15	100	full	yes	yes	up
MGT2	16	100	full	yes	yes	up
EXT1	17	10000	full	yes	yes	down
EXT2	18	10000	full	yes	yes	down
EXT3	19	10000	full	yes	yes	disabled
EXT4	20	any	any	yes	yes	down
EXT5	21	any	any	yes	yes	down
EXT6	22	any	any	yes	yes	down
EXT7	23	any	any	yes	yes	down
EXT8	24	any	any	yes	yes	down
EXT9	25	any	any	yes	yes	down

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

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

Command mode: All

Alias	Port	Tag	Type	Fast	RMON	Lrn	Fld	PVID	NAME	VLAN (s)
INT1	1	y	Internal	n	d	e	e	1	INT1	1
INT2	2	y	Internal	n	d	e	e	1	INT2	1
INT3	3	y	Internal	n	d	e	e	1	INT3	1
INT4	4	y	Internal	n	d	e	e	1	INT4	1
INT5	5	y	Internal	n	d	e	e	1	INT5	1
INT6	6	y	Internal	n	d	e	e	1	INT6	1
INT7	7	y	Internal	n	d	e	e	1	INT7	1
INT8	8	y	Internal	n	d	e	e	1	INT8	1
INT9	9	y	Internal	n	d	e	e	1	INT9	1
INT10	10	y	Internal	n	d	e	e	1	INT10	1
INT11	11	y	Internal	n	d	e	e	1	INT11	1
INT12	12	y	Internal	n	d	e	e	1	INT12	1
INT13	13	y	Internal	n	d	e	e	1	INT13	1
INT14	14	y	Internal	n	d	e	e	1	INT14	1
MGT1	15	y	Mgmt	n	d	e	e	4095*	MGT1	4095
MGT2	16	y	Mgmt	n	d	e	e	4095*	MGT2	4095
EXT1	17	n	External	n	d	e	e	1	EXT1	1
EXT2	18	n	External	n	d	e	e	1	EXT2	1
EXT3	19	n	External	n	d	e	e	1	EXT3	1
EXT4	20	n	External	n	d	e	e	1	EXT4	1
...										
* = PVID is tagged.										

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

Port information includes:

- Port alias and number
- Whether the port uses VLAN tagging or not (y or n)
- Type of port (Internal, External, or Management)
- Whether the port has Port Fast Forwarding enabled (**F**ast)
- Whether the port has Remote Monitoring (RMON) enabled
- Whether the port has FDB Learning enabled (**L**rn)
- Whether the port has Port Flood Blocking enabled (**F**ld)
- Port VLAN ID (PVID)
- Port name
- VLAN membership

Port Transceiver Status

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

show transceiver

Command mode: All

Port	Device	TX-Enable	RX-Signal	TX-Fault
-----	-----	-----	-----	-----
17 - EXT1	SR-SFP+	enabled	LOST	none
18 - EXT2	SR-SFP+	enabled	LOST	none
19 - EXT3	SR-SFP+	****	NOT Installed	****

Virtual Machines Information

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

Table 58 Virtual Machines Information Options

Command Syntax and Usage

show virt port *<port alias or number>*

Displays Virtual Machine information for the selected port.

Command mode: All

show virt vm

Displays all Virtual Machine information.

Command mode: All

VM Information

The following command displays VM information:

show virt vm

Command mode: All

IP Address	VMAC Address	Index	Port	VM Group (Profile)
*127.31.46.50	00:50:56:4e:62:f5	4	INT3	
*127.31.46.10	00:50:56:4f:f2:85	2	INT4	
+127.31.46.51	00:50:56:72:ec:86	1	INT3	
+127.31.46.11	00:50:56:7c:1c:ca	3	INT4	
127.31.46.25	00:50:56:9c:00:c8	5	INT4	
127.31.46.15	00:50:56:9c:21:2f	0	INT4	
127.31.46.35	00:50:56:9c:29:29	6	INT3	
Number of entries: 8				
* indicates VMware ESX Service Console Interface				
+ indicates VMware ESX/ESXi VMKernel or Management Interface				

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

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

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 59 VMware Information Options

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

VMware Host Information

The following command displays VM host information:

show virt vmware hosts

Command mode: All

UUID	Name(s), IP Address

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

VM host information includes the following:

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

Information Dump

The following command dumps switch information:

show information-dump

Command mode: All

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

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

CHAPTER 3

Statistics Commands

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

Table 60 Statistics Commands

Command Syntax and Usage

show layer3 counters

Command mode: All

Displays Layer 3 statistics.

show snmp-server counters

Command mode: All

Displays SNMP statistics. See [page 192](#) for sample output.

show ntp counters

Displays Network Time Protocol (NTP) Statistics.

Command mode: All

See [page 196](#) for a sample output and a description of NTP Statistics.

show counters

Dumps all switch statistics. Use this command to gather data for tuning and debugging switch performance. If you want to capture dump data to a file, set your communication software on your workstation to capture session data prior to issuing the dump command.

Command mode: All

For details, see [page 197](#).

Port Statistics

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

Table 61 Port Statistics Commands

Command Syntax and Usage

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

Displays IEEE 802.1X statistics for the port.

Command mode: All

See [page 128](#) for sample output.

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

Displays Active MultiPath (AMP) statistics for the port.

Command mode: All

See [page 132](#) for sample output.

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

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

Command mode: All

See [page 133](#) for sample output.

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

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

Command mode: All

See [page 134](#) for sample output.

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

Displays interface statistics for the port.

Command mode: All

See [page 137](#) for sample output.

Table 61 Port Statistics Commands**Command Syntax and Usage**

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

Displays IP statistics for the port.

Command mode: All

See [page 140](#) for sample output.

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

Displays link statistics for the port.

Command mode: All

See [page 140](#) for sample output.

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

Displays Remote Monitoring (RMON) statistics for the port.

Command mode: All

See [page 141](#) for sample output.

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

Displays statistics for the port.

Command mode: All

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

Clears all statistics for the port.

Command mode: All except User EXEC

clear interfaces

Clears statistics for all ports.

Command mode: All except User EXEC

802.1X Authenticator Statistics

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

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

Command mode: All

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

Table 62 802.1X 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 63 802.1X Authenticator Diagnostics of a Port

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

Table 63 802.1X Authenticator Diagnostics of a Port

Statistics	Description
authTimeoutsWhile Authenticating	Total number of times that the state machine transitions from AUTHENTICATING to ABORTING, as a result of the Backend Authentication state machine indicating authentication timeout.
authFailWhile Authenticating	Total number of times that the state machine transitions from AUTHENTICATING to HELD, as a result of the Backend Authentication state machine indicating authentication failure.
authReauthsWhile Authenticating	Total number of times that the state machine transitions from AUTHENTICATING to ABORTING, as a result of a re-authentication request
authEapStartsWhile Authenticating	Total number of times that the state machine transitions from AUTHENTICATING to ABORTING, as a result of an EAPOL-Start message being received from the Supplicant.
authEapLogoffWhile Authenticating	Total number of times that the state machine transitions from AUTHENTICATING to ABORTING, as a result of an EAPOL-Logoff message being received from the Supplicant.
authReauthsWhile Authenticated	Total number of times that the state machine transitions from AUTHENTICATED to CONNECTING, as a result of a re-authentication request.
authEapStartsWhile Authenticated	Total number of times that the state machine transitions from AUTHENTICATED to CONNECTING, as a result of an EAPOL-Start message being received from the Supplicant.
authEapLogoffWhile Authenticated	Total number of times that the state machine transitions from AUTHENTICATED to DISCONNECTED, as a result of an EAPOL-Logoff message being received from the Supplicant.
backendResponses	Total number of times that the state machine sends an initial Access-Request packet to the Authentication server. Indicates that the Authenticator attempted communication with the Authentication Server.
backendAccessChallenges	Total number of times that the state machine receives an initial Access-Challenge packet from the Authentication server. Indicates that the Authentication Server has communication with the Authenticator.

Table 63 802.1X Authenticator Diagnostics of a Port

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.

Active MultiPath Statistics

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

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

Command mode: All

AMP statistics for port EXT1:		
Keep-alive packets sent:		0
Keep-alive packets rcvd:		0
Fdb-Flush packets sent:		0
Fdb-Flush packets rcvd:		0
Dropped packets	:	0

Table 64 AMP Statistics of a Port

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

Bridging Statistics

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

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

Command mode: All

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

Table 65 Bridging Statistics of a Port

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

Ethernet Statistics

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

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

Command mode: All

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

Table 66 Ethernet Statistics for Port

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

Table 66 Ethernet Statistics for Port

Statistics	Description
dot3StatsSingleCollision Frames	<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>
dot3StatsMultipleCollision Frames	<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>
dot3StatsExcessive Collisions	<p>A count of frames for which transmission on a particular interface fails due to excessive collisions.</p>
dot3StatsInternalMac TransmitErrors	<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 66 Ethernet Statistics for Port

Statistics	Description
dot3StatsFrameTooLongs	<p>A count of frames received on a particular interface that exceed the maximum permitted frame size.</p> <p>The count represented by an instance of this object is incremented when the <code>frameTooLong</code> status is returned by the MAC service to the LLC (or other MAC user). Received frames for which multiple error conditions obtained are, according to the conventions of IEEE 802.3 Layer Management, counted exclusively according to the error status presented to the LLC.</p>
dot3StatsInternalMacReceiveErrors	<p>A count of frames for which reception on a particular interface fails due to an internal MAC sub layer receive error. A frame is only counted by an instance of this object if it is not counted by the corresponding instance of either the <code>dot3StatsFrameTooLongs</code> object, the <code>dot3StatsAlignmentErrors</code> object, or the <code>dot3StatsFCSErrors</code> object.</p> <p>The precise meaning of the count represented by an instance of this object is implementation-specific. In particular, an instance of this object may represent a count of received errors on a particular interface that are not otherwise counted.</p>

Interface Statistics

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

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

Command mode: All

Interface statistics for port EXT1:		
	ifHCIn Counters	ifHCOut Counters
Octets:	51697080313	51721056808
UcastPkts:	65356399	65385714
BroadcastPkts:	0	6516
MulticastPkts:	0	0
FlowCtrlPkts:	0	0
Discards:	0	0
Errors:	0	21187
Ingress Discard reasons for port EXT1:		
VLAN Discards:	0	
Empty Egress Portmap:	0	
Filter Discards:	0	
Policy Discards:	0	
Non-Forwarding State:	0	
IBP/CBP Discards:	0	

Table 67 Interface Statistics for Port

Statistics	Description
ifInOctets	The total number of octets received on the interface, including framing characters.
ifInUcastPkts	The number of packets, delivered by this sub-layer to a higher sub-layer, which were not addressed to a multicast or broadcast address at this sub-layer.
ifInBroadcastPkts	The number of packets, delivered by this sub-layer to a higher sub-layer, which were addressed to a broadcast address at this sub-layer.
ifInMulticastPkts	The total number of packets that higher-level protocols requested to be transmitted, and which were addressed to a multicast address at this sub-layer, including those that were discarded or not sent. For a MAC layer protocol, this includes both Group and Functional addresses.
ifInFlowControlPkts	The total number of flow control pause packets received on the interface.

Table 67 Interface Statistics for Port

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.

Table 67 Interface Statistics for Port

Statistics	Description
VLAN Discards	Discarded because the packet was tagged with a VLAN to which this port is not a member.
Empty Egress Portmap	Dropped due to an egress port bitmap of zero condition (no ports in the egress mask). This counter increments whenever the switching decision found that there was no port to send out.
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).

Interface Protocol Statistics

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

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

Command mode: All

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

Table 68 Interface Protocol Statistics

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

Link Statistics

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

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

Command mode: All

Link statistics for port INT1:		
linkStateChange:		1

Table 69 Link Statistics

Statistics	Description
linkStateChange	The total number of link state changes.

RMON Statistics

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

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

Command mode: All.

```
RMON statistics for port EXT2:

etherStatsDropEvents:           NA
etherStatsOctets:              0
etherStatsPkts:                0
etherStatsBroadcastPkts:       0
etherStatsMulticastPkts:       0
etherStatsCRCAlignErrors:      0
etherStatsUndersizePkts:       0
etherStatsOversizePkts:        0
etherStatsFragments:           NA
etherStatsJabbers:             0
etherStatsCollisions:          0
etherStatsPkts64Octets:        0
etherStatsPkts65to127Octets:   0
etherStatsPkts128to255Octets:  0
etherStatsPkts256to511Octets:  0
etherStatsPkts512to1023Octets: 0
etherStatsPkts1024to1518Octets: 0
```

Table 70 RMON Statistics

Statistics	Description
etherStatsDropEvents	The total number of packets received that were dropped because of system resource constraints.
etherStatsOctets	The total number of octets of data (including those in bad packets) received on the network (excluding framing bits but including FCS octets).
etherStatsPkts	The total number of packets (including bad packets, broadcast packets, and multicast packets) received.
etherStatsBroadcastPkts	The total number of good packets received that were directed to the broadcast address.
etherStatsMulticastPkts	The total number of good packets received that were directed to a multicast address.

Table 70 RMON Statistics

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

Table 70 RMON Statistics

Statistics	Description
etherStatsPkts256to511 Octets	The total number of packets (including bad packets) received that were greater than 255 octets in length (excluding framing bits but including FCS octets).
etherStatsPkts512to1023 Octets	The total number of packets (including bad packets) received that were greater than 511 octets in length (excluding framing bits but including FCS octets).
etherStatsPkts1024to1518 Octets	The total number of packets (including bad packets) received that were greater than 1023 octets in length (excluding framing bits but including FCS octets).

Layer 2 Statistics

Table 71 Layer 2 Statistics Commands

Command Syntax and Usage

show active-multipath counters

Displays Active MultiPath Protocol (AMP) statistics. For more detailed commands, see [page 145](#).

Command mode: All

show mac-address-table counters

Displays FDB statistics. See [page 147](#) for sample output.

Command mode: All

clear mac-address-table counters

Clears FDB statistics.

Command mode: All except User EXEC

show interface port <port alias or number> lacp counters

Displays Link Aggregation Control Protocol (LACP) statistics. See [page 148](#) for sample output.

Command mode: All

clear interface port <port alias or number> lacp counters

Clears Link Aggregation Control Protocol (LACP) statistics.

Command mode: All except User EXEC

show hotlinks counters

Displays Hot Links statistics. See [page 149](#) for sample output.

Command mode: All except User EXEC

clear hotlinks

Clears all Hot Links statistics.

Command mode: All except User EXEC

Table 71 Layer 2 Statistics Commands**Command Syntax and Usage**

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

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

Command mode: All except User EXEC

show oam counters

Displays OAM statistics. See [page 151](#) for sample output.

Command mode: All except User EXEC

Active MultiPath Statistics

Table 72 AMP Statistics Commands**Command Syntax and Usage**

show active-multipath counters

Displays all AMP statistics.

Command mode: All

show active-multipath group [*<AMP group number>*] **counters**

Displays AMP statistics for the selected AMP group. See [page 146](#) for sample output.

Command mode: All

clear active-multipath [*<AMP group number>*]

Clears AMP statistics.

Command mode: All except User EXEC

Active MultiPath Group Statistics

Use the following command to display Active MultiPath (AMP) group statistics:

```
show active-multipath group <group number> counters
```

Command mode: All

Group	Link	Keep-alive Sent	Pkts Rcvd	Fdb-Flush Sent	Pkts Rcvd	Pkts Dropped
1	Port EXT1	26	0	0	0	0
	Port EXT2	0	0	0	0	0

This displays shows AMP group statistics for an access switch. AMP statistics are described in the following table:

Table 73 AMP Statistics

Statistic	Description
Group	AMP group number.
Link	Ports/portchannels (trunks) used for the AMP link.
Keep-alive Pkts Sent	Number of keep-alive packets sent.
Keep-alive Pkts Rcvd	Number of keep-alive packets received.
Fdb-Flush Pkts Sent	Number of FDB-flush packets sent.
Fdb-Flush Pkts Rcvd	Number of FDB-flush packets received.
Packets Dropped	Number of invalid AMP packets dropped.

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

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

Table 75 LACP Statistics

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

Hotlinks Statistics

Use the following command to display Hot Links statistics:

show hotlinks counters

Command mode: All

```
Hot Links Trigger Stats:

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

The following table describes the Hotlinks statistics:

Table 76 Hotlinks Statistics

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

LLDP Port Statistics

Use the following command to display LLDP statistics:

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

Command mode: All

LLDP Port INT1 Statistics	

Frames Transmitted	: 0
Frames Received	: 0
Frames Received in Errors	: 0
Frames Discarded	: 0
TLVs Unrecognized	: 0
Neighbors Aged Out	: 0
...	

The following table describes the LLDP port statistics:

Table 77 LLDP port Statistics

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

OAM Statistics

Use the following command to display OAM statistics:

show oam counters

Command mode: All

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

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

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

OAM statistics include the following:

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

Layer 3 Statistics

Table 78 Layer 3 Statistics Commands

Command Syntax and Usage

```
show ip gea
show ip gea bucket <IP address>
show ip gea ecmp <IP address>
```

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

Command mode: All

```
show ip counters
```

Displays IP statistics. See [page 156](#) for sample output.

Command mode: All

```
clear ip counters
```

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

Command mode: All except User EXEC

```
show ipv6 counters
```

Displays IPv6 statistics. See [page 159](#) for sample output.

Command mode: All

```
clear ipv6 counters
```

Clears IPv6 statistics. Use this command with caution as it deletes all the IPv6 statistics.

Command mode: All except User EXEC

```
show ip route counters
```

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

Command mode: All

```
show ip arp counters
```

Displays Address Resolution Protocol (ARP) statistics. See [page 164](#) for sample output.

Command mode: All

Table 78 Layer 3 Statistics Commands**Command Syntax and Usage****show ip dns counters**

Displays Domain Name System (DNS) statistics. See [page 165](#) for sample output.

Command mode: All

show ip icmp counters

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

Command mode: All

show ip tcp counters

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

Command mode: All

show ip udp counters

Displays UDP statistics. See [page 170](#) for sample output.

Command mode: All

show ip ospf counters

Displays OSPF statistics. See [page 173](#) for sample output.

Command mode: All

show ipv6 ospf3 counters

Displays OSPFv3 statistics. See [page 179](#) for sample output.

Command mode: All

show ip igmp counters

Displays IGMP statistics. See [page 171](#) for sample output.

Command mode: All

show layer3 igmp-groups

Displays the total number of IGMP groups that are registered on the switch.

Command mode: All

show layer3 ipmc-groups

Displays the total number of current IP multicast groups that are registered on the switch.

Command mode: All

Table 78 Layer 3 Statistics Commands

Command Syntax and Usage

show ip vrrp counters

When virtual routers are configured, you can display the protocol statistics for VRRP. See [page 183](#) for sample output.

Command mode: All

show ip rip counters

Displays Routing Information Protocol (RIP) statistics. See [page 184](#) for sample output.

Command mode: All

clear ip arp counters

Clears Address Resolution Protocol (ARP) statistics.

Command mode: All except User EXEC

clear ip dns counters

Clears Domain Name System (DNS) statistics.

Command mode: All except User EXEC

clear ip icmp counters

Clears Internet Control Message Protocol (ICMP) statistics.

Command mode: All except User EXEC

clear ip tcp counters

Clears Transmission Control Protocol (TCP) statistics.

Command mode: All except User EXEC

clear ip udp counters

Clears User Datagram Protocol (UDP) statistics.

Command mode: All except User EXEC

clear ip igmp [<VLAN number>] counters

Clears IGMP statistics.

Command mode: All

Table 78 Layer 3 Statistics Commands

Command Syntax and Usage

clear ip vrrp counters

Clears VRRP statistics.

Command mode: All

clear ip counters

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

Command mode: All

clear ip rip counters

Clears Routing Information Protocol (RIP) statistics.

Command mode: All except User EXEC

clear ip ospf counters

Clears Open Shortest Path First (OSPF) statistics.

Command mode: All except User EXEC

show layer3 counters

Dumps all Layer 3 statistics. Use this command to gather data for tuning and debugging switch performance. If you want to capture dump data to a file, set your communication software on your workstation to capture session data prior to issuing the dump command.

Command mode: All

IPv4 Statistics

The following command displays IPv4 statistics:

show ip counters

Command mode: All

Use the following command to clear IPv4 statistics:

clear ip counters

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

Table 79 IP Statistics

Statistic	Description
ipInReceives	The total number of input datagrams received from interfaces, including those received in error.
ipInHdrErrors	The number of input datagrams discarded due to errors in their IP headers, including bad checksums, version number mismatch, other format errors, time-to-live exceeded, errors discovered in processing their IP options, and so forth.
ipInAddrErrors	The number of input datagrams discarded because the IP address in their IP header's destination field was not a valid address to be received at this entity (the switch). This count includes invalid addresses (for example, 0.0.0.0) and addresses of unsupported Classes (for example, Class E). For entities which are not IP Gateways and therefore do not forward datagrams, this counter includes datagrams discarded because the destination address was not a local address.

Table 79 IP Statistics

Statistic	Description
ipForwDatagrams	The number of input datagrams for which this entity (the switch) was not their final IP destination, as a result of which an attempt was made to find a route to forward them to that final destination. In entities which do not act as IP Gateways, this counter will include only those packets, which were Source-Routed via this entity (the switch), and the Source-Route option processing was successful.
ipInUnknownProtos	The number of locally addressed datagrams received successfully but discarded because of an unknown or unsupported protocol.
ipInDiscards	The number of input IP datagrams for which no problems were encountered to prevent their continued processing, but which were discarded (for example, for lack of buffer space). Note that this counter does not include any datagrams discarded while awaiting re-assembly.
ipInDelivers	The total number of input datagrams successfully delivered to IP user-protocols (including ICMP).
ipOutRequests	The total number of IP datagrams which local IP user-protocols (including ICMP) supplied to IP in requests for transmission. Note that this counter does not include any datagrams counted in ipForwDatagrams.
ipOutDiscards	The number of output IP datagrams for which no problem was encountered to prevent their transmission to their destination, but which were discarded (for example, for lack of buffer space). Note that this counter would include datagrams counted in ipForwDatagrams if any such packets met this (discretionary) discard criterion.
ipOutNoRoutes	The number of IP datagrams discarded because no route could be found to transmit them to their destination. Note that this counter includes any packets counted in ipForwDatagrams, which meet this <i>no-route</i> criterion. Note that this includes any datagrams which a host cannot route because all of its default gateways are down.
ipReasmReqds	The number of IP fragments received which needed to be reassembled at this entity (the switch).
ipReasmOKs	The number of IP datagrams successfully re- assembled.

Table 79 IP Statistics

Statistic	Description
ipReasmFails	The number of failures detected by the IP re- assembly algorithm (for whatever reason: timed out, errors, and so forth). Note that this is not necessarily a count of discarded IP fragments since some algorithms (notably the algorithm in RFC 815) can lose track of the number of fragments by combining them as they are received.
ipFragOKs	The number of IP datagrams that have been successfully fragmented at this entity (the switch).
ipFragFails	The number of IP datagrams that have been discarded because they needed to be fragmented at this entity (the switch) but could not be, for example, because their <code>Don't Fragment</code> flag was set.
ipFragCreates	The number of IP datagram fragments that have been generated as a result of fragmentation at this entity (the switch).
ipRoutingDiscards	The number of routing entries, which were chosen to be discarded even though they are valid. One possible reason for discarding such an entry could be to free-up buffer space for other routing entries.
ipDefaultTTL	The default value inserted into the <code>Time-To-Live</code> (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.
ipReasmTimeout	The maximum number of seconds, which received fragments are held while they are awaiting reassembly at this entity (the switch).

IPv6 Statistics

The following command displays IPv6 statistics:

show ipv6 counters

Command mode: All

Use the following command to clear IPv6 statistics:

clear ipv6 counters

```

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

ICMP Statistics
*****
Received :
33 ICMPPkts      0 ICMPErrPkt      0 DestUnreach  0 TimeExcds
0   ParmProbs    0 PktTooBigMsg    9 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 PktTooBigMsgs  10 EchoReq      9 EchoReply
0   RouterSols   0 RouterAdv      11 NeighSols    5 NeighborAdv
0   RedirectMsgs 0 AdminProhibMsgs

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

```

Table 80 describes the IPv6 statistics.

Table 80 IPv6 Statistics

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

Table 80 IPv6 Statistics

Statistic	Description
OutNoRoutes	Number of IP datagrams discarded because no route could be found to transmit them to their destination. Note that this includes any datagrams which a host cannot route because all of its default gateways are down.
ReasmReqds	Number of IP fragments received which needed to be reassembled at this entity (the switch).
ReasmOKs	Number of IP datagrams successfully re- assembled.
ReasmFails	Number of failures detected by the IP re- assembly algorithm (for whatever reason: timed out, errors, and so forth). Note that this is not necessarily a count of discarded IP fragments since some algorithms (notably the algorithm in RFC 815) can lose track of the number of fragments by combining them as they are received.
FragOKs	Number of IP datagrams that have been successfully fragmented at this entity (the switch).
FragFails	Number of IP datagrams that have been discarded because they needed to be fragmented at this entity (the switch) but could not be, for example, because their <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 81 ICMP Statistics

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

Table 81 ICMP Statistics

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

[Table 82](#) describes the UDP statistics.

Table 82 UDP Statistics

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

Route Statistics

The following command displays route statistics:

show ip route counters

Command mode: All

Route statistics:			
ipRoutesCur:	11	ipRoutesHighWater:	11
ipRoutesMax:	2048		

Table 83 Route Statistics

Statistic	Description
ipRoutesCur	The total number of outstanding routes in the route table.
ipRoutesHighWater	The highest number of routes ever recorded in the route table.
ipRoutesMax	The maximum number of routes that are supported.

ARP statistics

The following command displays Address Resolution Protocol statistics.

show ip arp counters

Command mode: All

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

Table 84 ARP Statistics

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

DNS Statistics

The following command displays Domain Name System statistics.

show ip dns counters

Command mode: All

DNS statistics:	
dnsOutRequests:	0
dnsBadRequests:	0

Table 85 DNS Statistics

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

ICMP Statistics

The following command displays ICMP statistics:

show ip icmp counters

Command mode: All

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

Table 86 ICMP Statistics

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

Table 86 ICMP Statistics

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

TCP Statistics

The following command displays TCP statistics:

show ip tcp counters

Command mode: All

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

Table 87 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 LBOUND 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 UBOUND 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.

Table 87 TCP Statistics

Statistic	Description
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.
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).
tcpCurBuff	The total number of outstanding memory allocations from heap by TCP protocol stack.
tcpCurConn	The total number of outstanding TCP sessions that are currently opened.
tcpOutRsts	The number of TCP segments sent containing the RST flag.

UDP Statistics

The following command displays UDP statistics:

show ip udp counters

Command mode: All

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

Table 88 UDP Statistics

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

IGMP Statistics

The following command displays statistics about the use of the IGMP Multicast Groups:

show ip igmp counters

Command mode: All

IGMP Snoop vlan 2 statistics:			

rxIgmpValidPkts:	0	rxIgmpInvalidPkts:	0
rxIgmpGenQueries:	0	rxIgmpGrpSpecificQueries:	0
rxIgmpGroupSrcSpecificQueries:	0		
rxIgmpLeaves:	0	rxIgmpReports:	0
txIgmpReports:	0	txIgmpGrpSpecificQueries:	0
txIgmpLeaves:	0	rxIgmpV3CurrentStateRecords:	0
rxIgmpV3SourceListChangeRecords:	0	rxIgmpV3FilterChangeRecords:	0

Table 89 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
rxIgmpLeaves	Total number of Leave requests received
rxIgmpReports	Total number of Membership Reports received
txIgmpReports	Total number of Membership reports transmitted
txIgmpGrpSpecificQueries	Total number of Membership Query packets transmitted to specific groups
txIgmpLeaves	Total number of Leave messages transmitted
rxIgmpV3CurrentStateRecords	Total number of Current State records received
rxIgmpV3SourceListChangeRecords	Total number of Source List Change records received.
rxIgmpV3FilterChangeRecords	Total number of Filter Change records received.

OSPF Statistics

Table 90 OSPF Statistics Commands

Command Syntax and Usage

show ip ospf counters

Displays OSPF statistics.

Command mode: All

See [page 173](#) for sample output.

show ip ospf area counters

Displays OSPF area statistics.

Command mode: All except User EXEC

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

Displays OSPF interface statistics.

Command mode: All except User EXEC

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 91 OSPF General Statistics

Statistic	Description
Rx/Tx Stats:	
Rx Pkts	The sum total of all OSPF packets received on all OSPF areas and interfaces.
Tx Pkts	The sum total of all OSPF packets transmitted on all OSPF areas and interfaces.
Rx Hello	The sum total of all Hello packets received on all OSPF areas and interfaces.
Tx Hello	The sum total of all Hello packets transmitted on all OSPF areas and interfaces.
Rx Database	The sum total of all Database Description packets received on all OSPF areas and interfaces.
Tx Database	The sum total of all Database Description packets transmitted on all OSPF areas and interfaces.
Rx ls Requests	The sum total of all Link State Request packets received on all OSPF areas and interfaces.
Tx ls Requests	The sum total of all Link State Request packets transmitted on all OSPF areas and interfaces.
Rx ls Acks	The sum total of all Link State Acknowledgement packets received on all OSPF areas and interfaces.
Tx ls Acks	The sum total of all Link State Acknowledgement packets transmitted on all OSPF areas and interfaces.
Rx ls Updates	The sum total of all Link State Update packets received on all OSPF areas and interfaces.
Tx ls Updates	The sum total of all Link State Update packets transmitted on all OSPF areas and interfaces.

Table 91 OSPF General Statistics

Statistic	Description
Nbr Change Stats:	
hello	The sum total of all Hello packets received from neighbors on all OSPF areas and interfaces.
Start	The sum total number of neighbors in this state (that is, an indication that Hello packets should now be sent to the neighbor at intervals of <code>HelloInterval</code> seconds.) across all OSPF areas and interfaces.
n2way	The sum total number of bidirectional communication establishment between this router and other neighboring routers.
adjoint ok	The sum total number of decisions to be made (again) as to whether an adjacency should be established/maintained with the neighbor across all OSPF areas and interfaces.
negotiation done	The sum total number of neighbors in this state wherein the Master/slave relationship has been negotiated, and sequence numbers have been exchanged, across all OSPF areas and interfaces.
exchange done	The sum total number of neighbors in this state (that is, in an adjacency's final state) having transmitted a full sequence of Database Description packets, across all OSPF areas and interfaces.
bad requests	The sum total number of Link State Requests which have been received for a link state advertisement not contained in the database across all interfaces and OSPF areas.
bad sequence	<p>The sum total number of Database Description packets which have been received that either:</p> <ul style="list-style-type: none"> a. Has an unexpected DD sequence number b. Unexpectedly has the init bit set c. Has an options field differing from the last Options field received in a Database Description packet. <p>Any of these conditions indicate that some error has occurred during adjacency establishment for all OSPF areas and interfaces.</p>
loading done	The sum total number of link state updates received for all out-of-date portions of the database across all OSPF areas and interfaces.
n1way	The sum total number of Hello packets received from neighbors, in which this router is not mentioned across all OSPF interfaces and areas.

Table 91 OSPF General Statistics

Statistic	Description
rst_ad	The sum total number of times the Neighbor adjacency has been reset across all OPSF areas and interfaces.
down	The total number of Neighboring routers down (that is, in the initial state of a neighbor conversation.) across all OSPF areas and interfaces.
Intf Change Stats:	
hello	The sum total number of Hello packets sent on all interfaces and areas.
down	The sum total number of interfaces down in all OSPF areas.
loop	The sum total of interfaces no longer connected to the attached network across all OSPF areas and interfaces.
unloop	The sum total number of interfaces, connected to the attached network in all OSPF areas.
wait timer	The sum total number of times the Wait Timer has been fired, indicating the end of the waiting period that is required before electing a (Backup) Designated Router across all OSPF areas and interfaces.
backup	The sum total number of Backup Designated Routers on the attached network for all OSPF areas and interfaces.
nbr change	The sum total number of changes in the set of bidirectional neighbors associated with any interface across all OSPF areas.

Table 91 OSPF General Statistics

Statistic	Description
Timers Kickoff:	
hello	The sum total number of times the Hello timer has been fired (which triggers the send of a Hello packet) across all 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 92 OSPFv3 Statistics Commands

Command Syntax and Usage

show ipv6 ospf counters

Displays OSPFv3 statistics.

Command mode: All

See [page 173](#) for sample output.

show ipv6 ospf area counters

Displays OSPFv3 area statistics.

Command mode: All except User EXEC

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

Displays OSPFv3 interface statistics.

Command mode: All except User EXEC

OSPFv3 Global Statistics

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

show ipv6 ospf counters

Command mode: All

OSPFv3 stats			

Rx/Tx/Disd Stats:	Rx	Tx	Discarded
	-----	-----	-----
Pkts	9695	95933	0
hello	9097	8994	0
database	39	51	6
ls requests	16	8	0
ls acks	172	360	0
ls updates	371	180	0
Nbr change stats:		Intf change Stats:	
down	0	down	5
attempt	0	loop	0
init	1	waiting	6
n2way	1	ptop	0
exstart	1	dr	4
exchange done	1	backup	6
loading done	1	dr other	0
full	1	all events	33
all events	6		
Timers kickoff			
hello	8988		
wait	6		
poll	0		
nbr probe	0		
Number of LSAs			
originated		180	
rcvd newer originations		355	

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

Table 93 OSPFv3 General Statistics

Statistics	Description
Rx/Tx Stats:	
Rx Pkts	The sum total of all OSPFv3 packets received on all OSPFv3 interfaces.
Tx Pkts	The sum total of all OSPFv3 packets transmitted on all OSPFv3 interfaces.
Discarded Pkts	The sum total of all OSPFv3 packets discarded.
Rx hello	The sum total of all Hello packets received on all OSPFv3 interfaces.
Tx hello	The sum total of all Hello packets transmitted on all OSPFv3 interfaces.
Discarded hello	The sum total of all Hello packets discarded, including packets for which no associated interface has been found.
Rx database	The sum total of all Database Description packets received on all OSPFv3 interfaces.
Tx database	The sum total of all Database Description packets transmitted on all OSPFv3 interfaces.
Discarded database	The sum total of all Database Description packets discarded.
Rx ls requests	The sum total of all Link State Request packets received on all OSPFv3 interfaces.
Tx ls requests	The sum total of all Link State Request packets transmitted on all OSPFv3 interfaces.
Discarded ls requests	The sum total of all Link State Request packets discarded.
Rx ls acks	The sum total of all Link State Acknowledgement packets received on all OSPFv3 interfaces.
Tx ls acks	The sum total of all Link State Acknowledgement packets transmitted on all OSPFv3 interfaces.
Discarded ls acks	The sum total of all Link State Acknowledgement packets discarded.
Rx ls updates	The sum total of all Link State Update packets received on all OSPFv3 interfaces.
Tx ls updates	The sum total of all Link State Update packets transmitted on all OSPFv3 interfaces.

Table 93 OSPFv3 General Statistics

Statistics	Description
Discarded ls updates	The sum total of all Link State Update packets discarded.
Nbr Change Stats:	
down	The total number of Neighboring routers down (that is, in the initial state of a neighbor conversation.) across all OSPFv3 interfaces.
attempt	The total number of transitions into attempt state of neighboring routers across all OSPFv3 interfaces.
init	The total number of transitions into init state of neighboring routers across all OSPFv3 interfaces.
n2way	The total number of bidirectional communication establishment between this router and other neighboring routers.
exstart	The total number of transitions into exstart state of neighboring routers across all OSPFv3 interfaces
exchange done	The total number of neighbors in this state (that is, in an adjacency's final state) having transmitted a full sequence of Database Description packets, across all OSPFv3 interfaces.
loading done	The total number of link state updates received for all out-of-date portions of the database across all OSPFv3 interfaces.
full	The total number of transitions into full state of neighboring routers across all OSPFv3 interfaces.
all events	The total number of state transitions of neighboring routers across all OSPFv3 interfaces.

Table 93 OSPFv3 General Statistics

Statistics	Description
Intf Change Stats:	
down	The total number of transitions into down state of all OSPFv3 interfaces.
loop	The total number of transitions into loopback state of all OSPFv3 interfaces.
waiting	The total number of transitions into waiting state of all OSPFv3 interfaces.
ptop	The total number of transitions into point-to-point state of all OSPFv3 interfaces.
dr	The total number of transitions into Designated Router other state of all OSPFv3 interfaces.
backup	The total number of transitions into backup state of all OSPFv3 interfaces.
all events	The total number of changes associated with any OSPFv3 interface, including changes into internal states.
Timers Kickoff:	
hello	The total number of times the Hello timer has been fired (which triggers the send of a Hello packet) across all OSPFv3 interfaces.
wait	The total number of times the wait timer has been fired (which causes an interface to exit waiting state), across all OPSFv3 interfaces.
poll	The total number of times the timer whose firing causes hellos to be sent to inactive NBMA and Demand Circuit neighbors has been fired, across all OPSFv3 interfaces.
nbr probe	The total number of times the neighbor probe timer has been fired, across all OPSFv3 interfaces.
Number of LSAs:	
originated	The number of LSAs originated by this router.
rcvd newer originations	The number of LSAs received that have been determined to be newer originations.

VRRP Statistics

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

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

show ip vrrp counters

Command mode: All

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

Table 94 VRRP Statistics

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

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
```


Management Processor Statistics

Table 95 Management Processor Statistics Commands

Command Syntax and Usage

show mp packet

Displays packet statistics, to check for leads and load.

Command mode: All

To view a sample output and a description of the stats, see [page 186](#).

show mp tcp-block

Displays all TCP control blocks that are in use.

Command mode: All

To view a sample output and a description of the stats, see [page 188](#).

show mp udp-block

Displays all UDP control blocks that are in use.

Command mode: All

To view a sample output, see [page 188](#).

show mp cpu

Displays CPU utilization for periods of up to 1, 4, and 64 seconds.

Command mode: All

To view a sample output and a description of the stats, see [page 189](#).

MP Packet Statistics

The following command displays MP packet statistics:

show mp packet

Command mode: All except User EXEC

```
Packet counts seen by MP:
allocs:          859
frees:           859
failures:         0

  small packet buffers:
  -----
    current:              0
    hi-watermark:         4
    hi-water time:  17:56:35 Tue Jul 14, 2009

  medium packet buffers:
  -----
    current:              0
    hi-watermark:         1
    hi-water time:  17:56:16 Tue Jul 14, 2009

  jumbo packet buffers:
  -----
    current:              0
    hi-watermark:         0
```

Table 96 Packet Statistics

Statistics	Description
allocs	Total number of packet allocations from the packet buffer pool by the TCP/IP protocol stack.
frees	Total number of times the packet buffers are freed (released) to the packet buffer pool by the TCP/IP protocol stack.
failures	Total number of packet allocation failures from the packet buffer pool by the TCP/IP protocol stack.
small packet buffers	
current	Total number of packet allocations with size less than 128 bytes from the packet buffer pool by the TCP/IP protocol stack.
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.

Table 96 Packet Statistics

Statistics	Description
hi-water time	Time stamp that indicates when the hi-watermark was reached.
medium packet buffers	
current	Total number of packet allocations with size between 128 to 1536 bytes from the packet buffer pool by the TCP/IP protocol stack.
hi-watermark	The highest number of packet allocation with size between 128 to 1536 bytes from the packet buffer pool by the TCP/IP protocol stack.
hi-water time	Time stamp that indicates when the hi-watermark was reached.
jumbo packet buffers	
current	Total number of packet allocations with more than 1536 bytes from the packet buffer pool by the TCP/IP protocol stack.
hi-watermark	The highest number of packet allocation with more than 1536 bytes from the packet buffer pool by the TCP/IP protocol stack.

TCP Statistics

The following command displays TCP statistics:

show mp tcp-block

Command mode: All except User EXEC

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

Table 97 MP Specified TCP Statistics

Statistics	Description
10ad41e8/10ad5790	Memory
0.0.0.0/47.81.27.5	Destination IP address
0/1171	Destination port
0.0.0.0/47.80.23.243	Source IP
80/23	Source port
listen/established	State

UDP Statistics

The following command displays UDP statistics:

show mp udp-block

Command mode: All except User EXEC

All UDP allocated control blocks:				
161:	listen			

CPU Statistics

The following command displays the CPU utilization statistics:

show mp cpu

Command mode: All except User EXEC.

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

Table 98 CPU Statistics

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

Access Control List Statistics

Table 99 ACL Statistics Commands

Command Syntax and Usage

show access-control list <1-640> counters

Displays the Access Control List Statistics for a specific ACL.

Command mode: All

show access-control counters

Displays all ACL statistics.

Command mode: All except User EXEC

show access-control vmap <1-128> counters

Displays VLAN Map statistics for the selected VMAP. For details, see [page 191](#).

Command mode: All

clear access-control list

Clears ACL statistics.

Command mode: All except User EXEC

ACL Statistics

This option displays statistics for the selected ACL.

show access-control counters

Command mode: All

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

VMAP Statistics

This option displays statistics for the selected VLAN Map.

show access-control vmap <1-128> **counters**

Command mode: All

Hits for VMAP 1:	57515
Hits for VMAP 2:	74970

SNMP Statistics

The following command displays SNMP statistics:

show snmp-server counters

Command mode: All except User EXEC

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

Table 100 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 100 SNMP Statistics

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

Table 100 SNMP Statistics

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

Table 100 SNMP Statistics

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

NTP Statistics

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

The following command displays NTP statistics:

show ntp counters

Command mode: All

```
NTP statistics:
  Primary Server:
    Requests Sent:          17
    Responses Received:     17
    Updates:                1
  Secondary Server:
    Requests Sent:          0
    Responses Received:     0
    Updates:                0

Last update based on response from primary/secondary server.
Last update time: 18:04:16 Tue Jul 13, 2009
Current system time: 18:55:49 Tue Jul 13, 2009
```

Table 101 NTP Statistics

Field	Description
Primary Server	<ul style="list-style-type: none"> ■ Requests Sent: The total number of NTP requests the switch sent to the primary NTP server to synchronize time. ■ Responses Received: The total number of NTP responses received from the primary NTP server. ■ Updates: The total number of times the switch updated its time based on the NTP responses received from the primary NTP server.
Secondary Server	<ul style="list-style-type: none"> ■ Requests Sent: The total number of NTP requests the switch sent to the secondary NTP server to synchronize time. ■ Responses Received: The total number of NTP responses received from the secondary NTP server. ■ Updates: The total number of times the switch updated its time based on the NTP responses received from the secondary NTP server.
Last update based on response from primary server	Last update of time on the switch based on either primary or secondary NTP response received.
Last update time	The time stamp showing the time when the switch was last updated.
Current system time	The switch system time when the following command was issued: show ntp counters

Statistics Dump

The following command dumps switch statistics:

show counters

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

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

CHAPTER 4

Configuration Commands

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

Table 102 General Configuration Commands

Command Syntax and Usage

show running-config

Dumps current configuration to a script file.

Command mode: All

For details, see [page 407](#).

copy running-config backup-config

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

Command mode: All

For details, see [page 407](#).

copy running-config startup-config

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

Command mode: All

Table 102 General Configuration Commands

Command Syntax and Usage

copy running-config {ftp|tftp}

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

Command mode: All

copy {ftp|tftp} running-config

Restores current configuration from a FTP/TFTP server.

Command mode: All

For details, see [page 408](#).

Viewing and Saving Changes

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

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

Saving the Configuration

You must save configuration settings to flash memory, so the GbESM 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 425](#).

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 103 System Configuration Commands

Command Syntax and Usage

system date <yyyy> <mm> <dd>

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

Command mode: Global configuration

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

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

Command mode: Global configuration

system timezone

Configures the time zone where the switch resides. You are prompted to select your location (continent, country, region) by the timezone wizard. Once a region is selected, the switch updates the time to reflect local changes to Daylight Savings Time, etc.

Command mode: Global configuration

[no] **system daylight**

Disables or enables daylight savings time in the system clock. When enabled, the switch will add an extra hour to the system clock so that it is consistent with the local clock. By default, this option is disabled.

Command mode: Global configuration

system idle <1-60>

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

Command mode: Global configuration

system linkscan {fast|normal|slow}

Configures the link scan interval used to poll the status of ports.

Command mode: Global configuration

Table 103 System Configuration Commands

Command Syntax and Usage

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

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

Command mode: Global configuration

[no] banner *<1-80 characters>*

Configures a login banner of up to 80 characters. When a user or administrator logs into the switch, the login banner is displayed. It is also displayed as part of the output from the `show sys-info` command.

Command mode: Global configuration

[no] hostname *<character string>*

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

Command mode: Global configuration

[no] system reset-control

Enables or disables the reset control flag. When enabled, the switch continues to function after a crash of the main processor, using the last known Layer 2/3 information.

Command mode: Global configuration

[no] system packet-logging

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

Command mode: Global configuration

show system

Displays the current system parameters.

Command mode: All

System Error Disable and Recovery Configuration

The Error Disable and Recovery feature allows the switch to automatically disable a port if an error condition is detected on the port. The port remains in the error-disabled state until it is re-enabled manually, or re-enabled automatically by the switch after a timeout period has elapsed. The error-disabled state of a port does not persist across a system reboot.

Table 104 Error Disable Configuration Commands

Command Syntax and Usage

errdisable timeout *<30 - 86400>*

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

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

Command mode: Global configuration

errdisable recovery

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

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

Command mode: Global configuration

no errdisable recovery

Globally disables error-recovery for error-disabled ports.

Command mode: Global configuration

show errdisable

Displays the current system Error Disable configuration.

Command mode: All

System Host Log Configuration

Table 105 Host Log Configuration Commands

Command Syntax and Usage

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

Sets the IP address of the first or second syslog host.

Command mode: Global configuration

logging host <1-2> **severity** <0-7>

This option sets the severity level of the first or second syslog host displayed. The default is 7, which means log all severity levels.

Command mode: Global configuration

logging host <1-2> **facility** <0-7>

This option sets the facility level of the first or second syslog host displayed. The default is 0.

Command mode: Global configuration

logging console

Enables delivering syslog messages to the console. It is enabled by default.

Command mode: Global configuration

no logging console

Disables delivering syslog messages to the console. When necessary, disabling console ensures the switch is not affected by syslog messages. It is enabled by default.

Command mode: Global configuration

[no] logging log [<feature>]

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

Command mode: Global configuration

show logging

Displays the current syslog settings.

Command mode: All

SSH Server Configuration

For the 1/10Gb Uplink ESM, these commands enable Secure Shell access from any SSH client.

Table 106 SSH Server Configuration Commands

Command Syntax and Usage

ssh interval *<0-24>*

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

Command mode: Global configuration

ssh scp-password

Set the administration password for SCP access.

Command mode: Global configuration

ssh generate-host-key

Generate the RSA host key.

Command mode: Global configuration

ssh generate-server-key

Generate the RSA server key.

Command mode: Global configuration

ssh port *<TCP port number>*

Sets the SSH server port number.

Command mode: Global configuration

ssh scp-enable

Enables the SCP apply and save.

Command mode: Global configuration

no ssh scp-enable

Disables the SCP apply and save.

Command mode: Global configuration

ssh enable

Enables the SSH server.

Command mode: Global configuration

Table 106 SSH Server Configuration Commands

Command Syntax and Usage
no ssh enable Disables the SSH server. Command mode: Global configuration
show ssh Displays the current SSH server configuration. Command mode: All

RADIUS Server Configuration

Table 107 RADIUS Configuration Commands

Command Syntax and Usage

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

Sets the primary RADIUS server address.

Command mode: Global configuration

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

Sets the secondary RADIUS server address.

Command mode: Global configuration

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

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

Command mode: Global configuration

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

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

Command mode: Global configuration

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

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

Command mode: Global configuration

radius-server retransmit *<1-3>*

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

Command mode: Global configuration

radius-server timeout *<1-10>*

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

Command mode: Global configuration

Table 107 RADIUS Configuration Commands

Command Syntax and Usage

[no] radius-server backdoor

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

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

Command mode: Global configuration

radius-server enable

Enables the RADIUS server.

Command mode: Global configuration

no radius-server enable

Disables the RADIUS server.

Command mode: Global configuration

show radius-server

Displays the current RADIUS server parameters.

Command mode: All

TACACS+ Server Configuration

TACACS (Terminal Access Controller Access Control system) is an authentication protocol that allows a remote access server to forward a user's login 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. (TACACS is 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 108 TACACS+ Server Commands

Command Syntax and Usage

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

Defines the primary TACACS+ server address.

Command mode: Global configuration

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

Defines the secondary TACACS+ server address.

Command mode: Global configuration

[no] tacacs-server primary-host *<IP address>* **key** *<1-32 characters>*

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

Command mode: Global configuration

[no] tacacs-server secondary-host *<IP address>* **key** *<1-32 characters>*

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

Command mode: Global configuration

Table 108 TACACS+ Server Commands**Command Syntax and Usage****[default]** **tacacs-server port** *<TCP port number>*

Enter the number of the TCP port to be configured, between 1 and 65000. The default is 49.

Command mode: Global configuration

tacacs-server retransmit *<1-3>*

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

Command mode: Global configuration

tacacs-server attempts *<1-10>*

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

Command mode: Global configuration

tacacs-server timeout *<4-15>*

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

Command mode: Global configuration

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

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

Command mode: Global configuration

[no] **tacacs-server backdoor**

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

Enabling this feature allows you to bypass the TACACS+ servers. It is recommended that you use Secure Backdoor to ensure the switch is secured, because Secure Backdoor disallows access through the back door when the TACACS+ servers are responding.

The default setting is disabled.

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

Command mode: Global configuration

Table 108 TACACS+ Server Commands**Command Syntax and Usage****[no] tacacs-server secure-backdoor**

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

This feature is recommended to permit access to the switch when the TACACS+ servers become unresponsive. If no back door is enabled, the only way to gain access when TACACS+ servers are unresponsive is to use the back door via the console port.

The default is `disabled`.

Command mode: Global configuration

[no] tacacs-server privilege-mapping

Enables or disables TACACS+ privilege-level mapping.

The default value is `disabled`.

Command mode: Global configuration

[no] tacacs-server password-change

Enables or disables TACACS+ password change.

The default value is `disabled`.

Command mode: Global configuration

primary-password

Configures the password for the primary TACACS+ server. The CLI will prompt you for input.

Command mode: Global configuration

secondary-password

Configures the password for the secondary TACACS+ server. The CLI will prompt you for input.

Command mode: Global configuration

[no] tacacs-server command-authorization

Enables or disables TACACS+ command authorization.

Command mode: Global configuration

Table 108 TACACS+ Server Commands

Command Syntax and Usage

[no] tacacs-server command-logging

Enables or disables TACACS+ command logging.

Command mode: Global configuration

[no] tacacs-server directed-request [restricted|no-truncate]

Enables or disables TACACS+ directed request, which uses a specified TACACS+ server for authentication, authorization, accounting. When enabled, When directed-request is enabled, each user must add a configured TACACS+ server hostname to the username (for example, username@hostname) during login.

This command allows the following options:

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

[no] tacacs-server enable

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

Command mode: Global configuration

show tacacs-server

Displays current TACACS+ configuration parameters.

Command mode: All

LDAP Server Configuration

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

Table 109 LDAP Configuration commands

Command Syntax and Usage

[no] ldap-server primary-host *<IP address>*

Sets the primary LDAP server address.

Command mode: Global configuration

[no] ldap-server secondary-host *<IP address>*

Sets the secondary LDAP server address.

Command mode: Global configuration

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

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

Command mode: Global configuration

ldap-server retransmit *<1-3>*

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

Command mode: Global configuration

ldap-server timeout *<4-15>*

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

Command mode: Global configuration

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

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

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

Command mode: Global configuration

Table 109 LDAP Configuration commands

Command Syntax and Usage	
[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 GbESM, contact your Service and Support line.</p> <p>Command mode: Global configuration</p>
ldap-server enable	<p>Enables the LDAP server.</p> <p>Command mode: Global configuration</p>
no ldap-server enable	<p>Disables the LDAP server.</p> <p>Command mode: Global configuration</p>
show ldap-server	<p>Displays the current LDAP server parameters.</p> <p>Command mode: All</p>

NTP Server Configuration

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

Table 110 NTP Configuration Commands

Command Syntax and Usage

[no] ntp primary-server *<IP address>*

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

Command mode: Global configuration

[no] ntp secondary-server *<IP address>*

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

Command mode: Global configuration

[no] ntp ipv6 primary-server *<IPv6 address>*

Prompts for the IPv6 addresses of the primary NTP server to which you want to synchronize the switch clock.

Note: To delete the IPv6 primary server, use the following command:

no ntp primary-server *<IP address>*

Command mode: Global configuration

[no] ntp ipv6 secondary-server *<IPv6 address>*

Prompts for the IPv6 addresses of the secondary NTP server to which you want to synchronize the switch clock.

Note: To delete the IPv6 secondary server, use the following command:

no ntp secondary-server *<IP address>*

Command mode: Global configuration

ntp interval *<5-44640>*

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

Command mode: Global configuration

Table 110 NTP Configuration Commands

Command Syntax and Usage

ntp enable

Enables the NTP synchronization service.

Command mode: Global configuration

no ntp enable

Disables the NTP synchronization service.

Command mode: Global configuration

show ntp

Displays the current NTP service settings.

Command mode: All

System SNMP Configuration

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

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

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

SNMP parameters that can be modified include:

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

Table 111 System SNMP Commands

Command Syntax and Usage

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

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

Command mode: Global configuration

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

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

Command mode: Global configuration

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

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

Command mode: Global configuration

Table 111 System SNMP Commands**Command Syntax and Usage****snmp-server read-community** <1-32 characters>

Configures the SNMP read community string. The read community string controls SNMP “get” access to the switch. It can have a maximum of 32 characters. The default read community string is *public*.

Command mode: Global configuration

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

Configures the SNMP write community string. The write community string controls SNMP “set” and “get” access to the switch. It can have a maximum of 32 characters. The default write community string is *private*.

Command mode: Global configuration

snmp-server timeout <1-30>

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

Command mode: Global configuration

[no] snmp-server authentication-trap

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

Command mode: Global configuration

[no] snmp-server link-trap

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

Command mode: Global configuration

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

Configures the source interface for SNMP traps.

To send traps through the management ports, specify interface 128.

Command mode: Global configuration

show snmp-server

Displays the current SNMP configuration.

Command mode: All

SNMPv3 Configuration

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

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

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

Table 112 SNMPv3 Configuration Commands

Command Syntax and Usage
snmp-server user <1-16> This command allows you to create a user security model (USM) entry for an authorized user. You can also configure this entry through SNMP. Command mode: Global configuration To view command options, see page 221 .
snmp-server view <1-128> This command allows you to create different MIB views. Command mode: Global configuration To view command options, see page 222 .
snmp-server access <1-32> This command allows you to specify access rights. The View-based Access Control Model defines a set of services that an application can use for checking access rights of the user. You need access control when you have to process retrieval or modification request from an SNMP entity. Command mode: Global configuration To view command options, see page 224 .

Table 112 SNMPv3 Configuration Commands

snmp-server group <1-16>

A group maps the user name to the access group names and their access rights needed to access SNMP management objects. A group defines the access rights assigned to all names that belong to a particular group.

Command mode: Global configuration

To view command options, see [page 226](#).

snmp-server community <1-16>

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

Command mode: Global configuration

To view command options, see [page 227](#).

snmp-server target-address <1-16>

This command allows you to configure destination information, consisting of a transport domain and a transport address. This is also termed as transport endpoint. The SNMP MIB provides a mechanism for performing source address validation on incoming requests, and for selecting community strings based on target addresses for outgoing notifications.

Command mode: Global configuration

To view command options, see [page 228](#).

snmp-server target-parameters <1-16>

This command allows you to configure SNMP parameters, consisting of message processing model, security model, security level, and security name information. There may be multiple transport endpoints associated with a particular set of SNMP parameters, or a particular transport endpoint may be associated with several sets of SNMP parameters.

Command mode: Global configuration

To view command options, see [page 229](#).

snmp-server notify <1-16>

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

Command mode: Global configuration

To view command options, see [page 231](#).

Table 112 SNMPv3 Configuration Commands

snmp-server version {v1v2v3|v3only}

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

Command mode: Global configuration

show snmp-server v3

Displays the current SNMPv3 configuration.

Command mode: All

User Security Model Configuration

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

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

Table 113 User Security Model Configuration Commands

Command Syntax and Usage

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

This command allows you to configure a string that represents the name of the user. This is the login name that you need in order to access the switch.

Command mode: Global configuration

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

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

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

When you configure an authentication algorithm, you must provide a password, otherwise you will get an error message during validation. This command allows you to create or change your password for authentication.

Command mode: Global configuration

Table 113 User Security Model Configuration Commands

Command Syntax and Usage

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

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

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

You can create or change the privacy password.

Command mode: Global configuration

no snmp-server user <1-16>

Deletes the USM user entries.

Command mode: Global configuration

show snmp-server v3 user <1-16>

Displays the USM user entries.

Command mode: All

SNMPv3 View Configuration

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

Table 114 SNMPv3 View Configuration Commands

Command Syntax and Usage

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

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

Command mode: Global configuration

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

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

Command mode: Global configuration

Table 114 SNMPv3 View Configuration Commands

Command Syntax and Usage

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

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

Command mode: Global configuration

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

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

Command mode: Global configuration

no snmp-server view <1-128>

Deletes the `vacmViewTreeFamily` group entry.

Command mode: Global configuration

show snmp-server v3 view <1-128>

Displays the current `vacmViewTreeFamily` configuration.

Command mode: All

View-based Access Control Model Configuration

The view-based Access Control Model defines a set of services that an application can use for checking access rights of the user. Access control is needed when the user has to process SNMP retrieval or modification request from an SNMP entity.

Table 115 View-based Access Control Model Commands

Command Syntax and Usage

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

Defines the name of the group.

Command mode: Global configuration

snmp-server access <1-32> **prefix** <1-32 characters>

Defines the name of the context. An SNMP context is a collection of management information that an SNMP entity can access. An SNMP entity has access to many contexts. For more information on naming the management information, see RFC2571, the SNMP Architecture document.

The view-based Access Control Model defines a table that lists the locally available contexts by contextName.

Command mode: Global configuration

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

Allows you to select the security model to be used.

Command mode: Global configuration

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

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

Command mode: Global configuration

snmp-server access <1-32> **match** {exact|prefix}

If the value is set to `exact`, then all the rows whose contextName exactly matches the prefix are selected. If the value is set to `prefix` then the all the rows where the starting octets of the contextName exactly match the prefix are selected.

Command mode: Global configuration

Table 115 View-based Access Control Model Commands**Command Syntax and Usage**

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

Defines a read view name that allows you read access to a particular MIB view. If the value is empty or if there is no active MIB view having this value then no access is granted.

Command mode: Global configuration

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

Defines a write view name that allows you write access to the MIB view. If the value is empty or if there is no active MIB view having this value then no access is granted.

Command mode: Global configuration

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

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

Command mode: Global configuration

no snmp-server access <1-32>

Deletes the View-based Access Control entry.

Command mode: Global configuration

show snmp-server v3 access <1-32>

Displays the View-based Access Control configuration.

Command mode: All

SNMPv3 Group Configuration

Table 116 SNMPv3 Group Configuration Commands

Command Syntax and Usage

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

Defines the security model.

Command mode: Global configuration

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

Sets the user name as defined in the following command on [page 221](#):
snmp-server user <1-16> name <1-32 characters>

Command mode: Global configuration

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

The name for the access group as defined in the following command:
snmp-server access <1-32> name <1-32 characters> on [page 221](#).

Command mode: Global configuration

no snmp-server group <1-16>

Deletes the vacmSecurityToGroup entry.

Command mode: Global configuration

show snmp-server v3 group <1-16>

Displays the current vacmSecurityToGroup configuration.

Command mode: All

SNMPv3 Community Table Configuration

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

Table 117 SNMPv3 Community Table Configuration Commands

Command Syntax and Usage

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

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

Command string: Global configuration

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

Defines the user name as defined in the following command on [page 221](#):

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

Command string: Global configuration

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

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

Command mode: Global configuration

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

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

Command mode: Global configuration

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

Deletes the community table entry.

Command mode: Global configuration

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

Displays the community table configuration.

Command mode: All

SNMPv3 Target Address Table Configuration

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

Table 118 Target Address Table Configuration Commands

Command Syntax and Usage

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

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

Command mode: Global configuration

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

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

Command mode: Global configuration

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

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

Command mode: Global configuration

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

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

Command mode: Global configuration

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

Defines the name as defined in the following command on [page 229](#):
`snmp-server target-parameters` <1-16> **name** <1-32 characters>

Command mode: Global configuration

Table 118 Target Address Table Configuration Commands**Command Syntax and Usage**

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

Deletes the Target Address Table entry.

Command mode: Global configuration

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

Displays the current Target Address Table configuration.

Command mode: All

SNMPv3 Target Parameters Table Configuration

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

Table 119 Target Parameters Table Configuration Commands**Command Syntax and Usage**

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

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

Command mode: Global configuration

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

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

Command mode: Global configuration

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

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

Command mode: Global configuration

Table 119 Target Parameters Table Configuration Commands

Command Syntax and Usage

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

Defines the name that identifies the user in the USM table (page 221) on whose behalf the SNMP messages are generated using this entry.

Command mode: Global configuration

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

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

Command mode: Global configuration

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

Deletes the targetParamsTable entry.

Command mode: Global configuration

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

Displays the current targetParamsTable configuration.

Command mode: All

SNMPv3 Notify Table Configuration

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

Table 120 Notify Table Commands

Command Syntax and Usage

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

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

Command mode: Global configuration

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

Allows you to configure a tag that contains a tag value which is used to select entries in the Target Address Table. Any entry in the `snmpTargetAddrTable`, that matches the value of this tag, is selected.

Command mode: Global configuration

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

Deletes the notify table entry.

Command mode: Global configuration

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

Displays the current notify table configuration.

Command mode: All

System Access Configuration

Table 121 System Access Configuration Commands

Command Syntax and Usage

access user administrator-password

access user operator-password

access user user-password

Allows you to change the password. You must enter the current password in use for validation.

Command Mode: Global configuration

[no] access http enable

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

Command mode: Global configuration

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

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

Command mode: Global configuration

[no] access snmp {read-only|read-write}

Disables or provides read-only/write-read SNMP access.

Command mode: Global configuration

[no] access telnet enable

Enables or disables Telnet access. This command is enabled by default.

Command mode: Global configuration

[default] access telnet port [*<1-65535>*]

Sets an optional Telnet server port number for cases where the server listens for Telnet sessions on a non-standard port.

Command mode: Global configuration

[default] access tftp-port [*<1-65535>*]

Sets the TFTP port for the switch. The default is port 69.

Command mode: Global configuration

Table 121 System Access Configuration Commands**Command Syntax and Usage****[no] access tsbbi enable**

Enables or disables Telnet/SSH configuration through the Browser-Based Interface (BBI).

Command mode: Global configuration

[no] access userbbi enable

Enables or disables user configuration access through the Browser-Based Interface (BBI).

Command mode: Global configuration

show access

Displays the current system access parameters.

Command mode: All

Management Network Configuration

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

Table 122 Management Network Configuration Commands**Command Syntax and Usage****access management-network** *<IP address>* *<IP mask>*

Adds a defined network through which switch access is allowed through Telnet, SNMP, RIP, or the BLADEOS browser-based interface. A range of IP addresses is produced when used with a network mask address. Specify an IP address and mask address in dotted-decimal notation.

Note: If you configure the management network without including the switch interfaces, the configuration causes the Firewall Load Balancing health checks to fail and creates a “Network Down” state on the network.

Command mode: Global configuration

no access management-network *<IP address>* *<IP mask>*

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

Command mode: Global configuration

Table 122 Management Network Configuration Commands

Command Syntax and Usage

show access management-network

Displays the current management network configuration.

Command mode: All except User EXEC

clear access management-network

Removes all defined management networks.

Command mode: Global configuration

User Access Control Configuration

The following table describes user-access control commands.

Passwords can be a maximum of 128 characters.

Table 123 User Access Control Configuration Commands

Command Syntax and Usage

access user <1-10>

Configures the User ID.

Command mode: Global configuration

access user eject <user name>

Ejects the specified user from the GbESM.

Command mode: Global configuration

access user user-password <1-128 characters>

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

Command mode: Global configuration

access user operator-password <1-128 characters>

Sets the operator (`oper`) password. The operator manages all functions of the switch. He or she can view all switch information and statistics and can reset ports or the entire switch.
Command mode: Global configuration

Table 123 User Access Control Configuration Commands

Command Syntax and Usage

access user administrator-password *<1-128 characters>*

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

Access includes “oper” functions.

Command mode: Global configuration

show access user

Displays the current user status.

Command mode: All except User EXEC

System User ID Configuration**Table 124** User ID Configuration Commands

Command Syntax and Usage

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

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

Command mode: Global configuration

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

Defines the user name of maximum eight characters.

Command mode: Global configuration

access user *<1-10>* **password**

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

Command mode: Global configuration

access user *<1-10>* **enable**

Enables the user ID.

Command mode: Global configuration

Table 124 User ID Configuration Commands

Command Syntax and Usage

no access user <1-10> enable

Disables the user ID.

Command mode: Global configuration

no access user <1-10>

Deletes the user ID.

Command mode: Global configuration

show access user

Displays the current user ID configuration.

Command mode: All except User EXEC

Strong Password Configuration

Table 125 Strong Password Configuration Commands

Command Syntax and Usage

access user strong-password enable

Enables Strong Password requirement.

Command mode: Global configuration

no access user strong-password enable

Disables Strong Password requirement.

Command mode: Global configuration

access user strong-password expiry <1-365>

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

Command mode: Global configuration

access user strong-password warning <1-365>

Configures the number of days before password expiration, that a warning is issued to users. The default value is 15 days.

Command mode: Global configuration

Table 125 Strong Password Configuration Commands

Command Syntax and Usage	
access user strong-password faillog <1-255>	
Configures the number of failed login attempts allowed before a security notification is logged. The default value is 3 login attempts.	
Command mode: Global configuration	
show access user strong-password	
Displays the current Strong Password configuration.	
Command mode: All except User EXEC	

HTTPS Access Configuration

Table 126 HTTPS Access Configuration Commands

Command Syntax and Usage

[no] access https enable

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

Command mode: Global configuration

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

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

Command mode: Global configuration

access https generate-certificate

Allows you to generate a certificate to connect to the SSL to be used during the key exchange. A default certificate is created when HTTPS is enabled for the first time. The user can create a new certificate defining the information that they want to be used in the various fields. For example:

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

You will be asked to confirm if you want to generate the certificate. It will take approximately 30 seconds to generate the certificate. Then the switch will restart SSL agent.

Command mode: Global configuration

access https save-certificate

Allows the client, or the Web browser, to accept the certificate and save the certificate to Flash to be used when the switch is rebooted.

Command mode: Global configuration

show access

Displays the current SSL Web Access configuration.

Command mode: All except User EXEC

Custom Daylight Savings Time Configuration

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

Relative offset example:

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

Calendar date example:

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

Table 127 Custom DST Configuration Commands

Command Syntax and Usage

system custom-dst start-rule *<WDDMMhh>*

Configures the start date for custom DST, as follows:

WDDMMhh

W = week (0-5, where 0 means use the calendar date)

D = day of the week (01-07, where 01 is Monday)

MM = month (1-12)

hh = hour (0-23)

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

Command mode: Global configuration

system custom-dst end-rule *<WDDMMhh>*

Configures the end date for custom DST, as follows:

WDDMMhh

W = week (0-5, where 0 means use the calendar date)

D = day of the week (01-07, where 01 is Monday)

MM = month (1-12)

hh = hour (0-23)

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

Command mode: Global configuration

system custom-dst enable

Enables the Custom Daylight Savings Time settings.

Command mode: Global configuration

Table 127 Custom DST Configuration Commands

Command Syntax and Usage

no system custom-dst enable

Disables the Custom Daylight Savings Time settings.

Command mode: Global configuration

show custom-dst

Displays the current Custom DST configuration.

Command mode: All except User EXEC

sFlow Configuration

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

Table 128 sFlow Configuration commands

Command Syntax and Usage

sflow enable

Enables the sFlow agent.

Command mode: Global configuration

no sflow enable

Disables the sFlow agent.

Command mode: Global configuration

sflow server <IP address>

Defines the sFlow server address.

Command mode: Global configuration

sflow port <1-65535>

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

Command mode: Global configuration

show sflow

Displays sFlow configuration parameters.

Command mode: All

sFlow Port Configuration

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

Table 129 sFlow Port Configuration commands

Command Syntax and Usage

[no] sflow polling <5-60>

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

Command mode: Interface port

[no] sflow sampling <256-65536>

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

Command mode: Interface port

Port Configuration

Use the Port Configuration commands to configure settings for switch ports (INTx) and (EXTx).

Table 130 Port Configuration Commands

Command Syntax and Usage

interface port *<port alias or number>*

Enter Interface port mode.

Command mode: Global configuration

dot1p *<0-7>*

Configures the port's 802.1p priority level.

Command mode: Interface port

pvid *<VLAN number>*

Sets the default VLAN number which will be used to forward frames which are not VLAN tagged. The default number is 1 for non-management ports.

Command mode: Interface port

name *<1-64 characters>*

Sets a name for the port. The assigned port name appears next to the port number on some information and statistics screens. The default is set to None.

Command mode: Interface port

[no] bpdu-guard

Enables or disables BPDU guard, to avoid spanning-tree loops on ports with Port Fast Forwarding enabled.

[no] dscp-marking

Enables or disables DSCP re-marking on a port.

Command mode: Interface port

[no] rmon

Enables or disables Remote Monitoring for the port. RMON must be enabled for any RMON configurations to function.

Command mode: Interface port

Table 130 Port Configuration Commands**Command Syntax and Usage**

[no] tagging

Disables or enables VLAN tagging for this port. The default setting is disabled for external ports (EXTx) and enabled for internal server ports (INTx).

Command mode: Interface port

[no] tag-pvid

Disables or enables VLAN tag persistence. When disabled, the VLAN tag is removed from packets whose VLAN tag matches the port PVID. The default setting is disabled for internal server ports (INTx) and external ports (EXTx), and enabled for management (MGTx) ports.

Command mode: Interface port

[no] fastforward

Disables or enables Port Fast Forwarding, which permits a port that participates in Spanning Tree to bypass the Listening and Learning states and enter directly into the Forwarding state. While in the Forwarding state, the port listens to the BPDUs to learn if there is a loop and, if dictated by normal STG behavior (following priorities, etc.), the port transitions into the Blocking state. This feature permits the GbESM to interoperate well within Rapid Spanning Tree networks.

Command mode: Interface port

[no] flood-blocking

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

Command mode: Interface port

[no] learning

Enables or disables FDB learning on the port.

Command mode: Interface port

[no] broadcast-threshold <0-262143>

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

Command mode: Interface port

Table 130 Port Configuration Commands

Command Syntax and Usage	
[no] multicast-threshold <0-262143>	Limits the number of multicast packets per second to the specified value. If disabled, the port forwards all multicast packets. Command mode: Interface port
[no] dest-lookup-threshold <0-262143>	Limits the number of unknown unicast packets per second to the specified value. If disabled, the port forwards all unknown unicast packets. Command mode: Interface port
no shutdown	Enables the port. Command mode: Interface port
shutdown	Disables the port. (To temporarily disable a port without changing its configuration attributes, refer to “Temporarily Disabling a Port” on page 247.) Command mode: Interface port
show interface port <port alias or number>	Displays current port parameters. Command mode: All

Port Error Disable and Recovery Configuration

The Error Disable and Recovery feature allows the switch to automatically disable a port if an error condition is detected on the port. The port remains in the error-disabled state until it is re-enabled manually, or re-enabled automatically by the switch after a timeout period has elapsed. The error-disabled state of a port does not persist across a system reboot.

Table 131 Port Error Disable Commands

Command Syntax and Usage

errdisable recovery

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

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

Command mode: Interface port

no errdisable recovery

Enables automatic error-recovery for the port.

Command mode: Interface port

show interface port <port alias or number> errdisable

Displays current port Error Disable parameters.

Command mode: All

Port Link Configuration

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

Table 132 Port Link Configuration Commands

Command Syntax and Usage

speed {10|100|1000|10000|auto}

Sets the link speed. Some options are not valid on all ports. The choices include:

- ☐ 10 Mbps
- ☐ 100 Mbps
- ☐ 1000 Mbps
- ☐ 10000 Mps
- ☐ any (auto negotiate port speed)

Command mode: Interface port

Table 132 Port Link Configuration Commands

Command Syntax and Usage

duplex {full|half|any}

Sets the operating mode. The choices include:

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

Command mode: Interface port

[no] flowcontrol {receive|send|both}

Sets the flow control. The choices include:

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

Command mode: Interface port

[no] auto

Turns auto-negotiation on or off.

[no] fastld

Enables or disables Fast Link Down detection, which allows the switch to quickly detect link-down events on 1G copper ports (1000BASE-T).

Note: This command applies only to 1G copper ports.

Command mode: Interface port

show interface port <port alias or number>

Displays current port parameters.

Command mode: All

Temporarily Disabling a Port

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

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

Because this configuration sets a temporary state for the port, you do not need to use a save operation. The port state will revert to its original configuration when the 1/10Gb Uplink ESM is reset. See the [“Operations Commands” on page 409](#) for other operations-level commands.

UniDirectional Link Detection Configuration

UDLD commands are described in the following table.

Table 133 Port UDLD Configuration commands

Command Syntax and Usage

[no] udld

Enables or disables UDLD on the port.

Command mode: Interface port

[no] udld aggressive

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

- ❑ **Normal:** Detect unidirectional links that have mis-connected interfaces. The port is disabled if UDLD determines that the port is mis-connected. Use the “no” form to select normal operation.
- ❑ **Aggressive:** In addition to the normal mode, the aggressive mode disables the port if the neighbor stops sending UDLD probes for 7 seconds.

Command mode: Interface port

show udld

Displays current port UDLD parameters.

Command mode: All

Port OAM Configuration

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

OAM Discovery commands are described in the following table.

Table 134 Port OAM Configuration commands

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

Port ACL Configuration

Table 135 ACL/QoS Configuration Commands

Command Syntax and Usage
access-control list <1-640> Adds the specified ACL list to the port. You can add multiple ACL lists to a port. Command mode: Interface port
no access-control list <1-640> Deletes the specified ACL list from the port. Command mode: Interface port

Table 135 ACL/QoS Configuration Commands

Command Syntax and Usage

access-control group *<1-640>*

Adds the specified ACL Group to the port. You can add multiple ACL Groups to a port.

Command mode: Interface port

no access-control group *<1-640>*

Removes the specified ACL from the port.

Command mode: Interface port

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

Displays current ACL QoS parameters.

Command mode: All

Port Spanning Tree Configuration

Table 136 Port STP Options

Command Syntax and Usage

[no] spanning-tree edge

Enables or disables this port as an edge port. An edge port is not connected to a bridge, and can begin forwarding traffic as soon as the link is up. Configure server ports as edge ports (enabled).

Note: After you configure the port as an edge port, you must disable the port and then re-enable the port for the change to take effect.

Command mode: Interface port

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

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

- ☐ **no**: Configures the port to detect the link type, and automatically match its settings.
- ☐ **p2p**: Configures the port for Point-To-Point protocol.
- ☐ **shared**: Configures the port to connect to a shared medium (usually a hub).

The default link type is `auto`.

Command mode: Interface port

show interface port {<port alias or number>}

Displays current port configuration parameters.

Command mode: All

Stacking Configuration

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

The Stacking Configuration menu is available only after Stacking is enabled and the switch is reset. For more information, see “[Stacking Boot Menu](#)” on page 454.

Table 137 Stacking Options

Command Syntax and Usage

[no] stack name *<1-32 characters>*

Defines a name for the stack.

Command mode: Global configuration

[no] stack backup *<csnum (1-6)>*

Defines the backup switch in the stack, based on its configured switch number (csnum).

Command mode: Global configuration

show stack switch-number *<csnum (1-6)>*

Displays the current stacking parameters.

Command mode: All

Stacking Switch Configuration

Table 138 Stacking Switch Options

Command Syntax and Usage

stack switch-number <csnum (1-6)> **universal-unic-id** <UUID>

Binds the selected switch to the stack, based on the UUID of the chassis in which the switch resides. You also must enter the bay number to specify a switch within the chassis. Following is an example UUID:

uuid 49407441b1a511d7b95df58f4b6f99fe

Command mode: Global configuration

stack switch-number <csnum (1-6)> **bay** <1-10>

Binds the selected switch to the stack, based on its bay number in the chassis. You also must enter the UUID to specify the chassis in which the switch resides.

Command mode: Global configuration

stack switch-number <csnum (1-6)> **bind** <asnum (1-6)>

Binds the selected switch to the stack, based on its assigned switch number (asnum).

Command mode: Global configuration

stack switch-number <csnum (1-6)> **mac** <MAC address>

Binds the selected switch to the stack, based on its MAC address.

Command mode: Global configuration

no stack switch-number <csnum (1-6)>

Deletes the selected switch from the stack.

Command mode: Global configuration

show stack attached-switches

Displays the current stacking switch parameters.

Command mode: Global configuration

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 GbESM 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 139 802.1p Configuration Commands

Command Syntax and Usage

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

Maps the 802.1p priority of to the Class of Service queue (COSq) priority. Enter the 802.1p priority value (0-7), followed by the Class of Service queue that handles the matching traffic.

Command mode: Global configuration

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

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

Command mode: Global configuration

Table 139 802.1p Configuration Commands

Command Syntax and Usage

qos transmit-queue number-cos {2|8}

Sets the number of Class of Service queues (COSq) for switch ports. Depending on the numcos setting, the valid COSq range for the priq and qweight commands is as follows:

- If numcos is 2 (the default), the COSq range is 0-1.
- If numcos is 8, the COSq range is 0-7.

You must apply, save, and reset the switch to activate the new configuration.

Note: In Stacking mode, the number of COS queues available is 1 or 7, because one COS queue is reserved for Stacking.

Command mode: Global configuration

show qos transmit-queue

Displays the current 802.1p parameters.

Command mode: All except User EXEC

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 140 DSCP Configuration Commands

Command Syntax and Usage

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

Maps the initial DiffServ Code Point (DSCP) value to a new value. Enter the DSCP value (0-63) of incoming packets, followed by the new value.

Command mode: Global configuration

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

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

Command mode: Global configuration

qos dscp re-marking

Turns on DSCP re-marking globally.

Command mode: Global configuration

Table 140 DSCP Configuration Commands

Command Syntax and Usage

no qos dscp re-marking

Turns off DSCP re-marking globally.

Command mode: Global configuration

show qos dscp

Displays the current DSCP parameters.

Command mode: All except User EXEC

Access Control Configuration

Use these commands to create Access Control Lists and ACL Groups. ACLs define matching criteria used for IP filtering and Quality of Service functions.

For information about assigning ACLs to ports, see [“Port ACL Configuration” on page 248](#).

Table 141 General ACL Configuration Commands

Command Syntax and Usage

[no] access-control list <1-640>

Configures an Access Control List.

Command mode: Global configuration

To view command options, see [page 256](#).

[no] access-control group <1-640>

Configures an ACL Group.

Command mode: Global configuration

To view command options, see [page 264](#).

show access-control

Displays the current ACL parameters.

Command mode: All except User EXEC

Access Control List Configuration

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

Table 142 ACL Configuration Commands

Command Syntax and Usage	
[no] access-control list <1-640> egress-port port <port alias or number>	
Configures the ACL to function on egress packets.	
Command mode: Global configuration	
access-control list <1-640> action {permit deny set-priority <0-7>}	
Configures a filter action for packets that match the ACL definitions. You can choose to permit (pass) or deny (drop) packets, or set the 802.1p priority level (0-7).	
Command mode: Global configuration	
access-control list <1-640> statistics	
Enables or disables the statistics collection for the Access Control List.	
Command mode: All except User EXEC	
default access-control list <1-640>	
Resets the ACL parameters to their default values.	
Command mode: Global configuration	
show access-control list <1-640>	
Displays the current ACL parameters.	
Command mode: All except User EXEC	

Ethernet Filtering Configuration

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

Table 143 Ethernet Filtering Configuration Commands

Command Syntax and Usage

**[no] access-control list <1-640> ethernet
source-mac-address <MAC address> <MAC mask>**

Defines the source MAC address for this ACL.

Command mode: Global configuration

**[no] access-control list <1-640> ethernet
destination-mac-address <MAC address> <MAC mask>**

Defines the destination MAC address for this ACL.

Command mode: Global configuration

**[no] access-control list <1-640> ethernet
vlan <VLAN ID> <VLAN mask>**

Defines a VLAN number and mask for this ACL.

Command mode: Global configuration

**[no] access-control list <1-640> ethernet ethernet-type
{arp|ip|ipv6|mpls|rarp|any|<other (0x600-0xFFFF)>}**

Defines the Ethernet type for this ACL.

Command mode: Global configuration

[no] access-control list <1-640> ethernet priority <0-7>

Defines the Ethernet priority value for the ACL.

Command mode: Global configuration

default access-control list <1-640> ethernet

Resets Ethernet parameters for the ACL to their default values.

Command mode: Global configuration

Table 143 Ethernet Filtering Configuration Commands

Command Syntax and Usage

no access-control list <1-640> **ethernet**

Removes Ethernet parameters for the ACL.

Command mode: Global configuration

show access-control list <1-640> **ethernet**

Displays the current Ethernet parameters for the ACL.

Command mode: All except User EXEC

IPv4 Filtering Configuration

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

Table 144 IP version 4 Filtering Configuration Commands

Command Syntax and Usage

[no] access-control list <1-640> **ipv4 source-ip-address** <IP address>
<IP mask>

Defines a source IP address for the ACL. If defined, traffic with this source IP address will match this ACL. Specify an IP address in dotted decimal notation.

Command mode: Global configuration

[no] access-control list <1-640> **ipv4 destination-ip-address**
<IP address> <IP mask>

Defines a destination IP address for the ACL. If defined, traffic with this destination IP address will match this ACL.

Command mode: Global configuration

Table 144 IP version 4 Filtering Configuration Commands

Command Syntax and Usage	
[no] access-control list <1-640> ipv4 protocol <0-255>	
Defines an IP protocol for the ACL. If defined, traffic from the specified protocol matches this filter. Specify the protocol number. Listed below are some of the well-known protocols.	
Number	Name
1	icmp
2	igmp
6	tcp
17	udp
89	ospf
112	vrrp
Command mode: Global configuration	
[no] access-control list <1-640> ipv4 type-of-service <0-255>	
Defines a Type of Service (ToS) value for the ACL. For more information on ToS, refer to RFC 1340 and 1349.	
Command mode: Global configuration	
default access-control list <1-640> ipv4	
Resets the IPv4 parameters for the ACL to their default values.	
Command mode: Global configuration	
show access-control list <1-640> ipv4	
Displays the current IPV4 parameters.	
Command mode: All except User EXEC	

TCP/UDP Filtering Configuration

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

Table 145 TCP/UDP Filtering Configuration Commands

Command Syntax and Usage	
[no] access-control list <1-640> tcp-udp source-port <1-65535> <mask (0xFFFF)>	
Defines a source port for the ACL. If defined, traffic with the specified TCP or UDP source port will match this ACL. Specify the port number. Listed below are some of the well-known ports:	
Number	Name
20	ftp-data
21	ftp
22	ssh
23	telnet
25	smtp
37	time
42	name
43	whois
53	domain
69	tftp
70	gopher
79	finger
80	http
Command mode: Global configuration	
[no] access-control list <1-640> tcp-udp destination-port <1-65535> <mask (0xFFFF)>	
Defines a destination port for the ACL. If defined, traffic with the specified TCP or UDP destination port will match this ACL. Specify the port number, just as with <code>source-port</code> above.	
Command mode: Global configuration	
[no] access-control list <1-640> tcp-udp flags <value (0x0-0x3f)> <mask (0x0-0x3f)>	
Defines a TCP/UDP flag for the ACL.	
Command mode: Global configuration	

Table 145 TCP/UDP Filtering Configuration Commands**Command Syntax and Usage**

```
default access-control list <1-640> tcp-udp
```

Resets the TCP/UDP parameters for the ACL to their default values.

Command mode: Global configuration

```
show access-control list <1-640> tcp-udp
```

Displays the current TCP/UDP Filtering parameters.

Command mode: All except User EXEC

Packet Format Filtering Configuration

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

Table 146 Packet Format Filtering Configuration Commands**Command Syntax and Usage**

```
[no] access-control list <1-640> packet-format  
  ethernet {ethertype2 | snap | llc}
```

Defines the Ethernet format for the ACL.

Command mode: Global configuration

```
[no] access-control list <1-640> packet-format tagging  
  {any | none | tagged}
```

Defines the tagging format for the ACL.

Command mode: Global configuration

```
[no] access-control list <1-640> packet-format ip {ipv4 | ipv6}
```

Defines the IP format for the ACL.

Command mode: Global configuration

Table 146 Packet Format Filtering Configuration Commands

Command Syntax and Usage

default access-control list <1-640> packet-format

Resets Packet Format parameters for the ACL to their default values.

Command mode: Global configuration

show access-control list <1-640> packet-format

Displays the current Packet Format parameters for the ACL.

Command mode: All except User EXEC

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 256](#).

For more information about assigning VLAN Maps to a VLAN, see [“VLAN Configuration” on page 312](#).

For more information about assigning VLAN Maps to a VM group, see [“VM Group Configuration” on page 402](#).

Table 147 lists the general VMAP configuration commands.

Table 147 VMAP Configuration Commands

Command Syntax and Usage	
[no] access-control vmap <1-128> egress-port <port alias or number>	
Configures the VMAP to function on egress packets.	
Command mode: Global configuration	
access-control vmap <1-128> action { permit deny set-priority <0-7>}	
Configures a filter action for packets that match the VMAP definitions. You can choose to permit (pass) or deny (drop) packets, or set the 802.1p priority level (0-7).	
Command mode: Global configuration	
access-control vmap <1-128> statistics	
Enables or disables the statistics collection for the VMAP.	
Command mode: All except User EXEC	
default access-control vmap <1-128>	
Resets the VMAP parameters to their default values.	
Command mode: Global configuration	
show access-control vmap <1-128>	
Displays the current VMAP parameters.	
Command mode: All except User EXEC	

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 148 ACL Group Configuration Commands

Command Syntax and Usage
access-control group <1-640> list <1-640> Adds the selected ACL to the ACL Group. Command mode: Global configuration
no access-control group <1-640> list <1-640> Removes the selected ACL from the ACL Group. Command mode: Global configuration
show access-control group <1-640> Displays the current ACL group parameters. Command mode: All except User EXEC

ACL Metering Configuration

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

Table 149 ACL Metering Configuration Commands

Command Syntax and Usage
access-control list <1-640> meter committed-rate <64-10000000> Configures the committed rate, in Kilobits per second. The committed rate must be a multiple of 64. Command mode: Global configuration
access-control list <1-640> meter maximum-burst-size <32-4096> Configures the maximum burst size, in Kilobits. Enter one of the following values for mbsize: 32, 64, 128, 256, 512, 1024, 2048, 4096 Command mode: Global configuration

Table 149 ACL Metering Configuration Commands**Command Syntax and Usage**

[no] access-control list <1-640> meter enable

Enables or disables ACL Metering.

Command mode: Global configuration

access-control list <1-640> meter action {drop|pass}

Configures the ACL Meter to either drop or pass out-of-profile traffic.

Command mode: Global configuration

default access-control list <1-640> meter

Sets the ACL meter configuration to its default values.

Command mode: Global configuration

no access-control list <1-640> meter

Deletes the selected ACL meter.

Command mode: Global configuration

show access-control list <1-640> meter

Displays current ACL Metering parameters.

Command mode: All

ACL Re-Mark Configuration

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

Table 150 Re-marking Configuration Commands

Command Syntax and Usage

access-control list <1-640> re-mark dot1p <0-7>

Defines 802.1p value. The value is the priority bits information in the packet structure.

Command mode: Global configuration

no access-control list <1-640> re-mark dot1p

Disables use of 802.1p value for re-marked packets.

Command mode: Global configuration

[no] access-control list <1-640> re-mark use-tos-precedence

Enable or disable mapping of TOS (Type of Service) priority to 802.1p priority for In-Profile packets. When enabled, the TOS value is used to set the 802.1p value.

Command mode: Global configuration

default access-control list <1-640> re-mark

Sets the ACL Re-mark configuration to its default values.

Command mode: Global configuration

show access-control list <1-640> re-mark

Displays current Re-mark parameters.

Command mode: All

Re-marking In-Profile Configuration

Table 151 ACL Re-marking In-Profile commands

Command Syntax and Usage

access-control list <1-640> re-mark in-profile dscp <0-63>

Sets the DiffServ Code Point (DSCP) of in-profile packets to the selected value.

Command mode: Global configuration

no access-control list <1-640> re-mark in-profile dscp

Disables use of DSCP value for in-profile traffic.

Command mode: Global configuration

show access-control list <1-640> re-mark

Displays current Re-mark parameters.

Command mode: All

Re-Marking Out-of-Profile Configuration

Table 152 ACL Re-marking Out-of-Profile commands

Command Syntax and Usage

access-control list <1-640> re-mark out-profile dscp <0-63>

Sets the DiffServ Code Point (DSCP) of out-of-profile packets to the selected value. The switch sets the DSCP value on Out-of-Profile packets.

Command mode: Global configuration

no access-control list <1-640> re-mark out-profile dscp

Disables use of DSCP value for out-of-profile traffic.

Command mode: Global configuration

show access-control list <1-640> re-mark

Displays current Re-mark parameters.

Command mode: All

Port Mirroring

Port mirroring is disabled by default. For more information about port mirroring on the GbESM, see “Appendix A: Troubleshooting” in the *BLADEOS 6.3 Application Guide*.

Note – Traffic on VLAN 4095 is not mirrored to the external ports.

Port Mirroring commands are used to configure, enable, and disable the monitor port. When enabled, network packets being sent and/or received on a target port are duplicated and sent to a monitor port. By attaching a network analyzer to the monitor port, you can collect detailed information about your network performance and usage.

Table 153 Port Mirroring Configuration Commands

Command Syntax and Usage

[no] port-mirroring enable

Enables or disables port mirroring.

Command mode: Global configuration

show port-mirroring

Displays current settings of the mirrored and monitoring ports.

Command mode: All except User EXEC

Port-Mirroring Configuration

Table 154 Port-Based Port-Mirroring Configuration Commands

Command Syntax and Usage

port-mirroring monitor-port *<port alias or number>* **mirroring-port**
<port alias or number> {**in**|**out**|**both**}

Adds the port to be mirrored. This command also allows you to enter the direction of the traffic. It is necessary to specify the direction because:

If the source port of the frame matches the mirrored port and the mirrored direction is ingress or both (ingress and egress), the frame is sent to the monitoring port.

If the destination port of the frame matches the mirrored port and the mirrored direction is egress or both, the frame is sent to the monitoring port.

Command mode: Global configuration

no port-mirroring monitor-port *<port alias or number>* **mirroring-port**
<port alias or number>

Removes the mirrored port.

Command mode: Global configuration

show port-mirroring

Displays the current settings of the monitoring port.

Command mode: All except User EXEC

Layer 2 Configuration

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

Table 155 Layer 2 Configuration Commands

Command Syntax and Usage

vlan *<VLAN number>*

Enter VLAN configuration mode.

Command mode: Global configuration

To view command options, see [page 312](#).

[no] spanning-tree pvst-compatibility

Enables or disables VLAN tagging of Spanning Tree BPDUs. The default setting is enabled.

Command mode: Global configuration

[no] spanning-tree uplinkfast

Enables or disables Fast Uplink Convergence, which provides rapid Spanning Tree convergence to an upstream switch during failover.

Note: When enabled, this feature increases bridge priorities to 65535 for all STGs (except the management STG) and path cost by 3000 for all external STP ports.

Command mode: Global configuration

spanning-tree uplinkfast max-update-rate *<10-200>*

Configures the station update rate. The default value is 40.

Command mode: Global configuration

[no] mac-address-table mac-notification

Enables or disables MAC Address Notification. With MAC Address Notification enabled, the switch generates a syslog message when a MAC address is added or removed from the MAC address table.

Command mode: Global configuration

show layer2

Displays current Layer 2 parameters.

Command mode: All

802.1X Configuration

These commands allow you to configure the GbESM as an IEEE 802.1X Authenticator, to provide port-based network access control.

Table 156 802.1x Configuration Commands

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

802.1X Global Configuration

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

Table 157 802.1X Global Configuration Commands

Command Syntax and Usage

dot1x mode [**force-unauthorized** | **auto** | **force-authorized**]

Sets the type of access control for all ports:

- ❑ **force-unauthorized** - the port is unauthorized unconditionally.
- ❑ **auto** - the port is unauthorized until it is successfully authorized by the RADIUS server.
- ❑ **force-authorized** - the port is authorized unconditionally, allowing all traffic.

The default value is `force-authorized`.

Command mode: Global configuration

dot1x quiet-time <0-65535>

Sets the time, in seconds, the authenticator waits before transmitting an EAP-Request/Identity frame to the supplicant (client) after an authentication failure in the previous round of authentication. The default value is 60 seconds.

Command mode: Global configuration

dot1x transmit-interval <1-65535>

Sets the time, in seconds, the authenticator waits for an EAP-Response/Identity frame from the supplicant (client) before retransmitting an EAP-Request/Identity frame. The default value is 30 seconds.

Command mode: Global configuration

dot1x supplicant-timeout <1-65535>

Sets the time, in seconds, the authenticator waits for an EAP-Response packet from the supplicant (client) before retransmitting the EAP-Request packet from the authentication server. The default value is 30 seconds.

Command mode: Global configuration

Table 157 802.1X Global Configuration Commands

Command Syntax and Usage

dot1x server-timeout *<1-65535>*

Sets the time, in seconds, the authenticator waits for a response from the RADIUS server before declaring an authentication timeout. The default value is 30 seconds.

The time interval between transmissions of the RADIUS Access-Request packet containing the supplicant's (client's) EAP-Response packet is determined by the current setting of radius-server timeout *<timeout-value>* (default is 3 seconds).

Command mode: Global configuration

dot1x max-request *<1-10>*

Sets the maximum number of times the authenticator retransmits an EAP-Request packet to the supplicant (client). The default value is 2.

Command mode: Global configuration

dot1x re-authentication-interval *<1-604800>*

Sets the time, in seconds, the authenticator waits before re-authenticating a supplicant (client) when periodic re-authentication is enabled. The default value is 3600 seconds.

Command mode: Global configuration

dot1x re-authenticate

Sets the re-authentication status to *on*. The default value is *off*.

Command mode: Global configuration

[no] dot1x re-authenticate

Sets the re-authentication status to *off*. The default value is *off*.

Command mode: Global configuration

[no] dot1x vlan-assign

Sets the dynamic VLAN assignment status to *on* or *off*. The default value is *off*.

Command mode: Global configuration

Table 157 802.1X Global Configuration Commands

Command Syntax and Usage

default dot1x

Resets the global 802.1X parameters to their default values.

Command mode: Global configuration

show dot1x

Displays current global 802.1X parameters.

Command mode: All

802.1X Guest VLAN Configuration

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

Table 158 802.1X Guest VLAN Configuration Commands

Command Syntax and Usage

[no] dot1x guest-vlan vlan *<VLAN number>*

Configures the Guest VLAN number.

Command mode: Global configuration

dot1x guest-vlan enable

Enables the 802.1X Guest VLAN.

Command mode: Global configuration

no dot1x guest-vlan enable

Disables the 802.1X Guest VLAN.

Command mode: Global configuration

show dot1x

Displays current 802.1X parameters.

Command mode: All

802.1X Port Configuration

The 802.1X port commands allows you to configure parameters that affect the selected port in the GbESM. These settings override the global 802.1X parameters.

Table 159 802.1X Port Commands

Command Syntax and Usage

dot1x mode force-unauthorized | auto | force-authorized

Sets the type of access control for the port:

- ❑ **force-unauthorized** - the port is unauthorized unconditionally.
- ❑ **auto** - the port is unauthorized until it is successfully authorized by the RADIUS server.
- ❑ **force-authorized** - the port is authorized unconditionally, allowing all traffic.

The default value is `force-authorized`.

Command mode: Interface port

dot1x quiet-time <0-65535>

Sets the time, in seconds, the authenticator waits before transmitting an EAP-Request/Identity frame to the supplicant (client) after an authentication failure in the previous round of authentication. The default value is 60 seconds.

Command mode: Interface port

dot1x transmit-interval <1-65535>

Sets the time, in seconds, the authenticator waits for an EAP-Response/Identity frame from the supplicant (client) before retransmitting an EAP-Request/Identity frame. The default value is 30 seconds.

Command mode: Interface port

dot1x supplicant-timeout <1-65535>

Sets the time, in seconds, the authenticator waits for an EAP-Response packet from the supplicant (client) before retransmitting the EAP-Request packet from the authentication server. The default value is 30 seconds.

Command mode: Interface port

Table 159 802.1X Port Commands**Command Syntax and Usage****dot1x server-timeout** *<1-65535>*

Sets the time, in seconds, the authenticator waits for a response from the RADIUS server before declaring an authentication timeout. The default value is 30 seconds.

The time interval between transmissions of the RADIUS Access-Request packet containing the supplicant's (client's) EAP-Response packet is determined by the current setting of the `radius-server timeout` command.

Command mode: Interface port

dot1x max-request *<1-10>*

Sets the maximum number of times the authenticator retransmits an EAP-Request packet to the supplicant (client). The default value is 2.

Command mode: Interface port

dot1x re-authentication-interval *<1-604800>*

Sets the time, in seconds, the authenticator waits before re-authenticating a supplicant (client) when periodic re-authentication is enabled. The default value is 3600 seconds.

Command mode: Interface port

dot1x re-authenticate

Sets the re-authentication status to `on`. The default value is `off`.

Command mode: Interface port

[no] dot1x re-authenticate

Sets the re-authentication status `off`. The default value is `off`.

Command mode: Interface port

[no] dot1x vlan-assign

Sets the dynamic VLAN assignment status to `on` or `off`. The default value is `off`.

Command mode: Interface port

default dot1x

Resets the 802.1X port parameters to their default values.

Command mode: Interface port

Table 159 802.1X Port Commands

Command Syntax and Usage

dot1x apply-global

Applies current global 802.1X configuration parameters to the port.

Command mode: Interface port

show interface port <port alias or number> dot1x

Displays current 802.1X port parameters.

Command mode: All

Active MultiPath Protocol Configuration

Use the following commands to configure Active MultiPath Protocol (AMP) for the GbESM.

Table 160 AMP Configuration Options

Command Syntax and Usage

[no] active-multipath aggr-portchannel lacp <1-65535>

Configures an LACP *admin key* to be used as the AMP Aggregator link. LACP trunks formed with this *admin key* will be used to link the two AMP Aggregators.

Note: This command does not apply to AMP Access switches.

Command mode: Global configuration

[no] active-multipath aggr-port <port alias or number>

Configures a port to be used as the AMP Aggregator link.

Note: This command does not apply to AMP Access switches.

Command mode: Global configuration

[no] active-multipath aggr-portchannel <trunk number>

Configures a trunk to be used as the AMP Aggregator link.

Note: This command does not apply to AMP Access switches.

Command mode: Global configuration

Table 160 AMP Configuration Options**Command Syntax and Usage****[no] active-multipath interval** <10-10000>

Configures the time interval between AMP *keep alive* messages, in centiseconds. The default value is 50.

Command mode: Global configuration

[no] active-multipath switch-priority <1-255>

Configures the AMP priority for the switch. The default value is 255.

A lower priority value denotes a higher precedence (so priority 1 is the highest priority.) It is recommended that aggregator switches be configured with lower priority values than access switches.

Command mode: Global configuration

[no] active-multipath timeout-count <1-20>

Configures the timeout count, which is the number of unreceived keep-alive packets the switch waits before declaring a timeout due to loss of connectivity with the peer. The default value is 4.

Command mode: Global configuration

[no] active-multipath switch-type access|aggregator

Defines the AMP switch type, as follows:

- ❑ **Access:** Connects to downstream servers. Only one AMP group can be configured on an access switch.
- ❑ **Aggregator:** Connects to upstream routers. Multiple AMP groups can be configured on an Aggregator switch.

The default switch type is *access*.

Note: It is recommended to configure the 1/10Gb Uplink ESM only as an access switch.

Command mode: Global configuration

active-multipath enable

Globally turns Active MultiPath on.

Command mode: Global configuration

Table 160 AMP Configuration Options**Command Syntax and Usage****no active-multipath enable**

Globally turns Active MultiPath off.

Command mode: Global configuration

default active-multipath

Resets Active MultiPath parameters to their default values, and optionally delete all AMP groups.

Command mode: Global configuration

show active-multipath

Displays the current AMP parameters.

Command mode: All

AMP Group Configuration

Use the following commands to configure an AMP group.

Table 161 AMP Group Configuration Options**Command Syntax and Usage****[no] active-multipath group** *<AMP group number>* **port** *<port alias or number>*

Adds the port as the first port in the AMP group.

Command mode: Global configuration

[no] active-multipath group *<AMP group number>* **port2** *<port alias or number>*

Adds the port as the second port in the AMP group.

Command mode: Global configuration

[no] active-multipath group *<AMP group number>* **portchannel lacp** *<1-65535>*

Adds the first LACP *admin key* to the AMP group. LACP trunks formed with this *admin key* will be used for AMP communication.

Command mode: Global configuration

Table 161 AMP Group Configuration Options**Command Syntax and Usage**

[no] active-multipath group *<AMP group number>* **portchannel2**
lacp *<1-65535>*

Adds the second LACP *admin key* to the AMP group. LACP trunks formed with this *admin key* will be used for AMP communication.

Command mode: Global configuration

[no] active-multipath group *<AMP group number>* **portchannel** *<trunk number>*

Adds the first trunk group to the AMP group.

Command mode: Global configuration

[no] active-multipath group *<AMP group number>* **portchannel2** *<trunk number>*

Adds the second trunk group to the AMP group.

Command mode: Global configuration

active-multipath group *<AMP group number>* **enable**

Enables the AMP group.

Command mode: Global configuration

no active-multipath group *<AMP group number>* **enable**

Disables the AMP group.

Command mode: Global configuration

no active-multipath group *<AMP group number>*

Deletes the AMP group.

Command mode: Global configuration

show active-multipath group *<AMP group number>*

Displays the current AMP group configuration.

Command mode: All

RSTP/MSTP/PVRST Configuration

BLADEOS supports the IEEE 802.1w Rapid Spanning Tree Protocol (RSTP) and IEEE 802.1s Multiple Spanning Tree Protocol (MSTP), and Per VLAN Rapid Spanning Tree Protocol (PVRST). MSTP allows you to map many VLANs to a small number of Spanning Tree Groups, each with its own topology.

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

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

Table 162 Multiple Spanning Tree Configuration Commands

Command Syntax and Usage

spanning-tree mstp name *<1-32 characters>*

Configures a name for the MSTP region. All devices within an MSTP region must have the same region name.

Command mode: Global configuration

spanning-tree mstp version *<0-65535>*

Configures a version number for the MSTP region. The version is used as a numerical identifier for the region. All devices within an MSTP region must have the same version number.

Command mode: Global configuration

spanning-tree mstp maximum-hop *<4-60>*

Configures the maximum number of bridge hops a packet may traverse before it is dropped. The default value is 20.

Command mode: Global configuration

Table 162 Multiple Spanning Tree Configuration Commands

Command Syntax and Usage
spanning-tree mode [mst pvrst pvst rstp] Selects and enables Multiple Spanning Tree mode (mst), Per VLAN Rapid Spanning Tree mode (pvrst), Per VLAN Spanning Tree mode (pvst), or Rapid Spanning Tree mode (rstp). The default mode is RSTP. Command mode: Global configuration
show spanning-tree mstp mrst Displays the current RSTP/MSTP/PVRST configuration. Command mode: All

Common Internal Spanning Tree Configuration

Table 163 describes the commands used to configure Common Internal Spanning Tree (CIST) parameters. The CIST provides compatibility with different MSTP regions and with devices running different Spanning Tree instances. It is equivalent to Spanning Tree Group 0.

Table 163 CIST Configuration Commands

Command Syntax and Usage
default spanning-tree mstp cist Resets all CIST parameters to their default values. Command mode: Global configuration
show spanning-tree mstp cist Displays the current CIST configuration. Command mode: All

CIST Bridge Configuration

CIST bridge parameters are used only when the switch is in MSTP mode. CIST parameters do not affect operation of STP/PVST+, RSTP, or PVRST.

Table 164 CIST Bridge Configuration Commands

Command Syntax and Usage

spanning-tree mstp cist-bridge priority <0-65535>

Configures the CIST bridge priority. The bridge priority parameter controls which bridge on the network is the MSTP root bridge. To make this switch the root bridge, configure the bridge priority lower than all other switches and bridges on your network. The lower the value, the higher the bridge priority.

The range is 0 to 65535, in steps of 4096 (0, 4096, 8192...), and the default value is 61440.

Command mode: Global configuration

spanning-tree mstp cist-bridge maximum-age <6-40>

Configures the CIST bridge maximum age. The maximum age parameter specifies the maximum time the bridge waits without receiving a configuration bridge protocol data unit before it reconfigures the MSTP network. The range is 6 to 40 seconds, and the default is 20 seconds.

Command mode: Global configuration

spanning-tree mstp cist-bridge forward-delay <4-30>

Configures the CIST bridge forward delay parameter. The forward delay parameter specifies the amount of time that a bridge port has to wait before it changes from the listening state to the learning state and from the learning state to the forwarding state. The range is 4 to 30 seconds, and the default is 15 seconds.

Command mode: Global configuration

show spanning-tree mstp cist

Displays the current CIST bridge configuration.

Command mode: All Except User EXEC

CIST Port Configuration

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

Table 165 CIST Port Configuration Commands

Command Syntax and Usage
spanning-tree mstp cist interface-priority <0-240>
<p>Configures the CIST port priority. The port priority helps determine which bridge port becomes the designated port. In a network topology that has multiple bridge ports connected to a single segment, the port with the lowest port priority becomes the designated port for the segment.</p> <p>The range is 0 to 240, in steps of 16 (0, 16, 32...), and the default is 128.</p> <p>Command mode: Interface port</p>
spanning-tree mstp cist path-cost <0-200000000>
<p>Configures the CIST port path cost. The port path cost is used to help determine the designated port for a segment. Port path cost is based on the port speed, and is calculated as follows:</p> <ul style="list-style-type: none">□ 100Mbps = 200000□ 1Gbps = 20000□ 10Gbps = 2000 <p>The default value of 0 (zero) indicates that the default path cost will be computed for an auto negotiated link speed.</p> <p>Command mode: Interface port</p>
spanning-tree mstp cist hello <1-10>
<p>Configures the CIST port Hello time. The Hello time specifies how often the root bridge transmits a configuration bridge protocol data unit (BPDU). Any bridge that is not the root bridge uses the root bridge Hello value. The range is 1 to 10 seconds, and the default is 2 seconds.</p> <p>Command mode: Interface port</p>

Table 165 CIST Port Configuration Commands

Command Syntax and Usage

spanning-tree mstp cist link-type {auto|p2p|shared}

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

auto: Configures the port to detect the link type, and automatically match its settings.

p2p: Configures the port for Point-To-Point protocol.

shared: Configures the port to connect to a shared medium (usually a hub).

The default link type is **auto**.

Command mode: Interface port

[no] spanning-tree mstp cist edge

Enables or disables this port as an edge port. An edge port is not connected to a bridge, and can begin forwarding traffic as soon as the link is up. Configure server ports as edge ports (enabled). The default value is disabled.

Note: After you configure the port as an edge port, you must disable the port (interface port *x* shutdown) and then re-enable the port (interface port *x* shutdown) for the change to take effect.

Command mode: Interface port

spanning-tree mstp cist enable

Enables MRST on the port.

Command mode: Interface port

no spanning-tree mstp cist enable

Disables MRST on the port.

Command mode: Interface port

show interface port <port alias or number> spanning-tree mstp cist

Displays the current CIST port configuration.

Command mode: All Except User EXEC

Spanning Tree Configuration

BLADEOS supports the IEEE 802.1D Spanning Tree Protocol (STP). STP is used to prevent loops in the network topology. Up to 128 Spanning Tree Groups can be configured on the switch (STG 128 is reserved for management).

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

Table 166 Spanning Tree Configuration Commands

Command Syntax and Usage

spanning-tree stp *<STG number>* **vlan** *<VLAN number>*

Associates a VLAN with a Spanning Tree and requires a VLAN ID as a parameter.

Command mode: Global configuration

no spanning-tree stp *<STG number>* **vlan** *<VLAN number>*

Breaks the association between a VLAN and a Spanning Tree and requires a VLAN ID as a parameter.

Command mode: Global configuration

no spanning-tree stp *<STG number>* **vlan all**

Removes all VLANs from a Spanning Tree.

Command mode: Global configuration

spanning-tree stp *<STG number>* **enable**

Globally enables Spanning Tree Protocol. STG is turned on by default.

Command mode: Global configuration

no spanning-tree stp *<STG number>* **enable**

Globally disables Spanning Tree Protocol.

Command mode: Global configuration

default spanning-tree *<STG number>*

Restores a Spanning Tree instance to its default configuration.

Command mode: Global configuration

show spanning-tree stp *<STG number>*

Displays current Spanning Tree Protocol parameters.

Command mode: All

Bridge Spanning Tree Configuration

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

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

Table 167 Bridge Spanning Tree Configuration Commands

Command Syntax and Usage

spanning-tree stp <STG number> **bridge priority** <0-65535>

Configures the bridge priority. The bridge priority parameter controls which bridge on the network is the STG root bridge. To make this switch the root bridge, configure the bridge priority lower than all other switches and bridges on your network. The lower the value, the higher the bridge priority. The default value is 65534.

RSTP/MSTP: The range is 0 to 61440, in steps of 4096 (0, 4096, 8192...), and the default is 61440.

Command mode: Global configuration

spanning-tree stp <STG number> **bridge hello-time** <1-10>

Configures the bridge Hello time. The Hello time specifies how often the root bridge transmits a configuration bridge protocol data unit (BPDU). Any bridge that is not the root bridge uses the root bridge Hello value. The range is 1 to 10 seconds, and the default is 2 seconds.

This command does not apply to MSTP.

Command mode: Global configuration

spanning-tree stp <STG number> **bridge maximum-age** <6-40>

Configures the bridge maximum age. The maximum age parameter specifies the maximum time the bridge waits without receiving a configuration bridge protocol data unit before it reconfigures the STG network. The range is 6 to 40 seconds, and the default is 20 seconds.

This command does not apply to MSTP.

Command mode: Global configuration

Table 167 Bridge Spanning Tree Configuration Commands

Command Syntax and Usage

spanning-tree stp <STG number> **bridge forward-delay** <4-30>

Configures the bridge forward delay parameter. The forward delay parameter specifies the amount of time that a bridge port has to wait before it changes from the listening state to the learning state and from the learning state to the forwarding state. The range is 4 to 30 seconds, and the default is 15 seconds.

This command does not apply to MSTP

Command mode: Global configuration

show spanning-tree stp <STG number> **bridge**

Displays the current bridge STG parameters.

Command mode: All

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

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

Spanning Tree Port Configuration

By default for STP/PVST+, Spanning Tree is turned off for internal ports and management ports, and turned on for external ports. By default for RSTP/MSTP, Spanning Tree is turned off for internal ports and management ports, and turned on for external ports, with internal ports configured as Edge ports. STG port parameters include:

- Port priority
- Port path cost

For more information about port Spanning Tree commands, see [“Port Spanning Tree Configuration” on page 250](#).

Table 168 Spanning Tree Port Commands

Command Syntax and Usage

spanning-tree stp *<STG number>* **priority** *<0-255>*

Configures the port priority. The port priority helps determine which bridge port becomes the designated port. In a network topology that has multiple bridge ports connected to a single segment, the port with the lowest port priority becomes the designated port for the segment. The default value is 128.

RSTP/MSTP: The range is 0 to 240, in steps of 16 (0, 16, 32...).

Note: In Stacking mode, the range is 0-255, in steps of 4 (0, 4, 8, 12...).

Command mode: Interface port

spanning-tree stp *<STG number>* **path-cost** *<1-65535, 0 for default>*

Configures the port path cost. The port path cost is used to help determine the designated port for a segment. Port path cost is based on the port speed, and is calculated as follows:

- 100Mbps = 19
- 1Gbps = 4
- 10Gbps = 2

The default value of 0 (zero) indicates that the default path cost will be computed for an auto negotiated link speed.

Command mode: Interface port

spanning-tree stp link-type {**auto**|**p2p**|**shared**}

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

- **auto**: Configures the port to detect the link type, and automatically match its settings.
- **p2p**: Configures the port for Point-To-Point protocol.
- **shared**: Configures the port to connect to a shared medium (usually a hub).

Command mode: Interface port

[no] spanning-tree stp edge

Enables or disables this port as an edge port. An edge port is not connected to a bridge, and can begin forwarding traffic as soon as the link is up. Configure server ports as edge ports (enabled).

Command mode: Interface port

Table 168 Spanning Tree Port Commands

Command Syntax and Usage

spanning-tree stp *<STG number>* **enable**

Enables STG on the port.

Command mode: Interface port

no spanning-tree stp *<STG number>* **enable**

Disables STG on the port.

Command mode: Interface port

show interface port *<port alias or number>* **spanning-tree stp** *<STG number>*

Displays the current STG port parameters.

Command mode: All

Forwarding Database Configuration

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

Table 169 FDB configuration commands

Command Syntax and Usage

mac-address-table aging *<0-65535>*

Configures the aging value for FDB entries, in seconds. The default value is 300.

Command mode: Global configuration

show mac-address-table

Display current FDB configuration.

Command mode: All except User EXEC

Static FDB Configuration

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

Table 170 FDB configuration commands

Command Syntax and Usage

mac-address-table static *<MAC address>* *<VLAN number>* *<port number>*

Adds a permanent FDB entry. Enter the MAC address using the following format,
xx:xx:xx:xx:xx:xx

For example, 08:00:20:12:34:56

You can also enter the MAC address as follows:

xxxxxxxxxxxx

For example, 080020123456

Command mode: Global configuration

no mac-address-table static *<MAC address>* *<VLAN number>*

Deletes a permanent FDB entry.

Command mode: Global configuration

clear mac-address-table static all

Clears all static FDB entries.

Command mode: Global configuration

show mac-address-table

Display current FDB configuration.

Command mode: All except User EXEC

Static Multicast MAC Configuration

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

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

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

Table 171 Static Multicast MAC configuration commands

Command Syntax and Usage

mac-address-table multicast *<MAC address>* *<VLAN number>*
<port alias or number>

Adds a static multicast entry. You can list ports separated by a space, or enter a range of ports separated by a hyphen (-). For example:

mac-address-table multicast 01:00:00:23:3f:01 200 int1-int4

Command mode: Global configuration

no mac-address-table multicast *<MAC address>* *<VLAN number>*
<port alias or number>

Deletes a static multicast entry.

Command mode: Global configuration

Table 171 Static Multicast MAC configuration commands

Command Syntax and Usage

```
clear mac-address-table multicast {all|mac <MAC address> |  
    vlan <VLAN number> |port <port alias or number> }
```

Clears static multicast entries.

Command mode: Global configuration

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

Display the current static multicast entries.

Command mode: All except User EXEC

LLDP Configuration

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

Table 172 LLDP commands

Command Syntax and Usage

```
lldp refresh-interval <5-32768>
```

Configures the message transmission interval, in seconds. The default value is 30.

Command mode: Global configuration

```
lldp holdtime-multiplier <2-10>
```

Configures the message hold time multiplier. The hold time is configured as a multiple of the message transmission interval.

The default value is 4.

Command mode: Global configuration

```
lldp trap-notification-interval <1-3600>
```

Configures the trap notification interval, in seconds. The default value is 5.

Command mode: Global configuration

```
lldp transmission-delay <1-8192>
```

Configures the transmission delay interval. The transmit delay timer represents the minimum time permitted between successive LLDP transmissions on a port.

The default value is 2.

Command mode: Global configuration

Table 172 LLDP commands

Command Syntax and Usage
lldp reinit-delay <1-10> Configures the re-initialization delay interval, in seconds. The re-initialization delay allows the port LLDP information to stabilize before transmitting LLDP messages. The default value is 2. Command mode: Global configuration
lldp enable Globally turns LLDP on. The default setting is on . Command mode: Global configuration
no lldp enable Globally turns LLDP off. Command mode: Global configuration
show lldp Display current LLDP configuration. Command mode: All

LLDP Port Configuration

Use the following commands to configure LLDP port options.

Table 173 LLDP Port commands

Command Syntax and Usage

lldp admin-status {disabled|tx_only|rx_only|tx_rx}

Configures the LLDP transmission type for the port, as follows:

- ☐ Transmit only
- ☐ Receive only
- ☐ Transmit and receive
- ☐ Disabled

The default setting is `tx_rx`.

Command mode: Interface port

[no] lldp trap-notification

Enables or disables SNMP trap notification for LLDP messages.

Command mode: Interface port

show interface port <port alias or number> lldp

Display current LLDP port configuration.

Command mode: All

LLDP Optional TLV configuration

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

Table 174 Optional TLV commands

Command Syntax and Usage

[no] lldp tlv portdesc

Enables or disables the Port Description information type.

Command mode: Interface port

[no] lldp tlv sysname

Enables or disables the System Name information type.

Command mode: Interface port

Table 174 Optional TLV commands**Command Syntax and Usage****[no] lldp tlv sysdescr**

Enables or disables the System Description information type.

Command mode: Interface port**[no] lldp tlv syscap**

Enables or disables the System Capabilities information type.

Command mode: Interface port**[no] lldp tlv mgmtaddr**

Enables or disables the Management Address information type.

Command mode: Interface port**[no] lldp tlv portvid**

Enables or disables the Port VLAN ID information type.

Command mode: Interface port**[no] lldp tlv portprot**

Enables or disables the Port and VLAN Protocol ID information type.

Command mode: Interface port**[no] lldp tlv vlanname**

Enables or disables the VLAN Name information type.

Command mode: Interface port**[no] lldp tlv protid**

Enables or disables the Protocol ID information type.

Command mode: Interface port**[no] lldp tlv macphy**

Enables or disables the MAC/Phy Configuration information type.

Command mode: Interface port**[no] lldp tlv powermdi**

Enables or disables the Power via MDI information type.

Command mode: Interface port

Table 174 Optional TLV commands**Command Syntax and Usage****[no] lldp tlv linkaggr**

Enables or disables the Link Aggregation information type.

Command mode: Interface port**[no] lldp tlv framesz**

Enables or disables the Maximum Frame Size information type.

Command mode: Interface port**[no] lldp tlv all**

Enables or disables all optional TLV information types.

Command mode: Interface port**show interface port** *<port alias or number>* **lldp**

Display current LLDP port configuration.

Command mode: All**Trunk Configuration**

Trunk groups can provide super-bandwidth connections between 1/10Gb Uplink ESMs 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 16 trunk groups can be configured on the GbESM, with the following restrictions:

- Any physical switch port can belong to no more than one trunk group.
- Up to 8 ports can belong to the same trunk group.
- Configure all ports in a trunk group with the same properties (speed, duplex, flow control, STG, VLAN, and so on).
- Trunking from non-BLADE devices must comply with Cisco® EtherChannel® technology.

By default, each trunk group is empty and disabled.

Table 175 Trunk Configuration Commands

Command Syntax and Usage	
portchannel <1-16> port <port alias or number>	
Adds a physical port to the current trunk group. You can add several ports, with each port separated by a comma (,).	
Command mode: Global configuration	
no portchannel <1-16> port <port alias or number>	
Removes a physical port from the current trunk group.	
Command mode: Global configuration	
[no] portchannel <1-16> enable	
Enables or Disables the current trunk group.	
Command mode: Global configuration	
no portchannel <1-16>	
Removes the current trunk group configuration.	
Command mode: Global configuration	
show portchannel <1-16>	
Displays current trunk group parameters.	
Command mode: All	

IP Trunk Hash Configuration

Use the following commands to configure IP trunk hash settings for the GbESM. Trunk hash parameters are set globally for the GbESM. 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 176](#) combined with the hash parameters listed in [Table 177](#).

Table 176 Trunk Hash Settings

Command Syntax and Usage

[no] portchannel hash ingress

Enables or disables use of the ingress port to compute the trunk hash value. The default setting is disabled.

Command mode: Global configuration

[no] portchannel hash L4port

Enables or disables use of Layer 4 service ports (TCP, UDP, etc.) to compute the hash value. The default setting is disabled.

Command mode: Global configuration

show portchannel hash

Display current trunk hash configuration.

Command mode: All

IP Trunk Hash Parameters

You can enable one or two of the following parameters, to configure any of the following valid combinations:

- SMAC (source MAC only)
- DMAC (destination MAC only)
- SIP (source IP only)
- DIP (destination IP only)
- SIP + DIP (source IP and destination IP)
- SMAC + DMAC (source MAC and destination MAC)

Use the following commands to configure trunk hash parameters for the GbESM.

Table 177 Trunk Hash Parameters

Command Syntax and Usage	
portchannel hash source-mac-address	
Enable trunk hashing on the source MAC.	
Command mode: Global configuration	
portchannel hash destination-mac-address	
Enable trunk hashing on the destination MAC.	
Command mode: Global configuration	
portchannel hash source-ip-address	
Enable trunk hashing on the source IP.	
Command mode: Global configuration	
portchannel hash destination-ip-address	
Enable trunk hashing on the destination IP.	
Command mode: Global configuration	
portchannel hash source-destination-ip	
Enable trunk hashing on the source and destination IP.	
Command mode: Global configuration	
portchannel hash source-destination-mac	
Enable trunk hashing on the source and destination MAC address.	
Command mode: Global configuration	
show portchannel hash	
Display current trunk hash setting.	
Command mode: All	

Link Aggregation Control Protocol Configuration

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

Table 178 Link Aggregation Control Protocol Commands

Command Syntax and Usage

lACP system-priority <1-65535>

Defines the priority value for the GbESM. Lower numbers provide higher priority. The default value is 32768.

Command mode: Global configuration

lACP timeout {short|long}

Defines the timeout period before invalidating LACP data from a remote partner. Choose *short* (3 seconds) or *long* (90 seconds). The default value is *long*.

Note: It is recommended that you use a timeout value of *long*, to reduce LACPDU processing. If your GbESM's CPU utilization rate remains at 100% for periods of 90 seconds or more, consider using static trunks instead of LACP.

Command mode: Global configuration

no lACP <1-65535>

Deletes a selected LACP trunk, based on its *admin key*. This command is equivalent to disabling LACP on each of the ports configured with the same *admin key*.

Command mode: Global configuration

show lACP

Display current LACP configuration.

Command mode: All

LACP Port Configuration

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

Table 179 Link Aggregation Control Protocol Commands

Command Syntax and Usage

lacp mode {**off**|**active**|**passive**}

Set the LACP mode for this port, as follows:

- ❑ **off**
Turn LACP off for this port. You can use this port to manually configure a static trunk. The default value is **off**.
- ❑ **active**
Turn LACP on and set this port to active. Active ports initiate LACPDUs.
- ❑ **passive**
Turn LACP on and set this port to passive. Passive ports do not initiate LACPDUs, but respond to LACPDUs from active ports.

Command mode: Interface port

lacp priority <1-65535>

Sets the priority value for the selected port. Lower numbers provide higher priority. The default value is 32768.

Command mode: Interface port

lacp key <1-65535>

Set the admin key for this port. Only ports with the same *admin key* and *oper key* (operational state generated internally) can form a LACP trunk group.

Command mode: Interface port

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

Displays the current LACP configuration for this port.

Command mode: All

Layer 2 Failover Configuration

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

Table 180 Layer 2 Failover Configuration Commands

Command Syntax and Usage

failover vlan

Globally turns VLAN monitor `on`. When the VLAN Monitor is `on`, the switch automatically disables only internal ports that belong to the same VLAN as ports in the failover trigger. The default value is `off`.

Command mode: Global configuration

no failover vlan

Globally turns VLAN monitor `off`. When the VLAN Monitor is `on`, the switch automatically disables only internal ports that belong to the same VLAN as ports in the failover trigger. The default value is `off`.

Command mode: Global configuration

failover enable

Globally turns Layer 2 Failover `on`.

Command mode: Global configuration

no failover enable

Globally turns Layer 2 Failover `off`.

Command mode: Global configuration

show failover trigger

Displays current Layer 2 Failover parameters.

Command mode: All

Failover Trigger Configuration

Table 181 Failover Trigger Configuration Commands

Command Syntax and Usage	
[no] failover trigger <1-8> enable	
Enables or disables the Failover trigger.	
Command mode: Global configuration	
no failover trigger <1-8>	
Deletes the Failover trigger.	
Command mode: Global configuration	
failover trigger <1-8> limit <0-1024>	
Configures the minimum number of operational links allowed within each trigger before the trigger initiates a failover event. If you enter a value of zero (0), the switch triggers a failover event only when no links in the trigger are operational.	
Command mode: Global configuration	
show failover trigger <1-8>	
Displays the current failover trigger settings.	
Command mode: All except User EXEC	

Auto Monitor Configuration

Table 182 Auto Monitor Configuration Commands

Command Syntax and Usage

failover trigger <1-8> **amon portchannel** <trunk number>

Adds a trunk group to the Auto Monitor.

Command mode: Global configuration

no failover trigger <1-8> **amon portchannel** <trunk number>

Removes a trunk group from the Auto Monitor.

Command mode: Global configuration

failover trigger <1-8> **amon adminkey** <1-65535>

Adds a LACP admin key to the Auto Monitor. LACP trunks formed with this *admin key* will be included in the Auto Monitor.

Command mode: Global configuration

no failover trigger <1-8> **amon adminkey** <1-65535>

Removes a LACP admin key from the Auto Monitor.

Command mode: Global configuration

Failover Manual Monitor Port Configuration

Use these commands to define the port link(s) to monitor. The Manual Monitor Port configuration accepts only external uplink ports.

Note – AMON and MMON configurations are mutually exclusive.

Table 183 Failover Manual Monitor Port commands

Command Syntax and Usage

failover trigger <1-8> **mmmon monitor member** <port alias or number>

Adds the selected port to the Manual Monitor Port configuration.

Command mode: Global configuration

Table 183 Failover Manual Monitor Port commands**Command Syntax and Usage**

no failover trigger <1-8> **mmon monitor member** <port alias or number>

Removes the selected port from the Manual Monitor Port configuration.

Command mode: Global configuration

failover trigger <1-8> **mmon monitor portchannel** <trunk number>

Adds the selected trunk group to the Manual Monitor Port configuration.

Command mode: Global configuration

no failover trigger <1-8> **mmon monitor portchannel** <trunk number>

Removes the selected trunk group to the Manual Monitor Port configuration.

Command mode: Global configuration

failover trigger <1-8> **mmon monitor adminkey** <1-65535>

Adds an LACP *admin key* to the Manual Monitor Port configuration. LACP trunks formed with this *admin key* will be included in the Manual Monitor Port configuration.

Command mode: Global configuration

no failover trigger <1-8> **mmon monitor adminkey** <1-65535>

Removes an LACP admin key from the Manual Monitor Port configuration.

Command mode: Global configuration

show failover trigger <1-8>

Displays the current Failover settings.

Command mode: All except User EXEC

Failover Manual Monitor Control Configuration

Use these commands to define the port link(s) to control. The Manual Monitor Control configuration accepts internal and external ports, but not management ports.

Table 184 Failover Manual Monitor Control commands

Command Syntax and Usage

failover trigger <1-8> **mmon control member** <port alias or number>

Adds the selected port to the Manual Monitor Control configuration.

Command mode: Global configuration

no failover trigger <1-8> **mmon control member** <port alias or number>

Removes the selected port from the Manual Monitor Control configuration.

Command mode: Global configuration

failover trigger <1-8> **mmon control portchannel** <trunk number>

Adds the selected trunk group to the Manual Monitor Control configuration.

Command mode: Global configuration

no failover trigger <1-8> **mmon control portchannel** <trunk number>

Removes the selected trunk group to the Manual Monitor Control configuration.

Command mode: Global configuration

failover trigger <1-8> **mmon control adminkey** <1-65535>

Adds an LACP *admin key* to the Manual Monitor Control configuration. LACP trunks formed with this *admin key* will be included in the Manual Monitor Control configuration.

Command mode: Global configuration

no failover trigger <1-8> **mmon control adminkey** <1-65535>

Removes an LACP admin key from the Manual Monitor Control configuration.

Command mode: Global configuration

show failover trigger <1-8>

Displays the current Failover settings.

Command mode: All except User EXEC

Hot Links Configuration

Use these commands to configure Hot Links. For more information about Hot Links, see “Hot Links” in the *BLADEOS 6.3 Application Guide*.

Table 185 Hot Links Configuration Commands

Command Syntax and Usage	
[no] hotlinks bpdu	<p>Enables or disables the ability to flood BPDUs on the active Hot Links interface when the interface belongs to a Spanning Tree group that is globally turned <code>off</code>.</p> <p>The default value is <code>disabled</code>.</p> <p>Command mode: Global configuration</p>
[no] hotlinks fdb-update	<p>Enables or disables FDB Update, which allows the switch to send FDB and MAC update packets over the active interface.</p> <p>The default value is <code>disabled</code>.</p> <p>Command mode: Global configuration</p>
hotlinks enable	<p>Globally enables Hot Links.</p> <p>Command mode: Global configuration</p>
no hotlinks enable	<p>Globally disables Hot Links.</p> <p>Command mode: Global configuration</p>
show hotlinks	<p>Displays current Hot Links parameters.</p> <p>Command mode: All</p>

Hot Links Trigger Configuration

Table 186 Hot Links Trigger Configuration Commands

Command Syntax and Usage

hotlinks trigger <1-200> **forward-delay** <0-3600>

Configures the Forward Delay interval, in seconds. The default value is 1.

Command mode: Global configuration

hotlinks trigger <1-200> **name** <1-32 characters>

Defines a name for the Hot Links trigger.

Command mode: 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`.

Command mode: Global configuration

[no] **hotlinks trigger** <1-200> **enable**

Enables or disables the Hot Links trigger.

Command mode: Global configuration

no hotlinks trigger <1-200>

Deletes the Hot Links trigger.

Command mode: Global configuration

show hotlinks trigger <1-200>

Displays the current Hot Links settings.

Command mode: All

Hot Links Master Configuration

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

Table 187 Hot Links Master Configuration Commands

Command Syntax and Usage	
[no] hotlinks trigger <1-200> master port <port alias or number>	
Adds the selected port to the Hot Links Master interface.	
Command mode: Global configuration	
[no] hotlinks trigger <1-200> master portchannel <0-16>	
Adds the selected trunk group to the Master interface.	
Command mode: Global configuration	
[no] hotlinks trigger <1-200> master adminkey <0-65535>	
Adds 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. Enter 0 (zero) to clear the <i>admin key</i> .	
Command mode: Global configuration	
show hotlinks trigger <1-200>	
Displays the current Hot Links settings.	
Command mode: All	

Hot Links Backup Configuration

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

Table 188 Hot Links Backup Configuration Commands

Command Syntax and Usage

[no] hotlinks trigger <1-200> backup port <port alias or number>

Adds the selected port to the Hot Links Backup interface.

Command mode: Global configuration

[no] hotlinks trigger <1-200> backup portchannel <0-16>

Adds the selected trunk group to the Backup interface.

Command mode: Global configuration

[no] hotlinks trigger <1-200> backup adminkey <0-65535>

Adds an LACP *admin key* to the Backup interface. LACP trunks formed with this *admin key* will be included in the Backup interface. Enter 0 (zero) to clear the *admin key*.

Command mode: Global configuration

show hotlinks trigger <1-200>

Displays the current Hot Links settings.

Command mode: All

VLAN Configuration

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

By default, VLAN 1 is the only VLAN configured on the switch. Internal server ports and external uplink ports are members of VLAN 1 by default. Up to 1024 VLANs can be configured on the GbESM.

VLANs can be assigned any number between 1 and 4094. VLAN 4095 is reserved for switch management.

Table 189 VLAN Configuration Commands

Command Syntax and Usage

vlan <VLAN number>

Enter VLAN configuration mode.

Command mode: Global configuration

protocol-vlan <1-8>

Configures the Protocol-based VLAN (PVLAN).

Command mode: VLAN

name <1-32 characters>

Assigns a name to the VLAN or changes the existing name. The default VLAN name is the first one.

Command mode: VLAN

stg <STG number>

Assigns a VLAN to a Spanning Tree Group.

Command mode: VLAN

[no] vmap <1-128> [**extports**|**intports**]

Adds or removes a VLAN Map to the VLAN membership. You can choose to limit operation of the VLAN Map to internal ports only or external ports only. If you do not select a port type, the VMAP is applied to the entire VLAN.

Command mode: VLAN

Table 189 VLAN Configuration Commands

Command Syntax and Usage

member <port alias or number>

Adds port(s) to the VLAN membership.

Command mode: VLAN

no member <port alias or number>

Removes port(s) from this VLAN.

Command mode: VLAN

[no] management

Configures this VLAN as a management VLAN. You must add the management ports (MGT1 and MGT2) to each new management VLAN. External ports cannot be added to management VLANs.

Command mode: VLAN

enable

Enables this VLAN.

Command mode: VLAN

no enable

Disables this VLAN without removing it from the configuration.

Command mode: VLAN

no vlan <VLAN number>

Deletes this VLAN.

Command mode: VLAN

show vlan information

Displays the current VLAN configuration.

Command mode: All

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

Protocol-Based VLAN Configuration

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

Table 190 Protocol VLAN commands

Command Syntax and Usage

protocol-vlan <1-8> **frame-type** {ether2|llc|snap} <Ethernet type>

Configures the frame type and the Ethernet type for the selected protocol.

Ethernet type consists of a 4-digit (16 bit) hex code, such as 0080 (IPv4).

Command mode: VLAN

protocol-vlan <1-8> **protocol** <protocol type>

Selects a pre-defined protocol, as follows:

- ☐ decEther2: DEC Local Area Transport
- ☐ ipv4Ether2: Internet IP (IPv4)
- ☐ ipv6Ether2: IPv6
- ☐ ipx802.2: Novell IPX 802.2
- ☐ ipx802.3: Novell IPX 802.3
- ☐ ipxEther2: Novell IPX
- ☐ ipxSnap: Novell IPX SNAP
- ☐ netbios: NetBIOS 802.2
- ☐ rarpEther2: Reverse ARP
- ☐ sna802.2: SNA 802.2
- ☐ snaEther2: IBM SNA Service on Ethernet
- ☐ vinesEther2: Banyan VINES
- ☐ xnsEther2: XNS Compatibility

Command mode: VLAN

protocol-vlan <1-8> **priority** <0-7>

Configures the priority value for this PVLAN.

Command mode: VLAN

protocol-vlan <1-8> **member** <port alias or number>

Adds a port to the selected PVLAN.

Command mode: VLAN

Table 190 Protocol VLAN commands**Command Syntax and Usage**

no protocol-vlan <1-8> **member** *<port alias or number>*

Removes a port from the selected PVLAN.

Command mode: VLAN

[no] protocol-vlan <1-8> **tag-pvlan** *<port alias or number>*

Defines a port that will be tagged by the selected protocol on this VLAN.

Command mode: VLAN

protocol-vlan <1-8> **enable**

Enables the selected protocol on the VLAN.

Command mode: VLAN

no protocol-vlan <1-8> **enable**

Disables the selected protocol on the VLAN.

Command mode: VLAN

no protocol-vlan <1-8>

Deletes the selected protocol configuration from the VLAN.

Command mode: VLAN

show protocol-vlan <1-8>

Displays current parameters for the selected PVLAN.

Command mode: All

Private VLAN Configuration

Use the following commands to configure Private VLAN.

Table 191 Private VLAN commands

Command Syntax and Usage

private-vlan type primary

Configures the VLAN type as a Primary VLAN.

A Private VLAN must have only one primary VLAN. The primary VLAN carries unidirectional traffic to ports on the isolated VLAN or to community VLAN.

Command mode: VLAN

private-vlan type community

Configures the VLAN type as a community VLAN.

Community VLANs carry upstream traffic from host ports. A Private VLAN may have multiple community VLANs.

Command mode: VLAN

private-vlan type isolated

Configures the VLAN type as an isolated VLAN.

The isolated VLAN carries unidirectional traffic from host ports. A Private VLAN may have only one isolated VLAN.

Command mode: VLAN

no private-vlan type

Clears the private-VLAN type.

Command mode: VLAN

[no] private-vlan map [<2-4094>]

Configures Private VLAN mapping between a secondary VLAN and a primary VLAN. Enter the primary VLAN ID. Secondary VLANs have the *type* defined as *isolated* or *community*. Use the **no** form to remove the mapping between the secondary VLAN and the primary VLAN.

Command mode: VLAN

Table 191 Private VLAN commands

Command Syntax and Usage
private-vlan enable Enables the private VLAN. Command mode: VLAN
no private-vlan enable Disables the Private VLAN. Command mode: VLAN
show private-vlan [<2-4094>] Displays current parameters for the selected Private VLAN(s). Command mode: VLAN

Layer 3 Configuration

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

Table 192 Layer 3 Configuration Commands

Command Syntax and Usage

interface ip *<interface number>*

Configures the IP Interface. The GbESM supports up to 128 IP interfaces.

Command mode: Global configuration

To view command options, see [page 320](#).

route-map {*<1-32>*}

Enter IP Route Map mode.

Command mode: Global configuration

To view command options, see [page 331](#).

router rip

Configures the Routing Interface Protocol.

Command mode: Global configuration

To view command options, see [page 335](#).

router ospf

Configures OSPF.

Command mode: Global configuration

To view command options, see [page 339](#).

ipv6 router ospf

Enters OSPFv3 configuration mode.

Command mode: Global configuration

To view command options, see [page 382](#).

Table 192 Layer 3 Configuration Commands

Command Syntax and Usage

router bgp

Configures Border Gateway Protocol.

Command mode: Global configuration

To view command options, see [page 351](#).

router vrrp

Configures Virtual Router Redundancy.

Command mode: Global configuration

To view command options, see [page 369](#).

ip router-id *<IP address>*

Sets the router ID.

Command mode: Global configuration

show layer3

Displays the current IP configuration.

Command mode: All

IP Interface Configuration

The GbESM supports up to 128 IP interfaces. Each IP interface represents the GbESM on an IP subnet on your network. The Interface option is disabled by default.

Note – To maintain connectivity between the management module and the GbESM, use the management module interface to change the IP address of the switch.

Table 193 IP Interface Configuration Commands

Command Syntax and Usage

interface ip *<interface number>*

Enter IP interface mode.

Command mode: Global configuration

ip address *<IP address>* [*<IP netmask>*]

Configures the IP address of the switch interface, using dotted decimal notation.

Command mode: Interface IP

ip netmask *<IP netmask>*

Configures the IP subnet address mask for the interface, using dotted decimal notation.

Command mode: Interface IP

ipv6 address *<IP address (such as 3001:0:0:0:0:abcd:12)>*
[**anycast** | **enable** | **no enable**]

Configures the IPv6 address of the switch interface, using hexadecimal format with colons.

Command mode: Interface IP

ipv6 secaddr6 address *<IP address (such as 3001:0:0:0:0:abcd:12)>*
<prefix length> [**anycast**]

Configures the secondary IPv6 address of the switch interface, using hexadecimal format with colons.

Command mode: Interface IP

ipv6 prefixlen *<IPv6 prefix length (1-128)>*

Configures the subnet IPv6 prefix length. The default value is 0 (zero).

Command mode: Interface IP

Table 193 IP Interface Configuration Commands**Command Syntax and Usage****vlan** *<VLAN number>*

Configures the VLAN number for this interface. Each interface can belong to one VLAN.

IPv4: Each VLAN can contain multiple IPv4 interfaces.

IPv6: Each VLAN can contain only one IPv6 interface.

Command mode: Interface IP

[no] relay

Enables or disables the BOOTP relay on this interface. It is enabled by default.

Command mode: Interface IP

[no] ip6host

Enables or disables the IPv6 Host Mode on this interface. The default value is disabled for data interfaces, and enabled for the management interface.

Command mode: Interface IP

enable

Enables this IP interface.

Command mode: Interface IP

no enable

Disables this IP interface.

Command mode: Interface IP

no interface ip *<interface number>*

Removes this IP interface.

Command mode: Interface IP

show interface ip *<interface number>*

Displays the current interface settings.

Command mode: All

IPv6 Neighbor Discovery Configuration

The following table describes the IPv6 Neighbor Discovery Configuration commands.

Table 194 IPv6 Neighbor Discovery Configuration commands

Command Syntax and Usage	
[no] ipv6 nd suppress-ra	<p>Enables or disables IPv6 Router Advertisements on the interface. The default setting is disabled (suppress Router Advertisements).</p> <p>Command mode: Interface IP</p>
[no] ipv6 nd managed-config	<p>Enables or disables the managed address configuration flag of the interface. When enabled, the host IP address can be set automatically through DHCP.</p> <p>The default setting is disabled.</p> <p>Command mode: Interface IP</p>
[no] ipv6 nd other-config	<p>Enables or disables the other stateful configuration flag, which allows the interface to use DHCP for other stateful configuration. The default setting is disabled.</p> <p>Command mode: Interface IP</p>
ipv6 nd ra-lifetime <0-9000>	<p>Configures the IPv6 Router Advertisement lifetime interval. The RA lifetime interval must be greater than or equal to the RA maximum interval (advint).</p> <p>The default value is 1800 seconds.</p> <p>Command mode: Interface IP</p>
[no] ipv6 nd dad-attempts <1-10>	<p>Configures the maximum number of duplicate address detection attempts.</p> <p>The default value is 1.</p> <p>Command mode: Interface IP</p>
[no] ipv6 nd reachable-time <1-3600>	<p>Configures the advertised reachability time. The default value is 30 seconds.</p> <p>Command mode: Interface IP</p>

Table 194 IPv6 Neighbor Discovery Configuration commands**Command Syntax and Usage****[no] ipv6 nd ra-interval** *<4-1800>*

Configures the Router Advertisement maximum interval. The default value is 600 seconds.

Note: Set the maximum RA interval to a value greater than or equal to 4/3 of the minimum RA interval.

Command mode: Interface IP

[no] ipv6 nd ra-intervalmin *<4-1800>*

Configures the Router Advertisement minimum interval. The default value is 198 seconds.

Note: Set the minimum RA interval to a value less than or equal to 0.75 of the maximum RA interval.

Command mode: Interface IP

[no] ipv6 nd retransmit-time *<1-3600>*

Configures the Router Advertisement re-transmit timer. The default value is 1 second.

Command mode: Interface IP

[no] ipv6 nd hops-limit *<1-255>*

Configures the Router Advertisement hop limit.

The default value is 64.

Command mode: Interface IP

Default Gateway Configuration

The switch can be configured with up to 132 IPv4 gateways. Gateways 1–3 are reserved for default gateways. Gateway 132 is reserved for switch management.

This option is disabled by default.

Table 195 Default Gateway Commands

Command Syntax and Usage	
ip gateway <1-132> address <IP address>	
Configures the IP address of the default IP gateway using dotted decimal notation.	
Command mode: Global configuration	
ip gateway <1-132> interval <0-60>	
The switch pings the default gateway to verify that it's up. This command sets the time between health checks. The range is from 0 to 60 seconds. The default is 2 seconds.	
Command mode: Global configuration	
ip gateway <1-132> retry <1-120>	
Sets the number of failed health check attempts required before declaring this default gateway inoperative. The range is from 1 to 120 attempts. The default is 8 attempts.	
Command mode: Global configuration	
[no] ip gateway <1-132> arp-health-check	
Enables or disables Address Resolution Protocol (ARP) health checks. The default setting is disabled . The arp option does not apply to management gateways.	
Command mode: Global configuration	
ip gateway <1-132> enable	
Enables the gateway for use.	
Command mode: Global configuration	
no ip gateway <1-132> enable	
Disables the gateway.	
Command mode: Global configuration	

Table 195 Default Gateway Commands

Command Syntax and Usage

no ip gateway *<1-132>*

Deletes the gateway from the configuration.

Command mode: Global configuration

show ip gateway *<1-132>*

Displays the current gateway settings.

Command mode: All

IPv4 Static Route Configuration

Up to 128 IPv4 static routes can be configured.

Table 196 IP Static Route Configuration Commands

Command Syntax and Usage

ip route *<IP subnet>* *<IP netmask>* *<IP nexthop>* [*<interface number>*]

Adds a static route. You will be prompted to enter a destination IP address, destination subnet mask, and gateway address. Enter all addresses using dotted decimal notation.

Command mode: Global configuration

no ip route *<IP subnet>* *<IP netmask>* [*<interface number>*]

Removes a static route. The destination address of the route to remove must be specified using dotted decimal notation.

Command mode: Global configuration

no ip route destination-address *<IP address>*

Clears all IP static routes with this destination.

Command mode: Global configuration

Table 196 IP Static Route Configuration Commands

Command Syntax and Usage
no ip route gateway <IP address> Clears all IP static routes that use this gateway. Command mode: Global configuration
show ip route static Displays the current IP static routes. Command mode: All except User EXEC

IP Multicast Route Configuration

The following table describes the IP Multicast (IPMC) route commands.

Note – Before you can add an IPMC route, IGMP must be turned on and IGMP Relay must be enabled.

Table 197 IP Multicast Route Configuration Commands

Command Syntax and Usage
ip mroute <IPMC destination> <VLAN number> <port alias or number> { primary backup host } [<virtual router ID> none] Adds a static multicast route. The destination address, VLAN, and member port of the route must be specified. Indicate whether the route is used for a primary, backup, or host multicast router. Command mode: Global configuration
no ip mroute <IPMC destination> <VLAN number> <port alias or number> { primary backup host } [<virtual router ID> none] Removes a static multicast route. The destination address, VLAN, and member port of the route to remove must be specified. Command mode: Global configuration

Table 197 IP Multicast Route Configuration Commands**Command Syntax and Usage**

```
ip mroute <IP address> <VLAN number> portchannel <trunk group number>
    {primary|backup|host} [<virtual router ID> | none]
```

Adds a static multicast route. The destination address, VLAN, and member trunk group of the route must be specified. Indicate whether the route is used for a primary, backup, or host multicast router.

Command mode: Global configuration

```
no ip mroute <IP address> <VLAN number> portchannel <trunk group number>
    {primary|backup|host} [<virtual router ID> | none]
```

Removes a static multicast route. The destination address, VLAN, and member trunk group of the route to remove must be specified.

Command mode: Global configuration

```
ip mroute <IP address> <VLAN number> adminkey <1-65535>
    {primary|backup|host} [<virtual router ID> | none]
```

Adds a static multicast route. The destination address, VLAN, and LACP *admin key* of the route must be specified. Indicate whether the route is used for a primary, backup, or host multicast router.

Command mode: Global configuration

```
no ip mroute <IP address> <VLAN number> adminkey <1-65535> | none]
```

Removes a static multicast route. The destination address, VLAN, and LACP *admin key* of the route to remove must be specified.

Command mode: Global configuration

```
show ip mroute
```

Displays the current IP multicast routes.

Command mode: All except User EXEC

ARP Configuration

Address Resolution Protocol (ARP) is the TCP/IP protocol that resides within the Internet layer. ARP resolves a physical address from an IP address. ARP queries machines on the local network for their physical addresses. ARP also maintains IP to physical address pairs in its cache memory. In any IP communication, the ARP cache is consulted to see if the IP address of the computer or the router is present in the ARP cache. Then the corresponding physical address is used to send a packet.

Table 198 ARP Configuration Commands

Command Syntax and Usage
ip arp rearp <2-120>
Defines re-ARP period in minutes. You can set this duration between 2 and 120 minutes.
Command mode: Global configuration
show ip arp
Displays the current ARP configurations.
Command mode: All except User EXEC

ARP Static Configuration

Static ARP entries are permanent in the ARP cache and do not age out like the ARP entries that are learned dynamically. Static ARP entries enable the switch to reach the hosts without sending an ARP broadcast request to the network. Static ARPs are also useful to communicate with devices that do not respond to ARP requests. Static ARPs can also be configured on some gateways as a protection against malicious ARP Cache corruption and possible DOS attacks.

Table 199 ARP Static Configuration Commands

Command Syntax and Usage
ip arp <IP address> <MAC address> vlan <vlan number> port <port alias or number>
Adds a permanent ARP entry.
Command mode: Global configuration
no ip arp <IP address>
Deletes a permanent ARP entry.
Command mode: Global configuration

Table 199 ARP Static Configuration Commands**Command Syntax and Usage****no ip arp all**

Deletes all static ARP entries.

Command mode: Global configuration**show ip arp static**

Displays current static ARP configuration.

Command mode: All except User EXEC**IP Forwarding Configuration****Table 200** IP Forwarding Configuration Commands**Command Syntax and Usage****[no] ip routing directed-broadcasts**

Enables or disables forwarding directed broadcasts. The default setting is disabled.

Command mode: Global configuration**[no] ip routing no-icmp-redirect**

Enables or disables ICMP re-directs. The default setting is disabled.

Command mode: Global configuration**ip routing**

Enables IP forwarding (routing) on the GbESM. Forwarding is turned on by default.

Command mode: Global configuration**no ip routing**

Disables IP forwarding (routing) on the GbESM.

Command mode: Global configuration**show ip routing**

Displays the current IP forwarding settings.

Command mode: All except User EXEC

Network Filter Configuration

Table 201 IP Network Filter Configuration Commands

Command Syntax and Usage

ip match-address <1-256> <IP address> <IP netmask>

Sets the starting IP address and IP Netmask for this filter to define the range of IP addresses that will be accepted by the peer when the filter is enabled. The default address is 0.0.0.0 0.0.0.0

For Border Gateway Protocol (BGP), assign the network filter to an access-list in a route map, then assign the route map to the peer.

Command mode: Global configuration.

ip match-address <1-256> **enable**

Enables the Network Filter configuration.

Command mode: Global configuration

no ip match-address <1-256> **enable**

Disables the Network Filter configuration.

Command mode: Global configuration

no ip match-address <1-256>

Deletes the Network Filter configuration.

Command mode: Global configuration

show ip match-address [<1-256>]

Displays the current the Network Filter configuration.

Command mode: All except User EXEC

Routing Map Configuration

Note – The *map number* (1-32) represents the routing map you wish to configure.

Routing maps control and modify routing information.

Table 202 Routing Map Configuration Commands

Command Syntax and Usage

route-map <1-32>

Enter route map configuration mode.

Command mode: Route map

[no] access-list <1-8>

Configures the Access List.

Command mode: Route map

For more information, see [page 333](#).

[no] as-path-list <1-8>

Configures the Autonomous System (AS) Filter.

Command mode: Route map

For more information, see [page 334](#).

[no] as-path-preference <1-65535>

Sets the AS path preference of the matched route. You can configure up to three path preferences.

Command mode: Route map

[no] local-preference <0-4294967294>

Sets the local preference of the matched route, which affects both inbound and outbound directions. The path with the higher preference is preferred.

Command mode: Route map

[no] metric <1-4294967294>

Sets the metric of the matched route.

Command mode: Route map

Table 202 Routing Map Configuration Commands**Command Syntax and Usage****[no] metric-type {1|2}**

Assigns the type of OSPF metric. The default is type 1.

- **Type 1**—External routes are calculated using both internal and external metrics.
- **Type 2**—External routes are calculated using only the external metrics. Type 1 routes have more cost than Type 2.
- **none**—Removes the OSPF metric.

Command mode: Route map

precedence <1-255>

Sets the precedence of the route map. The smaller the value, the higher the precedence. Default value is 10.

Command mode: Route map

[no] weight <0-65534>

Sets the weight of the route map.

Command mode: Route map

enable

Enables the route map.

Command mode: Route map

no enable

Disables the route map.

Command mode: Route map

no route-map <1-32>

Deletes the route map.

Command mode: Route map

show route-map [<1-32>]

Displays the current route configuration.

Command mode: All except User EXEC

IP Access List Configuration

Note – The *route map number* (1-32) and the *access list number* (1-8) represent the IP access list you wish to configure.

Table 203 IP Access List Configuration Commands

Command Syntax and Usage

[no] access-list <1-8> match-address <1-256>

Sets the network filter number.

Command mode: Route map

See “[Network Filter Configuration](#)” on page 330 for details.

[no] access-list <1-8> metric <1-4294967294>

Sets the metric value in the AS-External (ASE) LSA.

Command mode: Route map

access-list <1-8> action {permit|deny}

Permits or denies action for the access list.

Command mode: Route map

access-list <1-8> enable

Enables the access list.

Command mode: Route map

no access-list <1-8> enable

Disables the access list.

Command mode: Route map

no access-list <1-8>

Deletes the access list.

Command mode: Route map

show route-map <1-32> access-list <1-8>

Displays the current Access List configuration.

Command mode: All except User EXEC

Autonomous System Filter Path Configuration

Note – The *rmap number* and the *path number* represent the AS path you wish to configure.

Table 204 AS Filter Configuration Commands

Command Syntax and Usage

as-path-list <1-8> **as-path** <1-65535>

Sets the Autonomous System filter’s path number.

Command mode: Route map

as-path-list <1-8> **action** {**permit**|**deny**}

Permits or denies Autonomous System filter action.

Command mode: Route map

as-path-list <1-8> **enable**

Enables the Autonomous System filter.

Command mode: Route map

no as-path-list <1-8> **enable**

Disables the Autonomous System filter.

Command mode: Route map

no as-path-list <1-8>

Deletes the Autonomous System filter.

Command mode: Route map

show route-map <1-32> **as-path-list** <1-8>

Displays the current Autonomous System filter configuration.

Command mode: All except User EXEC

Routing Information Protocol Configuration

RIP commands are used for configuring Routing Information Protocol parameters. This option is turned off by default.

Table 205 Routing Information Protocol Commands

Command Syntax and Usage
router rip Enter Router RIP configuration mode. Command mode: Router RIP
timers update <1-120> Configures the time interval for sending for RIP table updates, in seconds. The default value is 30 seconds. Command mode: Router RIP
enable Globally turns RIP on . Command mode: Router RIP
no enable Globally turns RIP off . Command mode: Router RIP
show ip rip Displays the current RIP configuration. Command mode: All except User EXEC

Routing Information Protocol Interface Configuration

The RIP Interface commands are used for configuring Routing Information Protocol parameters for the selected interface.

Note – Do not configure RIP version 1 parameters if your routing equipment uses RIP version 2.

Table 206 RIP Interface Commands

Command Syntax and Usage

ip rip version { 1 | 2 | both }

Configures the RIP version used by this interface. The default value is version 2.

Command mode: Interface IP

[no] ip rip supply

When enabled, the switch supplies routes to other routers. The default value is *enabled*.

Command mode: Interface IP

[no] ip rip listen

When enabled, the switch learns routes from other routers. The default value is *enabled*.

Command mode: Interface IP

[no] ip rip poison

When enabled, the switch uses split horizon with poisoned reverse. When disabled, the switch uses only split horizon. The default value is *disabled*.

Command mode: Interface IP

[no] ip rip split-horizon

Enables or disables split horizon. The default value is **enabled**.

Command mode: Interface IP

[no] ip rip triggered

Enables or disables Triggered Updates. Triggered Updates are used to speed convergence. When enabled, Triggered Updates force a router to send update messages immediately, even if it is not yet time for the update message. The default value is *enabled*.

Command mode: Interface IP

Table 206 RIP Interface Commands

Command Syntax and Usage

[no] ip rip multicast-updates

Enables or disables multicast updates of the routing table (using address 224.0.0.9). The default value is *enabled*.

Command mode: Interface IP

[no] ip rip default-action {listen|supply|both}

When enabled, the switch accepts RIP default routes from other routers, but gives them lower priority than configured default gateways. When disabled, the switch rejects RIP default routes. The default value is *none*.

Command mode: Interface IP

[no] ip rip metric [<1-15>]

Configures the route metric, which indicates the relative distance to the destination. The default value is 1.

Command mode: Interface IP

[no] ip rip authentication type [<password>]

Configures the authentication type. The default is *none*.

Command mode: Interface IP

[no] ip rip authentication key <password>

Configures the authentication key password.

Command mode: Interface IP

ip rip enable

Enables this RIP interface.

Command mode: Interface IP

no ip rip enable

Disables this RIP interface.

Command mode: Interface IP

show interface ip <interface number> rip

Displays the current RIP configuration.

Command mode: All

RIP Route Redistribution Configuration

The following table describes the RIP Route Redistribution commands.

Table 207 RIP Redistribution Commands

Command Syntax and Usage	
redistribute { fixed static ospf eospf ebgp ibgp } <1-32>	<p>Adds selected routing maps to the RIP route redistribution list. To add specific route maps, enter routing map numbers, separated by a comma (,). To add all 32 route maps, type all.</p> <p>The routes of the redistribution protocol matched by the route maps in the route redistribution list will be redistributed.</p> <p>Command mode: Router RIP</p>
no redistribute { fixed static ospf eospf ebgp ibgp } <1-32>	<p>Removes the route map from the RIP route redistribution list.</p> <p>To remove specific route maps, enter routing map numbers, separated by a comma (,). To remove all 32 route maps, type all.</p> <p>Command mode: Router RIP</p>
redistribute { fixed static ospf eospf ebgp ibgp } export <1-15>	<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 none.</p> <p>Command mode: Router RIP</p>
show ip rip redistribute	<p>Displays the current RIP route redistribute configuration.</p> <p>Command mode: All except User EXEC</p>

Open Shortest Path First Configuration

Table 208 OSPF Configuration Commands

Command Syntax and Usage

router ospf

Enter Router OSPF configuration mode.

Command mode: Global configuration

area-range *<1-16>*

Configures summary routes for up to 16 IP addresses.

Command mode: Router OSPF

See [page 343](#) to view command options.

ip ospf *<interface number>*

Configures the OSPF interface.

Command mode: Interface IP

See [page 344](#) to view command options.

area-virtual-link *<1-3>*

Configures the Virtual Links used to configure OSPF for a Virtual Link.

Command mode: Router OSPF

See [page 346](#) to view command options.

message-digest-key *<1-255>* **md5-key** *<text string>*

Assigns a string to MD5 authentication key.

Command mode: Router OSPF

host *<1-128>*

Configures OSPF for the host routes. Up to 128 host routes can be configured. Host routes are used for advertising network device IP addresses to external networks to perform server load balancing within OSPF. It also makes Area Border Route (ABR) load sharing and ABR failover possible.

Command mode: Router OSPF

See [page 348](#) to view command options.

Table 208 OSPF Configuration Commands

Command Syntax and Usage

lsdb-limit *<LSDB limit (0-6144, 0 for no limit)>*

Sets the link state database limit.

Command mode: Router OSPF

[no] default-information *<1-16777214> {<AS value (1-2)>}*

Sets one default route among multiple choices in an area. Use none for no default.

Command mode: Router OSPF

enable

Enables OSPF on the GbESM.

Command mode: Router OSPF

no enable

Disables OSPF on the GbESM.

Command mode: Router OSPF

show ip ospf

Displays the current OSPF configuration settings.

Command mode: All except User EXEC

Area Index Configuration

Table 209 Area Index Configuration Commands

Command Syntax and Usage

area <0-2> **area-id** <IP address>

Defines the IP address of the OSPF area number.

Command mode: Router OSPF

area <0-2> **type** {**transit**|**stub**|**nssa**}

Defines the type of area. For example, when a virtual link has to be established with the backbone, the area type must be defined as transit.

Transit area: allows area summary information to be exchanged between routing devices. Any area that is not a stub area or NSSA is considered to be transit area.

Stub area: is an area where external routing information is not distributed. Typically, a stub area is connected to only one other area.

NSSA: Not-So-Stubby Area (NSSA) is similar to stub area with additional capabilities. For example, routes originating from within the NSSA can be propagated to adjacent transit and backbone areas. External routes from outside the Autonomous System (AS) can be advertised within the NSSA but are not distributed into other areas.

Command mode: Router OSPF

area <0-2> **stub-metric** <1-65535>

Configures a stub area to send a numeric metric value. All routes received via that stub area carry the configured metric to potentially influencing routing decisions.

Metric value assigns the priority for choosing the switch for default route. Metric type determines the method for influencing routing decisions for external routes.

Command mode: Router OSPF

[no] **area** <0-2> **authentication-type** {**password**|**md5**}

None: No authentication required.

Password: Authenticates simple passwords so that only trusted routing devices can participate.

MD5: This parameter is used when MD5 cryptographic authentication is required.

Command mode: Router OSPF

Table 209 Area Index Configuration Commands

Command Syntax and Usage

area <0-2> **spf-interval** <1-255>

Configures the minimum time interval, in seconds, between two successive SPF (shortest path first) calculations of the shortest path tree using the Dijkstra’s algorithm. The default value is 10 seconds.

Command mode: Router OSPF

area <0-2> **enable**

Enables the OSPF area.

Command mode: Router OSPF

no area <0-2> **enable**

Disables the OSPF area.

Command mode: Router OSPF

no area <0-2>

Deletes the OSPF area.

Command mode: Router OSPF

show ip ospf area <0-2>

Displays the current OSPF configuration.

Command mode: All except User EXEC

OSPF Summary Range Configuration

Table 210 OSPF Summary Range Configuration Commands

Command Syntax and Usage

area-range <1-16> **address** <IP address> <IP netmask>

Displays the base IP address or the IP address mask for the range.

Command mode: Router OSPF

area-range <1-16> **area** <0-2>

Displays the area index used by the GbESM.

Command mode: Router OSPF

[no] area-range <1-16> **hide**

Hides the OSPF summary range.

Command mode: Router OSPF

area-range <1-16> **enable**

Enables the OSPF summary range.

Command mode: Router OSPF

no area-range <1-16> **enable**

Disables the OSPF summary range.

Command mode: Router OSPF

no area-range <1-16>

Deletes the OSPF summary range.

Command mode: Router OSPF

show ip ospf area-range <1-16>

Displays the current OSPF summary range.

Command mode: Router OSPF

OSPF Interface Configuration

Table 211 OSPF Interface Configuration Commands

Command Syntax and Usage	
ip ospf area <0-2>	Configures the OSPF area index. Command mode: Interface IP
ip ospf priority <0-255>	Configures the priority value for the GbESM's OSPF interfaces. A priority value of 255 is the highest and 1 is the lowest. A priority value of 0 specifies that the interface cannot be used as Designated Router (DR) or Backup Designated Router (BDR). Command mode: Interface IP
ip ospf cost <1-65535>	Configures cost set for the selected path—preferred or backup. Usually the cost is inversely proportional to the bandwidth of the interface. Low cost indicates high bandwidth. Command mode: Interface IP
ip ospf hello-interval <1-65535> ip ospf hello-interval <1-65535ms>	Configures the interval, in seconds or milliseconds, between the <code>hello</code> packets for the interfaces. Command mode: Interface IP
ip ospf dead-interval <1-65535> ip ospf dead-interval <1-65535ms>	Configures the health parameters of a <code>hello</code> packet, in seconds or milliseconds, before declaring a silent router to be down. Command mode: Interface IP
ip ospf transit-delay <1-3600>	Configures the transit delay in seconds. Command mode: Interface IP

Table 211 OSPF Interface Configuration Commands**Command Syntax and Usage**

ip ospf retransmit-interval <1-3600>

Configures the retransmit interval in seconds.

Command mode: Interface IP

[no] ip ospf key <key string>

Sets the authentication key to clear the password.

Command mode: Interface IP

[no] ip ospf message-digest-key <1-255>

Assigns an MD5 key to the interface.

Command mode: Interface IP

[no] ip ospf passive-interface

Sets the interface as passive. On a passive interface, you can disable OSPF protocol exchanges, but the router advertises the interface in its LSAs so that IP connectivity to the attached network segment will be established.

Command mode: Interface IP

[no] ip ospf point-to-point

Sets the interface as point-to-point.

Command mode: Interface IP

ip ospf enable

Enables OSPF interface.

Command mode: Interface IP

no ip ospf enable

Disables OSPF interface.

Command mode: Interface IP

Table 211 OSPF Interface Configuration Commands

Command Syntax and Usage
no ip ospf Deletes the OSPF interface. Command mode: Interface IP
show interface ip <i><interface number></i> ospf Displays the current settings for OSPF interface. Command mode: All except User EXEC

OSPF Virtual Link Configuration

Table 212 OSPF Virtual Link Configuration Commands

Command Syntax and Usage
area-virtual-link <i><1-3></i> area <i><0-2></i> Configures the OSPF area index for the virtual link. Command mode: Router OSPF
area-virtual-link <i><1-3></i> hello-interval <i><1-65535></i> area-virtual-link <i><1-3></i> hello-interval <i><1-65535ms></i> Configures the authentication parameters of a hello packet, in seconds or milliseconds. The default value is 10 seconds. Command mode: Router OSPF
area-virtual-link <i><1-3></i> dead-interval <i><1-65535></i> area-virtual-link <i><1-3></i> dead-interval <i><1-65535ms></i> Configures the health parameters of a hello packet, in seconds or milliseconds. The default value is 60 seconds. Command mode: Router OSPF
area-virtual-link <i><1-3></i> transit-delay <i><1-3600></i> Configures the delay in transit, in seconds. The default value is one second. Command mode: Router OSPF

Table 212 OSPF Virtual Link Configuration Commands**Command Syntax and Usage**

area-virtual-link *<1-3>* **retransmit-interval** *<1-3600>*

Configures the retransmit interval, in seconds. The default value is five seconds.

Command mode: Router OSPF

area-virtual-link *<1-3>* **neighbor-router** *<IP address>*

Configures the router ID of the virtual neighbor. The default value is 0.0.0.0.

Command mode: Router OSPF

[no] **area-virtual-link** *<1-3>* **key** *<password>*

Configures the password (up to eight characters) for each virtual link. The default setting is none.

Command mode: Router OSPF

area-virtual-link *<1-3>* **message-digest-key** *<1-255>*

Sets MD5 key ID for each virtual link. The default setting is none.

Command mode: Router OSPF

area-virtual-link *<1-3>* **enable**

Enables OSPF virtual link.

Command mode: Router OSPF

no area-virtual-link *<1-3>* **enable**

Disables OSPF virtual link.

Command mode: Router OSPF

no area-virtual-link *<1-3>*

Deletes OSPF virtual link.

Command mode: Router OSPF

show ip ospf area-virtual-link *<1-3>*

Displays the current OSPF virtual link settings.

Command mode: All except User EXEC

OSPF Host Entry Configuration

Table 213 OSPF Host Entry Configuration Commands

Command Syntax and Usage	
host <1-128> address <IP address>	
Configures the base IP address for the host entry.	
Command mode: Router OSPF	
host <1-128> area <0-2>	
Configures the area index of the host.	
Command mode: Router OSPF	
host <1-128> cost <1-65535>	
Configures the cost value of the host.	
Command mode: Router OSPF	
host <1-128> enable	
Enables OSPF host entry.	
Command mode: Router OSPF	
no host <1-128> enable	
Disables OSPF host entry.	
Command mode: Router OSPF	
no host <1-128>	
Deletes OSPF host entry.	
Command mode: Router OSPF	
show ip ospf host <1-128>	
Displays the current OSPF host entries.	
Command mode: All except User EXEC	

OSPF Route Redistribution Configuration.

Table 214 OSPF Route Redistribution Configuration Commands

Command Syntax and Usage

redistribute {**fixed**|**static**|**rip**|**ebgp**|**ibgp**} <*rmap ID (1-32)*>

Adds selected routing map to the rmap list.

This option adds a route map to the route redistribution list. The routes of the redistribution protocol matched by the route maps in the route redistribution list will be redistributed.

Command mode: Router OSPF

no redistribute {**fixed**|**static**|**rip**|**ebgp**|**ibgp**} <*rmap ID (1-32)*>

Removes the route map from the route redistribution list.

Removes routing maps from the rmap list.

Command mode: Router OSPF

[**no**] **redistribute** {**fixed**|**static**|**rip**|**ebgp**|**ibgp**} **export metric** <*1-16777214*> **metric-type** {**type1**|**type2**}

Exports the routes of this protocol as external OSPF AS-external LSAs in which the metric and metric type are specified. To remove a previous configuration and stop exporting the routes of the protocol, enter **none**.

Command mode: Router OSPF

show ip ospf redistribute

Displays the current route map settings.

Command mode: All except User EXEC

OSPF MD5 Key Configuration

Table 215 OSPF MD5 Key commands

Command Syntax and Usage	
message-digest-key <1-255> md5-key <1-16 characters>	
Sets the authentication key for this OSPF packet.	
Command mode: Router OSPF	
no message-digest-key <1-255>	
Deletes the authentication key for this OSPF packet.	
Command mode: Router OSPF	
show ip ospf message-digest-key <1-255>	
Displays the current MD5 key configuration.	
Command mode: All except User EXEC	

Border Gateway Protocol Configuration

Border Gateway Protocol (BGP) is an Internet protocol that enables routers on a network to share routing information with each other and advertise information about the segments of the IP address space they can access within their network with routers on external networks. BGP allows you to decide what is the “best” route for a packet to take from your network to a destination on another network, rather than simply setting a default route from your border router(s) to your upstream provider(s). You can configure BGP either within an autonomous system or between different autonomous systems. When run within an autonomous system, it's called internal BGP (iBGP). When run between different autonomous systems, it's called external BGP (eBGP). BGP is defined in RFC 1771.

BGP commands enable you to configure the switch to receive routes and to advertise static routes, fixed routes and virtual server IP addresses with other internal and external routers. In the current BLADEOS implementation, the 1/10Gb Uplink ESM 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 216 Border Gateway Protocol Commands

Command Syntax and Usage

router bgp

Enter Router BGP configuration mode.

Command mode: Global configuration

neighbor <1-16>

Configures each BGP *peer*. Each border router, within an autonomous system, exchanges routing information with routers on other external networks.

Command mode: Router BGP

To view command options, see [page 352](#).

as <0-65535>

Set Autonomous System number.

Command mode: Router BGP

Table 216 Border Gateway Protocol Commands

Command Syntax and Usage

local-preference <0-4294967294>

Sets the local preference. The path with the higher value is preferred.

When multiple peers advertise the same route, use the route with the shortest AS path as the preferred route if you are using eBGP, or use the local preference if you are using iBGP.

Command mode: Router BGP

enable

Globally turns BGP on.

Command mode: Router BGP

no enable

Globally turns BGP off.

Command mode: Router BGP

show ip bgp

Displays the current BGP configuration.

Command mode: All except User EXEC

BGP Peer Configuration

These commands are used to configure BGP peers, which are border routers that exchange routing information with routers on internal and external networks. The peer option is disabled by default.

Table 217 BGP Peer Configuration Commands

Command Syntax and Usage

neighbor <1-16> **remote-address** <IP address>

Defines the IP address for the specified peer (border router), using dotted decimal notation. The default address is 0.0.0.0.

Command mode: Router BGP

neighbor <1-16> **remote-as** <1-65535>

Sets the remote autonomous system number for the specified peer.

Command mode: Router BGP

Table 217 BGP Peer Configuration Commands**Command Syntax and Usage**

neighbor <1-16> **timers hold-time** <0, 3-65535>

Sets the period of time, in seconds, that will elapse before the peer session is torn down because the switch hasn't received a "keep alive" message from the peer. The default value is 180 seconds.

Command mode: Router BGP

neighbor <1-16> **timers keep-alive** <0, 1-21845>

Sets the keep-alive time for the specified peer, in seconds. The default value is 60 seconds.

Command mode: Router BGP

neighbor <1-16> **advertisement-interval** <1-65535>

Sets time, in seconds, between advertisements. The default value is 60 seconds.

Command mode: Router BGP

neighbor <1-16> **retry-interval** <1-65535>

Sets connection retry interval, in seconds. The default value is 120 seconds.

Command mode: Router BGP

neighbor <1-16> **route-origination-interval** <1-65535>

Sets the minimum time between route originations, in seconds. The default value is 15 seconds.

Command mode: Router BGP

neighbor <1-16> **time-to-live** <1-255>

Time-to-live (TTL) is a value in an IP packet that tells a network router whether or not the packet has been in the network too long and should be discarded. TTL specifies a certain time span in seconds that, when exhausted, would cause the packet to be discarded. The TTL is determined by the number of router hops the packet is allowed before it must be discarded.

This command specifies the number of router hops that the IP packet can make. This value is used to restrict the number of "hops" the advertisement makes. It is also used to support multi-hops, which allow BGP peers to talk across a routed network. The default number is set at 1.

Note: The TTL value is significant only to eBGP peers, for iBGP peers the TTL value in the IP packets is always 255 (regardless of the configured value).

Command mode: Router BGP

Table 217 BGP Peer Configuration Commands**Command Syntax and Usage**

neighbor <1-16> **route-map in** <1-32>

Adds route map into in-route map list.

Command mode: Router BGP

neighbor <1-16> **route-map out** <1-32>

Adds route map into out-route map list.

Command mode: Router BGP

no neighbor <1-16> **route-map in** <1-32>

Removes route map from in-route map list.

Command mode: Router BGP

no neighbor <1-16> **route-map out** <1-32>

Removes route map from out-route map list.

Command mode: Router BGP

no neighbor <1-16> **shutdown**

Enables this peer configuration.

Command mode: Router BGP

neighbor <1-16> **shutdown**

Disables this peer configuration.

Command mode: Router BGP

no neighbor <1-16>

Deletes this peer configuration.

Command mode: Router BGP

show ip bgp neighbor [<1-16>]

Displays the current BGP peer configuration.

Command mode: All except User EXEC

BGP Redistribution Configuration

Table 218 BGP Redistribution Configuration Commands

Command Syntax and Usage

[no] neighbor <1-16> redistribute default-metric <1-4294967294>

Sets default metric of advertised routes.

Command mode: Router BGP

**[no] neighbor <1-16> redistribute default-action
{import|originate|redistribute}**

Sets default route action.

Defaults routes can be configured as import, originate, redistribute, or none.

None: No routes are configured

Import: Import these routes.

Originate: The switch sends a default route to peers if it does not have any default routes in its routing table.

Redistribute: Default routes are either configured through default gateway or learned through other protocols and redistributed to peer. If the routes are learned from default gateway configuration, you have to enable static routes since the routes from default gateway are static routes. Similarly, if the routes are learned from a certain routing protocol, you have to enable that protocol.

Command mode: Router BGP

[no] neighbor <1-16> redistribute rip

Enables or disables advertising RIP routes.

Command mode: Router BGP

[no] neighbor <1-16> redistribute ospf

Enables or disables advertising OSPF routes.

Command mode: Router BGP

[no] neighbor <1-16> redistribute fixed

Enables or disables advertising fixed routes.

Command mode: Router BGP

Table 218 BGP Redistribution Configuration Commands

Command Syntax and Usage

[no] neighbor <1-16> redistribute static

Enables or disables advertising static routes.

Command mode: Router BGP

show ip bgp neighbor <1-16> redistribute

Displays current redistribution configuration.

Command mode: All except User EXEC

BGP Aggregation Configuration

These commands enable you to configure BGP aggregation to specify the routes/range of IP destinations a peer router accepts from other peers. All matched routes are aggregated to one route, to reduce the size of the routing table. By default, the first aggregation number is enabled and the rest are disabled.

Table 219 BGP Aggregation Configuration Commands

Command Syntax and Usage

aggregate-address <1-16> <IP address> <IP netmask>

Defines the starting subnet IP address for this aggregation, using dotted decimal notation. The default address is 0.0.0.0.

Command mode: Router BGP

aggregate-address <1-16> enable

Enables this BGP aggregation.

Command mode: Router BGP

no aggregate-address <1-16> enable

Disables this BGP aggregation.

Command mode: Router BGP

Table 219 BGP Aggregation Configuration Commands

Command Syntax and Usage

no aggregate-address <1-16>

Deletes this BGP aggregation.

Command mode: Router BGP

show ip bgp aggregate-address [<1-16>]

Displays the current BGP aggregation configuration.

Command mode: All except User EXEC

IGMP Configuration

Table 220 describes the commands used to configure basic IGMP parameters.

Table 220 IGMP Configuration Commands

Command Syntax and Usage

[no] ip igmp aggregate

Enables or disables IGMP Membership Report aggregation.

Command mode: Global configuration

ip igmp enable

Globally turns IGMP on.

Command mode: Global configuration

no ip igmp enable

Globally turns IGMP off.

Command mode: Global configuration

show ip igmp

Displays the current IGMP configuration parameters.

Command mode: All

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 221 describes the commands used to configure IGMP Snooping.

Table 221 IGMP Snooping Configuration Commands

Command Syntax and Usage	
<code>ip igmp snoop mrouter-timeout <1-600></code>	<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>Command mode: Global configuration</p>
<code>ip igmp snoop source-ip <IP address></code>	<p>Configures the source IP address used as a proxy for IGMP Group Specific Queries.</p> <p>Command mode: Global configuration</p>
<code>ip igmp snoop vlan <VLAN number></code>	<p>Adds the selected VLAN(s) to IGMP Snooping.</p> <p>Command mode: Global configuration</p>
<code>no ip igmp snoop vlan <VLAN number></code>	<p>Removes the selected VLAN(s) from IGMP Snooping.</p> <p>Command mode: Global configuration</p>
<code>no ip igmp snoop vlan all</code>	<p>Removes all VLANs from IGMP Snooping.</p> <p>Command mode: Global configuration</p>
<code>ip igmp snoop enable</code>	<p>Enables IGMP Snooping.</p> <p>Command mode: Global configuration</p>

Table 221 IGMP Snooping Configuration Commands

Command Syntax and Usage

no ip igmp snoop enable

Disables IGMP Snooping.

Command mode: Global configuration

show ip igmp snoop

Displays the current IGMP Snooping parameters.

Command mode: All

IGMPv3 Configuration

[Table 225](#) describes the commands used to configure IGMP version 3.

Table 222 IGMP version 3 Configuration Commands

Command Syntax and Usage

ip igmp snoop igmpv3 sources <1-64>

Configures the maximum number of IGMP multicast sources to snoop from within the group record. Use this command to limit the number of IGMP sources to provide more refined control. The default value is 8.

Command mode: Global configuration

[no] ip igmp snoop igmpv3 v1v2

Enables or disables snooping on IGMP version 1 and version 2 reports. When disabled, the switch drops IGMPv1 and IGMPv2 reports. The default value is **enabled**.

Command mode: Global configuration

[no] ip igmp snoop igmpv3 exclude

Enables or disables snooping on IGMPv3 Exclude Reports. When disabled, the switch ignores Exclude Reports. The default value is **enabled**.

Command mode: Global configuration

ip igmp snoop igmpv3 enable

Enables IGMP version 3. The default value is **enabled**.

Command mode: Global configuration

Table 222 IGMP version 3 Configuration Commands

Command Syntax and Usage
no ip igmp snoop igmpv3 enable Disables IGMP version 3. Command mode: Global configuration
show ip igmp snoop igmpv3 Displays the current IGMP v3 Snooping configuration. Command mode: All except User EXEC

IGMP Relay Configuration

When you configure IGMP Relay, also configure the IGMP Relay multicast routers.

Table 225 describes the commands used to configure IGMP Relay.

Table 223 IGMP Relay Configuration Commands

Command Syntax and Usage
ip igmp relay vlan <VLAN number> Adds the VLAN to the list of IGMP Relay VLANs. Command mode: Global configuration
no ip igmp relay vlan <VLAN number> Removes the VLAN from the list of IGMP Relay VLANs. Command mode: Global configuration
ip igmp relay report <0-150> Configures the interval between unsolicited Join reports sent by the switch, in seconds. The default value is 10. Command mode: Global configuration
ip igmp relay enable Enables IGMP Relay. Command mode: Global configuration

Table 223 IGMP Relay Configuration Commands

Command Syntax and Usage

no ip igmp relay enable

Disables IGMP Relay.

Command mode: Global configuration

show ip igmp relay

Displays the current IGMP Relay configuration.

Command mode: All except User EXEC

IGMP Relay Multicast Router Configuration

Table 225 describes the commands used to configure multicast routers for IGMP Relay.

Table 224 IGMP Relay Mrouter Configuration Commands

Command Syntax and Usage

ip igmp relay mrouter <1-2> address <IP address>

Configures the IP address of the IGMP multicast router used for IGMP Relay.

Command mode: Global configuration

ip igmp relay mrouter <1-2> interval <1-60>

Configures the time interval between ping attempts to the upstream Mrouters, in seconds. The default value is 2.

Command mode: Global configuration

ip igmp relay mrouter <1-2> retry <1-120>

Configures the number of failed ping attempts required before the switch declares this Mrouter is down. The default value is 4.

Command mode: Global configuration

ip igmp relay mrouter <1-2> attempt <1-128>

Configures the number of successful ping attempts required before the switch declares this Mrouter is up. The default value is 5.

Command mode: Global configuration

Table 224 IGMP Relay Mrouter Configuration Commands

Command Syntax and Usage	
ip igmp relay mrouter <1-2> version <1-2>	
Configures the IGMP version (1 or 2) of the multicast router.	
Command mode: Global configuration	
ip igmp relay mrouter <1-2> enable	
Enables the multicast router.	
Command mode: Global configuration	
no ip igmp relay mrouter <1-2> enable	
Disables the multicast router.	
Command mode: Global configuration	
no ip igmp relay mrouter <1-2>	
Deletes the multicast router from IGMP Relay.	
Command mode: Global configuration	

IGMP Static Multicast Router Configuration

Table 225 describes the commands used to configure a static multicast router.

Note – When static Mrouters are used, the switch continues learning dynamic Mrouters via IGMP snooping. However, dynamic Mrouters may not replace static Mrouters. If a dynamic Mrouter has the same port and VLAN combination as a static Mrouter, the dynamic Mrouter is not learned.

Table 225 IGMP Static Multicast Router Configuration Commands

Command Syntax and Usage	
ip igmp mrouter <port alias or number> <VLAN number> <version (1-3)>	
Selects a port/VLAN combination on which the static multicast router is connected, and configures the IGMP version (1 or 2) of the multicast router.	
Command mode: Global configuration	
no ip igmp mrouter <port alias or number> <VLAN number> <version (1-3)>	
Removes a static multicast router from the selected port/VLAN combination.	
Command mode: Global configuration	

Table 225 IGMP Static Multicast Router Configuration Commands

Command Syntax and Usage

clear ip igmp mrouter

Clears all static multicast routers from the switch.

Command mode: Global configuration

show ip igmp mrouter

Displays the current IGMP Static Multicast Router parameters.

Command mode: All except User EXEC

IGMP Filtering Configuration

[Table 226](#) describes the commands used to configure an IGMP filter.

Table 226 IGMP Filtering Configuration Commands

Command Syntax and Usage

ip igmp profile <1-16>

Configures the IGMP filter.

Command mode: Global configuration

To view command options, see [page 364](#).

ip igmp filtering

Enables IGMP filtering globally.

Command mode: Global configuration

no ip igmp filtering

Disables IGMP filtering globally.

Command mode: Global configuration

show ip igmp filtering

Displays the current IGMP Filtering parameters.

Command mode: All

IGMP Filter Definition

Table 227 describes the commands used to define an IGMP filter.

Table 227 IGMP Filter Definition Commands

Command Syntax and Usage	
ip igmp profile <1-16> range <IP address 1> <IP address 2>	
Configures the range of IP multicast addresses for this filter.	
Command mode: Global configuration	
ip igmp profile <1-16> action {allow deny}	
Allows or denies multicast traffic for the IP multicast addresses specified. The default action is deny.	
Command mode: Global configuration	
ip igmp profile <1-16> enable	
Enables this IGMP filter.	
Command mode: Global configuration	
no ip igmp profile <1-16> enable	
Disables this IGMP filter.	
Command mode: Global configuration	
no ip igmp profile <1-16>	
Deletes this filter's parameter definitions.	
Command mode: Global configuration	
show ip igmp profile <1-16>	
Displays the current IGMP filter.	
Command mode: All	

IGMP Filtering Port Configuration

Table 228 describes the commands used to configure a port for IGMP filtering.

Table 228 IGMP Filter Port Configuration Commands

Command Syntax and Usage

[no] ip igmp filtering

Enables or disables IGMP filtering on this port.

Command mode: Interface port

ip igmp profile <1-16>

Adds an IGMP filter to this port.

Command mode: Interface port

no ip igmp profile <1-16>

Removes an IGMP filter from this port.

Command mode: Interface port

show interface port <port alias or number> igmp-filtering

Displays the current IGMP filter parameters for this port.

Command mode: All except User EXEC

IGMP Advanced Configuration

Table 225 describes the commands used to configure advanced IGMP parameters.

Table 229 IGMP Advanced Configuration Commands

Command Syntax and Usage

ip igmp query-interval <1-600>

Sets the IGMP router query interval, in seconds. The default value is 125.

Command mode: Global configuration

ip igmp robust <2-10>

Configures the IGMP Robustness variable, which allows you to tune the switch for expected packet loss on the subnet. If the subnet is expected to be lossy (high rate of packet loss), increase the value. The default value is 2.

Command mode: Global configuration

Table 229 IGMP Advanced Configuration Commands

Command Syntax and Usage

ip igmp timeout <1-255>

Configures the timeout value for IGMP Membership Reports (host). Once the timeout value is reached, the switch removes the host from its IGMP table, if the conditions are met. The range is from 1 to 255 seconds. The default is 10 seconds.

Command mode: Global configuration

[no] ip igmp fastleave <VLAN number>

Enables or disables Fastleave processing. Fastleave allows the switch to immediately remove a port from the IGMP port list, if the host sends a Leave message, and the proper conditions are met. This command is disabled by default.

Command mode: Global configuration

[no] ip igmp flood

Configures the switch to flood unregistered IP multicast traffic to all ports. The default setting is **enabled**.

Note: If none of the IGMP hosts reside on the VLAN of the streaming server for a IPMC group, you must disable IGMP flooding to ensure that multicast data is forwarded across the VLANs for that IPMC group.

Command mode: Global configuration

[no] ip igmp cpu

Configures the switch to forward unregistered IP multicast traffic to the MP, which adds an entry in the IPMC table, as follows:

- ☐ If no Mrouter is present, drop subsequent packets with same IPMC.
- ☐ If an Mrouter is present, forward subsequent packets to the Mrouter(s) on the ingress VLAN.

The default setting is **enabled**.

Note: If both **flood** and **cpu** are disabled, then the switch drops all unregistered IPMC traffic.

Command mode: Global configuration

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 230 Domain Name Service Commands

Command Syntax and Usage

[no] ip dns primary-server *<IP address>*

You are prompted to set the IPv4 address for your primary DNS server, using dotted decimal notation.

Command mode: Global configuration

[no] ip dns secondary-server *<IP address>*

You are prompted to set the IPv4 address for your secondary DNS server, using dotted decimal notation. If the primary DNS server fails, the configured secondary will be used instead.

Command mode: Global configuration

[no] ip dns ipv6 primary-server *<IP address>*

You are prompted to set the IPv6 address for your primary DNS server, using hexadecimal format with colons.

Command mode: Global configuration

[no] ip dns ipv6 secondary-server *<IP address>*

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.

Command mode: Global configuration

ip dns ipv6 request-version {`ipv4`|`ipv6`}

Sets the protocol used for the first request to the DNS server, as follows:

- ☐ IPv4
- ☐ IPv6

Command mode: Global configuration

Table 230 Domain Name Service Commands

Command Syntax and Usage

[no] ip dns domain-name <string>

Sets the default domain name used by the switch.
For example: mycompany.com

Command mode: Global configuration

show ip dns

Displays the current Domain Name System settings.

Command mode: All except User EXEC

Bootstrap Protocol Relay Configuration

The Bootstrap Protocol (BOOTP) Relay commands are used to allow hosts to obtain their configurations from a Dynamic Host Configuration Protocol (DHCP) server. The BOOTP configuration enables the switch to forward a client request for an IP address to two DHCP/BOOTP servers with IP addresses that have been configured on the GbESM.

BOOTP relay is turned off by default.

Table 231 Bootstrap Protocol Relay Configuration Commands

Command Syntax and Usage

[no] ip bootp-relay {server1|server2} <IP address>

Sets the IP address of the first or second BOOTP server.

IPv4: To set an IPv4 address, use dotted decimal notation.

IPv6: To set an IPv6 address, use hexadecimal format with colons.

Command mode: Global configuration

ip bootp-relay enable

Globally turns on BOOTP relay.

Command mode: Global configuration

no ip bootp-relay enable

Globally turns off BOOTP relay.

Command mode: Global configuration

VRRP Configuration

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

By default, VRRP is disabled. BLADEOS has extended VRRP to include virtual servers as well, allowing for full active/active redundancy between switches. For more information on VRRP, see the “High Availability” chapter in the *BLADEOS 6.3 Application Guide*.

Table 232 Virtual Router Redundancy Protocol Commands

Command Syntax and Usage
router vrrp Enter Router VRRP configuration mode. Command mode: Global configuration
[no] hot-standby Enables or disables hot standby processing, in which two or more switches provide redundancy for each other. By default, this option is disabled. Command mode: Router VRRP
enable Globally enables VRRP on this switch. Command mode: Router VRRP
no enable Globally disables VRRP on this switch. Command mode: Router VRRP
show ip vrrp Displays the current VRRP parameters. Command mode: All

Virtual Router Configuration

These commands are used for configuring virtual routers for this switch. A virtual router is defined by its virtual router ID and an IP address. On each VRRP-capable routing device participating in redundancy for this virtual router, a virtual router will be configured to share the same virtual router ID and IP address.

Virtual routers are disabled by default.

Table 233 VRRP Virtual Router Configuration Commands

Command Syntax and Usage
virtual-router <1-128> virtual-router-id <1-255> Defines the virtual router ID (VRID). This is used in conjunction with the <code>[no] virtual-router <VRID> address <IP address></code> command below to define a virtual router on this switch. To create a pool of VRRP-enabled routing devices which can provide redundancy to each other, each participating VRRP device must be configured with the same virtual router. The VRID for standard virtual routers (where the virtual router IP address is not the same as any virtual server) can be any integer between 1 and 255. The default value is 1. All VRID values must be unique within the VLAN to which the virtual router's IP interface belongs. Command mode: Router VRRP
[no] virtual-router <1-128> address <IP address> Defines the IP address for this virtual router using dotted decimal notation. This is used in conjunction with the VRID (above) to configure the same virtual router on each participating VRRP device. The default address is 0.0.0.0. Command mode: Router VRRP
virtual-router <1-128> interface <interface number> Selects a switch IP interface. If the IP interface has the same IP address as the <code>addr</code> option above, this switch is considered the "owner" of the defined virtual router. An owner has a special priority of 255 (highest) and will always assume the role of master router, even if it must pre-empt another virtual router which has assumed master routing authority. This pre-emption occurs even if the <code>preem</code> option below is disabled. The default value is 1. Command mode: Router VRRP

Table 233 VRRP Virtual Router Configuration Commands

Command Syntax and Usage

virtual-router <1-128> **priority** <1-254>

Defines the election priority bias for this virtual server. The priority value can be any integer between 1 and 254. The default value is 100.

During the master router election process, the routing device with the highest virtual router priority number wins. If there is a tie, the device with the highest IP interface address wins. If this virtual router's IP address is the same as the one used by the IP interface, the priority for this virtual router will automatically be set to 255 (highest).

When priority tracking is used, this base priority value can be modified according to a number of performance and operational criteria.

Command mode: Router VRRP

virtual-router <1-128> **timers advertise** <1-255>

Defines the time interval between VRRP master advertisements. This can be any integer between 1 and 255 seconds. The default value is 1.

Command mode: Router VRRP

[no] **virtual-router** <1-128> **preemption**

Enables or disables master preemption. When enabled, if this virtual router is in backup mode but has a higher priority than the current master, this virtual router will preempt the lower priority master and assume control. Note that even when `preemption` is disabled, this virtual router will always pre-empt any other master if this switch is the owner (the IP interface address and virtual router `addr` are the same). By default, this option is enabled.

Command mode: Router VRRP

virtual-router <1-128> **enable**

Enables this virtual router.

Command mode: Router VRRP

no **virtual-router** <1-128> **enable**

Disables this virtual router.

Command mode: Router VRRP

Table 233 VRRP Virtual Router Configuration Commands

Command Syntax and Usage

no virtual-router <I-I28>

Deletes this virtual router from the switch configuration.

Command mode: Router VRRP

show ip vrrp virtual-router <I-I28>

Displays the current configuration information for this virtual router.

Command mode: All except User EXEC

Virtual Router Priority Tracking Configuration

These commands are used for modifying the priority system used when electing the master router from a pool of virtual routers. Various tracking criteria can be used to bias the election results. Each time one of the tracking criteria is met, the priority level for the virtual router is increased by an amount defined through the VRRP Tracking commands.

Criteria are tracked dynamically, continuously updating virtual router priority levels when enabled. If the virtual router preemption option is enabled, this virtual router can assume master routing authority when its priority level rises above that of the current master.

Some tracking criteria apply to standard virtual routers, otherwise called “virtual interface routers.” A virtual *server* router is defined as any virtual router whose IP address is the same as any configured virtual server IP address.

Table 234 VRRP Priority Tracking Configuration Commands

Command Syntax and Usage

[no] virtual-router <1-128> track virtual-routers

When enabled, the priority for this virtual router will be increased for each virtual router in master mode on this switch. This is useful for making sure that traffic for any particular client/server pairing are handled by the same switch, increasing routing and load balancing efficiency. This command is disabled by default.

Command mode: Router VRRP

[no] virtual-router <1-128> track interfaces

When enabled, the priority for this virtual router will be increased for each other IP interface active on this switch. An IP interface is considered active when there is at least one active port on the same VLAN. This helps elect the virtual routers with the most available routes as the master. This command is disabled by default.

Command mode: Router VRRP

[no] virtual-router <1-128> track ports

When enabled, the priority for this virtual router will be increased for each active port on the same VLAN. A port is considered “active” if it has a link and is forwarding traffic. This helps elect the virtual routers with the most available ports as the master. This command is disabled by default.

Command mode: Router VRRP

show ip vrrp virtual-router <1-128> track

Displays the current configuration for priority tracking for this virtual router.

Command mode: All except User EXEC

Virtual Router Group Configuration

Virtual Router Group commands are used for associating all virtual routers into a single logical virtual router, which forces all virtual routers on the GbESM 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 GbESMs in a hot-standby failover configuration, where only one switch is active at any time.

Table 235 VRRP Virtual Router Group Configuration Commands

Command Syntax and Usage

group virtual-router-id <1-255>

Defines the virtual router ID (VRID).

The VRID for standard virtual routers (where the virtual router IP address is not the same as any virtual server) can be any integer between 1 and 255. All VRID values must be unique within the VLAN to which the virtual router’s IP interface (see *interface* below) belongs. The default virtual router ID is 1.

Command mode: Router VRRP

group interface <interface number>

Selects a switch IP interface. The default switch IP interface number is 1.

Command mode: Router VRRP

group priority <1-254>

Defines the election priority bias for this virtual router group. This can be any integer between 1 and 254. The default value is 100.

During the master router election process, the routing device with the highest virtual router priority number wins.

Each virtual router group is treated as one entity regardless of how many virtual routers are in the group. When the switch tracks the virtual router group, it measures the resources contained in the group (such as interfaces, VLAN ports, real servers). The priority is updated as a group. Every virtual router in the group has the same priority.

The *owner* parameter does not apply to the virtual router group. The group itself cannot be an owner and therefore the priority is 1-254.

Command mode: Router VRRP

Table 235 VRRP Virtual Router Group Configuration Commands

Command Syntax and Usage

group advertisement <1-255>

Defines the time interval between VRRP master advertisements. This can be any integer between 1 and 255 seconds. The default is 1.

Command mode: Router VRRP

[no] group preemption

Enables or disables master pre-emption. When enabled, if the virtual router group is in backup mode but has a higher priority than the current master, this virtual router will pre-empt the lower priority master and assume control. Note that even when `preemption` is disabled, this virtual router will always pre-empt any other master if this switch is the owner (the IP interface address and virtual router address are the same). By default, this option is enabled.

Command mode: Router VRRP

group enable

Enables the virtual router group.

Command mode: Router VRRP

no group enable

Disables the virtual router group.

Command mode: Router VRRP

no group

Deletes the virtual router group from the switch configuration.

Command mode: Router VRRP

show ip vrrp group

Displays the current configuration information for the virtual router group.

Command mode: All except User EXEC

Virtual Router Group Priority Tracking Configuration

Note – If *Virtual Router Group Tracking* is enabled, then the tracking option will be available only under *group* option. The tracking setting for the other individual virtual routers will be ignored.

Table 236 Virtual Router Group Priority Tracking Configuration Commands

Command Syntax and Usage

[no] group track interfaces

When enabled, the priority for this virtual router will be increased for each other IP interface active on this switch. An IP interface is considered active when there is at least one active port on the same VLAN. This helps elect the virtual routers with the most available routes as the master. This command is disabled by default.

Command mode: Router VRRP

[no] group track ports

When enabled, the priority for this virtual router will be increased for each active port on the same VLAN. A port is considered “active” if it has a link and is forwarding traffic. This helps elect the virtual routers with the most available ports as the master. This command is disabled by default.

Command mode: Router VRRP

show ip vrrp group track

Displays the current configuration for priority tracking for this virtual router.

Command mode: All except User EXEC

VRRP Interface Configuration

Note – The *interface* represents the IP interface on which authentication parameters must be configured.

These commands are used for configuring VRRP authentication parameters for the IP interfaces used with the virtual routers.

Table 237 VRRP Interface Commands

Command Syntax and Usage

interface <interface number> **authentication** {**password**|**none**}

Defines the type of authentication that will be used: **none** (no authentication) or **password** (password authentication).

Command mode: Router VRRP

[**no**] **interface** <interface number> **password** <password>

Defines a plain text password up to eight characters long. This password will be added to each VRRP packet transmitted by this interface when password authentication is chosen (see **interface authentication** above).

Command mode: Router VRRP

no interface <interface number>

Clears the authentication configuration parameters for this IP interface. The IP interface itself is not deleted.

Command mode: Router VRRP

show ip vrrp interface <interface number>

Displays the current configuration for this IP interface's authentication parameters.

Command mode: All except User EXEC

VRRP Tracking Configuration

These commands are used for setting weights for the various criteria used to modify priority levels during the master router election process. Each time one of the tracking criteria is met (see “VRRP Virtual Router Priority Tracking Commands” on [page 372](#)), the priority level for the virtual router is increased by a defined amount.

Table 238 VRRP Tracking Configuration Commands

Command Syntax and Usage
tracking-priority-increment virtual-routers <0-254> Defines the priority increment value (0 through 254) for virtual routers in master mode detected on this switch. The default value is 2. Command mode: Router VRRP
tracking-priority-increment interfaces <0-254> Defines the priority increment value for active IP interfaces detected on this switch. The default value is 2. Command mode: Router VRRP
tracking-priority-increment ports <0-254> Defines the priority increment value for active ports on the virtual router’s VLAN. The default value is 2. Command mode: Router VRRP
show ip vrrp tracking-priority-increment Displays the current configuration of priority tracking increment values. Command mode: All except User EXEC
Note – These priority tracking options only define increment values. These options do not affect the VRRP master router election process until options under the VRRP Virtual Router Priority Tracking Commands (see page 372) are enabled.

IPv6 Default Gateway Configuration

The switch supports IPv6 default gateways.

- Gateway 1 is used for data traffic.
- Gateway 132 is reserved for management.

Table 239 describes the IPv6 Default Gateway Configuration commands.

Table 239 IPv6 Default Gateway Configuration commands

Command Syntax and Usage	
ip gateway6 {<gateway number>} address <IPv6 address>	
Configures the IPv6 address of the default gateway, in hexadecimal format with colons (such as 3001:0:0:0:0:abcd:12).	
Command mode: Global configuration	
[no] ip gateway6 {<gateway number>} enable	
Enables or disables the default gateway.	
Command mode: Global configuration	
no ip gateway6 {<gateway number>}	
Deletes the default gateway.	
Command mode: Global configuration	
show ipv6 gateway6 {<gateway number>}	
Displays the current IPv6 default gateway configuration.	
Command mode: All except User EXEC	

IPv6 Static Route Configuration

Table 240 describes the IPv6 static route configuration commands.

Table 240 IPv6 Static Route Configuration commands

Command Syntax and Usage
ip route6 <i><IPv6 address></i> <i><prefix length></i> <i><IPv6 gateway address></i> [<i><interface number></i>] Adds an IPv6 static route. Command mode: Global configuration
no ip route6 <i><IPv6 address></i> <i><prefix length></i> Removes the selected route. Command mode: Global configuration
no ip route6 [destination-address <i><IPv6 address></i> gateway <i><default gateway address></i> interface <i><interface number></i> all] Clears the selected IPv6 static routes. Command mode: Global configuration

IPv6 Neighbor Discovery Cache Configuration

Table 241 describes the IPv6 Neighbor Discovery cache configuration commands.

Table 241 IPv6 Neighbor Discovery Cache Configuration commands

Command Syntax and Usage

ip neighbors *<IPv6 address>* *<MAC address>* **vlan** *<VLAN number>*
port *<port number or alias>*

Adds a static entry to the Neighbor Discovery cache table.

Command mode: Global configuration

no ip neighbors {*<IPv6 address>* | **all**}

Deletes the selected entry from the static Neighbor Discovery cache table.

Command mode: Global configuration

no ip neighbors [**all if**|**all interface port**|**all vlan**|**all**]

Clears the selected static entries in the Neighbor Discovery cache table.

Command mode: Global configuration

Open Shortest Path First Version 3 Configuration

Table 242 OSPFv3 Configuration Commands

Command Syntax and Usage

[no] ipv6 router ospf

Enter OSPFv3 configuration mode. Enables or disables OSPFv3 routing protocol.

Command mode: Global configuration

abr-type [standard|cisco|ibm]

Configures the Area Border Router (ABR) type, as follows:

- ☐ Standard
- ☐ Cisco
- ☐ IBM

The default setting is `standard`.

Command mode: Router OSPF3

as-external lsdb-limit *<LSDB limit (0-2147483647, -1 for no limit)>*

Sets the link state database limit.

Command mode: Router OSPF3

exit-overflow-interval *<0-4294967295>*

Configures the number of seconds that a router takes to exit Overflow State. The default value is 0 (zero).

Command mode: Router OSPF3

reference-bandwidth *<0-4294967295>*

Configures the reference bandwidth, in kilobits per second, used to calculate the default interface metric. The default value is 100,000.

Command mode: Router OSPF3

timers spf {*<SPF delay (0-65535)>*} {*<SPF hold time (0-65535)>*}

Configures the number of seconds that SPF calculation is delayed after a topology change message is received. The default value is 5.

Configures the number of seconds between SPF calculations. The default value is 10.

Command mode: Router OSPF3

Table 242 OSPFv3 Configuration Commands

Command Syntax and Usage

router-id <IPv4 address>

Defines the router ID.

Command mode: Router OSPF3

[no] nssaAsbrDfRtTrans

Enables or disables setting of the P-bit in the default Type 7 LSA generated by an NSSA internal ASBR. The default setting is disabled.

Command mode: Router OSPF3

enable

Enables OSPFv3 on the switch.

Command mode: Router OSPF3

no enable

Disables OSPFv3 on the switch.

Command mode: Router OSPF3

show ipv6 ospf

Displays the current OSPF configuration settings.

Command mode: All

OSPFv3 Area Index Configuration

Table 243 OSPFv3 Area Index Configuration Options

Command Syntax and Usage

area *<area index>* **area-id** *<IP address>*

Defines the IP address of the OSPFv3 area number.

Command mode: Router OSPF3

area *<area index>* **type** {**transit**|**stub**|**nssa**} {**no-summary**}

Defines the type of area. For example, when a virtual link has to be established with the backbone, the area type must be defined as transit.

Transit area: allows area summary information to be exchanged between routing devices. Any area that is not a stub area or NSSA is considered to be transit area.

Stub area: is an area where external routing information is not distributed. Typically, a stub area is connected to only one other area.

NSSA: Not-So-Stubby Area (NSSA) is similar to stub area with additional capabilities. For example, routes originating from within the NSSA can be propagated to adjacent transit and backbone areas. External routes from outside the Autonomous System (AS) can be advertised within the NSSA but are not distributed into other areas.

Enables or disables the no-summary option. When enabled, the area-border router neither originates nor propagates Inter-Area-Prefix LSAs into stub/NSSA areas. Instead it generates a default Inter-Area-Prefix LSA.

The default setting is `disabled`.

Command mode: Router OSPF3

area *<area index>* **default-metric** *<metric value (1-16777215)>*

Configures the cost for the default summary route in a stub area or NSSA.

Command mode: Router OSPF3

area *<area index>* **default-metric type** *<1-3>*

Configures the default metric type applied to the route.

This command applies only to area type of Stub/NSSA.

Command mode: Router OSPF3

Table 243 OSPFv3 Area Index Configuration Options**Command Syntax and Usage**

area *<area index>* **stability-interval** *<1-255>*

Configures the stability interval for an NSSA, in seconds. When the interval expires, an elected translator determines that its services are no longer required. The default value is 40.

Command mode: Router OSPF3

area *<area index>* **translation-role** **always|candidate**

Configures the translation role for an NSSA area, as follows:

- ☐ Always: Type 7 LSAs are always translated into Type 5 LSAs.
- ☐ Candidate: An NSSA border router participates in the translator election process.

The default setting is *candidate*.

Command mode: Router OSPF3

area *<area index>* **enable**

Enables the OSPF area.

Command mode: Router OSPF3

area *<area index>* **no enable**

Disables the OSPF area.

Command mode: Router OSPF3

no area *<area index>*

Deletes the OSPF area.

Command mode: Router OSPF3

show ipv6 ospf areas

Displays the current OSPFv3 area configuration.

Command mode: All

OSPFv3 Summary Range Configuration

Table 244 OSPFv3 Summary Range Configuration Options

Command Syntax and Usage

area-range <1-16> **address** <IPv6 address> <prefix length (1-128)>

Configures the base IPv6 address and subnet prefix length for the range.

Command mode: Router OSPF3

area-range <1-16> **area** <area index (0-2)>

Configures the area index used by the switch.

Command mode: Router OSPF3

area-range <1-16> **lsa-type** **summary|Type7**

Configures the LSA type, as follows:

- ☐ Summary LSA
- ☐ Type7 LSA

Command mode: Router OSPF3

area-range <1-16> **tag** <0-4294967295>

Configures the route tag.

Command mode: Router OSPF3

[no] area-range <1-16> **hide**

Hides the OSPFv3 summary range.

Command mode: Router OSPF3

area-range <1-16> **enable**

Enables the OSPFv3 summary range.

Command mode: Router OSPF3

area-range <1-16> **no enable**

Disables the OSPFv3 summary range.

Command mode: Router OSPF3

Table 244 OSPFv3 Summary Range Configuration Options**Command Syntax and Usage****no area-range** <1-16>

Deletes the OSPFv3 summary range.

Command mode: Router OSPF3**show ipv6 ospf area-range**

Displays the current OSPFv3 summary range.

Command mode: All**OSPFv3 AS-External Range Configuration****Table 245** OSPFv3 AS_External Range Configuration Options**Command Syntax and Usage****summary-prefix** <1-16> **address** <IPv6 address> <IPv6 prefix length (1-128)>

Configures the base IPv6 address and the subnet prefix length for the range.

Command mode: Router OSPF3**summary-prefix** <1-16> **area** <area index (0-2)>

Configures the area index used by the switch.

Command mode: Router OSPF3**summary-prefix** <1-16> **aggregation-effect** {allowAll|denyAll|advertise|not-advertise}

Configures the aggregation effect, as follows:

- ❑ **allowAll**: If the area ID is 0.0.0.0, aggregated Type-5 LSAs are generated. Aggregated Type-7 LSAs are generated in all the attached NSSAs for the range.
- ❑ **denyAll**: Type-5 and Type-7 LSAs are not generated.
- ❑ **advertise**: If the area ID is 0.0.0.0, aggregated Type-5 LSAs are generated. For other area IDs, aggregated Type-7 LSAs are generated in the NSSA area.
- ❑ **not-advertise**: If the area ID is 0.0.0.0, Type-5 LSAs are not generated, while all NSSA LSAs within the range are cleared and aggregated Type-7 LSAs are generated for all NSSAs. For other area IDs, aggregated Type-7 LSAs are not generated in the NSSA area.

Command mode: Router OSPF3

Table 245 OSPFv3 AS_External Range Configuration Options

Command Syntax and Usage

[no] summary-prefix <1-16> translation

When enabled, the P-bit is set in the generated Type-7 LSA. When disabled, the P-bit is cleared. The default setting is disabled.

Command mode: Router OSPF3

summary-prefix <1-16> enable

Enables the OSPFv3 AS-external range.

Command mode: Router OSPF3

summary-prefix <1-16> no enable

Disables the OSPFv3 AS-external range.

Command mode: Router OSPF3

no summary-prefix <1-16>

Deletes the OSPFv3 AS-external range.

Command mode: Router OSPF3

show ipv6 ospf summary-prefix <1-16>

Displays the current OSPFv3 AS-external range.

Command mode: All

OSPFv3 Interface Configuration

Table 246 OSPFv3 Interface Configuration Options

Command Syntax and Usage

interface ip <interface number>

Enter Interface IP mode, from Global Configuration mode.

Command mode: Global configuration

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

Configures the OSPFv3 area index.

Command mode: Interface IP

Table 246 OSPFv3 Interface Configuration Options**Command Syntax and Usage**

ipv6 ospf area *<area index (0-2)>* **instance** *<0-255>*

Configures the instance ID for the interface.

Command mode: Interface IP

[no] ipv6 ospf priority *<priority value (0-255)>*

Configures the priority value for the switch's OSPFv3 interface.

A priority value of 255 is the highest and 1 is the lowest. A priority value of 0 specifies that the interface cannot be used as Designated Router (DR).

Command mode: Interface IP

[no] ipv6 ospf cost *<1-65535>*

Configures the metric value for sending a packet on the interface.

Command mode: Interface IP

[no] ipv6 ospf hello-interval *<1-65535>*

Configures the indicated interval, in seconds, between the `hello` packets, that the router sends on the interface.

Command mode: Interface IP

[no] ipv6 ospf dead-interval *<1-65535>*

Configures the health parameters of a `hello` packet, in seconds, before declaring a silent router to be down.

Command mode: Interface IP

[no] ipv6 ospf transmit-delay *<1-1800>*

Configures the estimated time, in seconds, taken to transmit LS update packet over this interface.

Command mode: Interface IP

[no] ipv6 ospf retransmit-interval *<1-1800>*

Configures the interval in seconds, between LSA retransmissions for adjacencies belonging to interface.

Command mode: Interface IP

Table 246 OSPFv3 Interface Configuration Options

Command Syntax and Usage

[no] ipv6 ospf passive-interface

Enables or disables the `passive` setting on the interface. On a passive interface, OSPFv3 protocol packets are suppressed.

Command mode: Interface IP

ipv6 ospf enable

Enables OSPFv3 on the interface.

Command mode: Interface IP

ipv6 ospf no enable

Disables OSPFv3 on the interface.

Command mode: Interface IP

no ipv6 ospf

Deletes OSPFv3 from interface.

Command mode: Interface IP

show ipv6 ospf interface

Displays the current settings for OSPFv3 interface.

Command mode: Interface IP

OSPFv3 Virtual Link Configuration

Table 247 OSPFv3 Virtual Link Configuration Options

Command Syntax and Usage

area-virtual-link <1-3> area <area index (0-2)>

Configures the OSPF area index.

Command mode: Router OSPF3

area-virtual-link <1-3> hello-interval <1-65535>

Configures the indicated interval, in seconds, between the hello packets, that the router sends on the interface.

Command mode: Router OSPF3

Table 247 OSPFv3 Virtual Link Configuration Options**Command Syntax and Usage**

area-virtual-link *<1-3>* **dead-interval** *<1-65535>*

Configures the time period, in seconds, for which the router waits for hello packet from the neighbor before declaring this neighbor down.

Command mode: Router OSPF3

area-virtual-link *<1-3>* **transmit-delay** *<1-1800>*

Configures the estimated time, in seconds, taken to transmit LS update packet over this interface.

Command mode: Router OSPF3

area-virtual-link *<1-3>* **retransmit-interval** *<1-1800>*

Configures the interval, in seconds, between link-state advertisement (LSA) retransmissions for adjacencies belonging to the OSPFv3 virtual link interface. The default value is five seconds.

Command mode: Router OSPF3

area-virtual-link *<1-3>* **neighbor-router** *<NBR router ID (IP address)>*

Configures the router ID of the virtual neighbor. The default setting is 0.0.0.0

Command mode: Router OSPF3

area-virtual-link *<1-3>* **enable**

Enables OSPF virtual link.

Command mode: Router OSPF3

area-virtual-link *<1-3>* **no enable**

Disables OSPF virtual link.

Command mode: Router OSPF3

no area-virtual-link *<1-3>*

Deletes OSPF virtual link.

Command mode: Router OSPF3

show ipv6 ospf area-virtual-link

Displays the current OSPFv3 virtual link settings.

Command mode: All

OSPFv3 Host Entry Configuration

Table 248 OSPFv3 Host Entry Configuration Options

Command Syntax and Usage	
host <i><1-128></i> address <i><IPv6 address></i> <i><prefix length (1-128)></i>	Configures the base IPv6 address and the subnet prefix length for the host entry. Command mode: Router OSPF3
host <i><1-128></i> area <i><area index (0-2)></i>	Configures the area index of the host. Command mode: Router OSPF3
host <i><1-128></i> cost <i><1-65535></i>	Configures the cost value of the host. Command mode: Router OSPF3
host <i><1-128></i> enable	Enables the host entry. Command mode: Router OSPF3
host <i><1-128></i> no enable	Disables the host entry. Command mode: Router OSPF3
no host <i><1-128></i>	Deletes the host entry. Command mode: Router OSPF3
show ipv6 ospf host [<i><1-128></i>]	Displays the current OSPFv3 host entries. Command mode: All

OSPFv3 Redist Entry Configuration

Table 249 OSPFv3 Redist Entry Configuration Options

Command Syntax and Usage

redist-config *<1-128>* **address** *<IPv6 address>* *<IPv6 prefix length (1-128)>*

Configures the base IPv6 address and the subnet prefix length for the redistribution entry.

Command mode: Router OSPF3

redist-config *<1-128>* **metric-value** *<1-16777215>*

Configures the route metric value applied to the route before it is advertised into the OSPFv3 domain.

Command mode: Router OSPF3

redist-config *<1-128>* **metric-type** *asExttype1|asExttype2*

Configures the metric type applied to the route before it is advertised into the OSPFv3 domain.

Command mode: Router OSPF3

[no] redist-config *<1-128>* **tag** *<0-4294967295>*

Configures the route tag.

Command mode: Router OSPF3

redist-config *<1-128>* **enable**

Enables the OSPFv3 redistribution entry.

Command mode: Router OSPF3

redist-config *<1-128>* **no enable**

Disables the OSPFv3 redistribution entry.

Command mode: Router OSPF3

no redist-config *<1-128>*

Deletes the OSPFv3 redistribution entry.

Command mode: Router OSPF3

show ipv6 ospf redist-config

Displays the current OSPFv3 redistribution configuration entries.

Command mode: Router OSPF3

OSPFv3 Redistribute Configuration

Table 250 OSPFv3 Redistribute Configuration Options

Command Syntax and Usage
[no] redistribute {connected static} export <i><metric value (1-16777215)></i> <i><metric type (1-2)></i> <i><tag (0-4294967295)></i> Exports the routes of this protocol as external OSPFv3 AS-external LSAs in which the metric, metric type, and route tag are specified. To remove a previous configuration and stop exporting the routes of the protocol, use the no form of the command. Command mode: Router OSPF3
show ipv6 ospf Displays the current OSPFv3 route redistribution settings. Command mode: All

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 251 IP Loopback Interface commands

Command Syntax and Usage
interface loopback <i><1-5></i> Enter Interface Loopback mode. Command mode: Global configuration
no interface loopback <i><1-5></i> Deletes the selected loopback interface. Command mode: Global configuration
ip address <i><IP address></i> Defines the loopback interface IP address. Command mode: Interface loopback
ip netmask <i><subnet mask></i> Defines the loopback interface subnet mask. Command mode: Interface loopback

Table 251 IP Loopback Interface commands

Command Syntax and Usage	
enable	Enables the loopback interface. Command mode: Interface loopback
no enable	Disables the loopback interface. Command mode: Interface loopback
show interface loopback <1-5>	Displays the current IP loopback interface parameters. Command mode: All

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 396](#)
- [“RMON Event Configuration” on page 397](#)
- [“RMON Alarm Configuration” on page 398](#)

RMON History Configuration

[Table 252](#) describes the RMON History commands.

Table 252 RMON History commands

Command Syntax and Usage

rmon history *<1-65535>* **interface-oid** *<1-127 characters>*

Configures the interface MIB Object Identifier. The IFOID must correspond to the standard interface OID, as follows:

1.3.6.1.2.1.2.2.1.1.x

where x is the `ifIndex`

Command mode: Global configuration

rmon history *<1-65535>* **requested-buckets** *<1-65535>*

Configures the requested number of buckets, which is the number of discrete time intervals over which data is to be saved. The default value is 30.

The maximum number of buckets that can be granted is 50.

Command mode: Global configuration

rmon history *<1-65535>* **polling-interval** *<1-3600>*

Configures the time interval over which the data is sampled for each bucket.

The default value is 1800.

Command mode: Global configuration

Table 252 RMON History commands

Command Syntax and Usage

rmon history <1-65535> **owner** <1-127 characters>

Enter a text string that identifies the person or entity that uses this History index.

Command mode: Global configuration

no rmon history <1-65535>

Deletes the selected History index.

Command mode: Global configuration

show rmon history

Displays the current RMON History parameters.

Command mode: All

RMON Event Configuration

Table 253 describes the RMON Event commands.

Table 253 RMON Event commands

Command Syntax and Usage

rmon event <1-65535> **description** <1-127 characters>

Enter a text string to describe the event.

Command mode: Global configuration

[no] rmon event <1-65535> **type** log|trap|both

Selects the type of notification provided for this event. For log events, an entry is made in the log table and sent to the configured syslog host. For trap events, an SNMP trap is sent to the management station.

Command mode: Global configuration

rmon event <1-65535> **owner** <1-127 characters>

Enter a text string that identifies the person or entity that uses this event index.

Command mode: Global configuration

Table 253 RMON Event commands

Command Syntax and Usage
no rmon event <I-65535> Deletes the selected RMON Event index. Command mode: Global configuration
show rmon event Displays the current RMON Event parameters. Command mode: All

RMON Alarm Configuration

The Alarm RMON group can track rising or falling values for a MIB object. The MIB object must be a counter, gauge, integer, or time interval. Each alarm index must correspond to an event index that triggers once the alarm threshold is crossed.

Table 254 describes the RMON Alarm commands.

Table 254 RMON Alarm commands

Command Syntax and Usage
rmon alarm <I-65535> oid <I-127 characters> Configures an alarm MIB Object Identifier. Command mode: Global configuration
rmon alarm <I-65535> interval <I-65535> Configures the time interval over which data is sampled and compared with the rising and falling thresholds. The default value is 1800. Command mode: Global configuration
rmon alarm <I-65535> sample abs delta 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">abs—absolute value, the value of the selected variable is compared directly with the thresholds at the end of the sampling interval.delta—delta value, the value of the selected variable at the last sample is subtracted from the current value, and the difference compared with the thresholds. Command mode: Global configuration

Table 254 RMON Alarm commands**Command Syntax and Usage**

```
rmon alarm <1-65535> alarm-type rising|falling|either
```

Configures the alarm type as rising, falling, or either (rising or falling).

Command mode: Global configuration

```
rmon alarm <1-65535> rising-limit <-2147483647 - 2147483647>
```

Configures the rising threshold for the sampled statistic. When the current sampled value is greater than or equal to this threshold, and the value at the last sampling interval was less than this threshold, a single event is generated.

Command mode: Global configuration

```
rmon alarm <1-65535> falling-limit <-2147483647 - 214748364>
```

Configures the falling threshold for the sampled statistic. When the current sampled value is less than or equal to this threshold, and the value at the last sampling interval was greater than this threshold, a single event is generated.

Command mode: Global configuration

```
rmon alarm <1-65535> rising-crossing-index <1-65535>
```

Configures the rising alarm event index that is triggered when a rising threshold is crossed.

Command mode: Global configuration

```
rmon alarm <1-65535> falling-crossing-index <1-65535>
```

Configures the falling alarm event index that is triggered when a falling threshold is crossed.

Command mode: Global configuration

```
rmon alarm <1-65535> owner <1-127 characters>
```

Enter a text string that identifies the person or entity that uses this alarm index.

Command mode: Global configuration

```
no rmon alarm <1-65535>
```

Deletes the selected RMON Alarm index.

Command mode: Global configuration

```
show rmon alarm
```

Displays the current RMON Alarm parameters.

Command mode: All

Virtualization Configuration

Table 255 describes the virtualization configuration options.

Table 255 Virtualization Configurations Options

Command Syntax and Usage

virt enable

Enables VMready.

Command mode: Global configuration

no virt enable

Disables VMready.

Note: This command deletes all configured VM groups.

Command mode: Global configuration

show virt

Displays the current virtualization parameters.

Command mode: All

VM Policy Bandwidth Management

Table 256 describes the bandwidth management options for the selected VM. Use these commands to limit the bandwidth used by each VM.

Table 256 VM Bandwidth Management Options

Command Syntax and Usage

virt vmpolicy vmbwidth [*<MAC address>* | *<UUID>* | *<name>* | *<IP address>* | *<index number>*] **txrate** *<64-10000000>*

The first value configures Committed Rate—the amount of bandwidth available to traffic transmitted from the VM to the switch, in kilobits per second. Enter the value in multiples of 64.

The second values configures the maximum burst size, in Kilobits. Enter one of the following values: 32, 64, 128, 256, 512, 1024, 2048, 4096.

The third value represents the ACL assigned to the transmission rate. The ACL is automatically, in sequential order, if not specified by the user. If there are no available ACLs, the TXrate cannot be configured. Each TXrate configuration reduces the number of available ACLs by one.

Command mode: Global configuration

[no] virt vmpolicy vmbwidth [*<MAC address>* | *<UUID>* | *<name>* | *<IP address>* | *<index number>*] **bwctrl**

Enables or disables bandwidth control on the VM policy.

Command mode: Global configuration

[no] virt vmpolicy vmbwidth [*<MAC address>* | *<UUID>* | *<name>* | *<IP address>* | *<index number>*]

Deletes the bandwidth management settings from this VM policy.

Command mode: Global configuration

show virt vmpolicy vmbandwidth

Displays the current VM bandwidth management parameters.

Command mode: All

VM Group Configuration

[Table 257](#) 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 257 VM Group commands

Command Syntax and Usage

virt vmgroup <1-32> **vlan** <VLAN number>

Assigns a VLAN to this VM group. If you do not assign a VLAN to the VM group, the switch automatically assigns an unused VLAN when adding a port or a VM to the VM Group.

Note: If you add a VM profile to this group, the group will use the VLAN assigned to the profile.

Command mode: Global configuration

[no] virt vmgroup <1-32> **vmap** <1-128> **intports|extports**

Assigns the selected VLAN Map to this group. You can choose to limit operation of the VLAN Map to internal ports only or external ports only. If you do not select a port type, the VMAP is applied to the entire VM Group.

For more information about configuring VLAN Maps, see [“VMAP Configuration” on page 263](#).

Command mode: Global configuration

[no] virt vmgroup <1-32> **tag**

Enables or disables VLAN tagging on ports in this VM group.

Command mode: Global configuration

virt vmgroup <1-32> **vm** [**<MAC address>** | **<UUID>** | **<name>** | **<IP address>** | **<index number>**]

Adds a VM to the VM group. Enter a unique identifier to select a VM.
The UUID and name parameters apply only if Virtual Center information is configured (**virt vmware vcspec**).
The VM index number is found in the VM information dump (**show virt vm**).

Note: If the VM is connected to a port that is contained within the VM group, do not add the VM to the VM group.

Command mode: Global configuration

Table 257 VM Group commands**Command Syntax and Usage**

```
no virt vmgroup <1-32> vm [<MAC address> | <UUID> | <name> |
<IP address> | <index number>]
```

Removes a VM from the VM group. Enter a unique identifier to select a VM.
 The UUID and name parameters apply only if Virtual Center information is configured (**virt vmware vcspec**).
 The VM index number is found in the VM information dump (**show virt vm**).

Command mode: Global configuration

```
virt vmgroup <1-32> profile <profile name (1-32 characters)>
```

Adds the selected VM profile to the VM group.

Command mode: Global configuration

```
no virt vmgroup <1-32> profile
```

Removes the VM profile assigned to the VM group.

Command mode: Global configuration

```
virt vmgroup <1-32> port <port number or alias>
```

Adds the selected port to the VM group.

Note: A port can be added to a VM group only if no VMs on that port are members of the VM group.

Command mode: Global configuration

```
no virt vmgroup <1-32> port <port number or alias>
```

Removes the selected port from the VM group.

Command mode: Global configuration

```
virt vmgroup <1-32> portchannel <trunk number>
```

Adds the selected trunk group to the VM group.

Command mode: Global configuration

```
no virt vmgroup <1-32> portchannel <trunk number>
```

Removes the selected trunk group from the VM group.

Command mode: Global configuration

Table 257 VM Group commands

Command Syntax and Usage

virt vmgroup <1-32> key <1-65535>
Adds an LACP admin key to the VM group. LACP trunks formed with this admin key will be included in the VM group.
Command mode: Global configuration
no virt vmgroup <1-32> key <1-65535>
Removes an LACP admin key from the VM group.
Command mode: Global configuration
[no] virt vmgroup <1-32> stg <STG number>
Assigns the VM group VLAN to a Spanning Tree Group (STG).
Command mode: Global configuration
show virt vmgroup <1-32>
Displays the current VM group parameters.
Command mode: All

VM Profile Configuration

Table 258 describes the VM Profiles configuration options.

Table 258 VM Profiles commands

Command Syntax and Usage

virt vmprofile <profile name (1-39 characters)>
Defines a name for the VM profile. The switch supports up to 32 VM profiles.
Command mode: Global configuration
no virt vmprofile <profile name (1-39 characters)>
Deletes the selected VM profile.
Command mode: Global configuration
virt vmprofile edit <profile name (1-39 characters)> vlan <VLAN number>
Assigns a VLAN to the VM profile.
Command mode: Global configuration

Table 258 VM Profiles commands

Command Syntax and Usage
<p>[no] virt vmprofile edit <i><profile name (1-39 characters)></i> shaping [<i><average (1-1000000000)></i> <i><burst (1-1000000000)></i> <i><peak (1-1000000000)></i>]</p> <p>Configures traffic shaping parameters implemented in the hypervisor, as follows:</p> <ul style="list-style-type: none"><input type="checkbox"/> Average traffic, in Kilobits per second<input type="checkbox"/> Maximum burst size, in Kilobytes<input type="checkbox"/> Peak traffic, in Kilobits per second<input type="checkbox"/> Delete traffic shaping parameters. <p>Command mode: Global configuration</p>
<p>show virt vmprofile [<i><profile name></i>]</p> <p>Displays the current VM Profile parameters.</p> <p>Command mode: All</p>

VM Ware Configuration

Table 259 describes the VMware configuration options. When the user configures the VMware Virtual Center, the VM Agent module in the switch can perform advanced functionality by communicating with the VMware management console. The Virtual Center provides VM and Host names, IP addresses, Virtual Switch and port group information. The VM Agent on the switch communicates with the Virtual Center to synchronize VM profiles between the switch and the VMware virtual switch.

Table 259 VM Ware commands

Command Syntax and Usage

virt vmware hbport <1-65535>

Configures the UDP port number used for heartbeat communication from the VM host to the Virtual Center. The default value is port 902.

Command mode: Global configuration

[no] virt vmware vcspec [<IP address> | [<username> noauth]

Defines the Virtual Center credentials on the switch. Once you configure the Virtual Center, VM Agent functionality is enabled across the system.

You are prompted for the following information:

- ☐ IP address of the Virtual Center
- ☐ User name and password for the Virtual Center
- ☐ Whether to authenticate the SSL security certificate (yes or no)

Command mode: Global configuration

show virt vmware

Displays the current VMware parameters.

Command mode: All

Configuration Dump

The dump program writes the current switch configuration to the terminal screen. To start the dump program, at the prompt, enter:

```
Router(config)# show running-config
```

The configuration is displayed with parameters that have been changed from the default values. The screen display can be captured, edited, and placed in a script file, which can be used to configure other switches through a Telnet connection. When using Telnet to configure a new switch, paste the configuration commands from the script file at the command line prompt of the switch. The active configuration can also be saved or loaded via FTP/TFTP, as described on [page 408](#).

Saving the Active Switch Configuration

When the `copy running-config {ftp|tftp}` command is used, the switch's active configuration commands (as displayed using `show running-config`) will be uploaded to the specified script configuration file on the FTP/TFTP server. To start the switch configuration upload, at the prompt, enter:

```
Router(config)# copy running-config ftp  
  
or  
  
Router(config)# copy running-config tftp
```

The switch prompts you for the server address and filename.

Note – The output file is formatted with line-breaks but no carriage returns—the file cannot be viewed with editors that require carriage returns (such as Microsoft Notepad).

Note – If the FTP/TFTP server is running SunOS or the Solaris operating system, the specified configuration file must exist prior to executing the `copy running-config` command and must be writable (set with proper permission, and not locked by any application). The contents of the specified file will be replaced with the current configuration data.

Restoring the Active Switch Configuration

When the `copy {ftp|tftp} running-config` command is used, the active configuration will be replaced with the commands found in the specified configuration file. The file can contain a full switch configuration or a partial switch configuration.

To start the switch configuration download, at the prompt, enter:

```
Router(config)# copy ftp running-config  
  
    or  
  
Router(config)# copy tftp running-config
```

The switch prompts you for the server address and filename.

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 260 General Operations Commands

Command Syntax and Usage

password *<1-128 characters>*

Allows the user to change the password. You must enter the current password in use for validation. The switch prompts for a new password between 1-128 characters.

Command Mode: Privileged EXEC

clear logging

Clears all Syslog messages.

Command Mode: Privileged EXEC

ntp send

Allows the user to send requests to the NTP server.

Command Mode: Privileged EXEC

Operations-Level Port Commands

Operations-level port options are used for temporarily disabling or enabling a port, and for re-setting the port.

Table 261 Port Operations Commands

Command Syntax and Usage

no interface port *<port number or alias>* **shutdown**

Temporarily enables the port. The port will be returned to its configured operation mode when the switch is reset.

Command Mode: Privileged EXEC

interface port *<port number or alias>* **shutdown**

Temporarily disables the port. The port will be returned to its configured operation mode when the switch is reset.

Command Mode: Privileged EXEC

interface port *<port number or alias>* **learning**

Temporarily enables FDB learning on the port.

Command Mode: Privileged EXEC

no interface port *<port number or alias>* **learning**

Temporarily disables FDB learning on the port.

Command Mode: Privileged EXEC

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

Displays the port interface operational state.

Command Mode: Privileged EXEC

Operations-Level Port 802.1X Commands

Operations-level port 802.1X options are used to temporarily set 802.1X parameters for a port.

Table 262 802.1X Operations Commands

Command Syntax and Usage

interface port *<port number or alias>* **dot1x init**

Re-initializes the 802.1X access-control parameters for the port. The following actions take place, depending on the 802.1X port configuration:

- **force unauth**: the port is placed in unauthorized state, and traffic is blocked.
- **auto**: the port is placed in unauthorized state, then authentication is initiated.
- **force auth**: the port is placed in authorized state, and authentication is not required.

Command Mode: Privileged EXEC

interface port *<port number or alias>* **dot1x re-authenticate**

Re-authenticates the supplicant (client) attached to the port. This command only applies if the port's 802.1X mode is configured as **auto**.

Command Mode: Privileged EXEC

Operations-Level VRRP Commands

Table 263 Virtual Router Redundancy Operations Commands

Command Syntax and Usage

router vrrp backup *<virtual router number (1-255)>*

Forces the specified master virtual router on this switch into backup mode. This is generally used for passing master control back to a preferred switch once the preferred switch has been returned to service after a failure. When this command is executed, the current master gives up control and initiates a new election by temporarily advertising its own priority level as 0 (lowest). After the new election, the virtual router forced into backup mode by this command will resume master control in the following cases:

- This switch owns the virtual router (the IP addresses of the virtual router and its IP interface are the same)
- This switch’s virtual router has a higher priority and preemption is enabled.
- There are no other virtual routers available to take master control.

Command Mode: Privileged EXEC

Operations-Level BGP Commands

Table 264 IP BGP Operations Commands

Command Syntax and Usage

router bgp start *<1-16>*

Starts the peer session.

Command Mode: Privileged EXEC

router bgp stop *<1-16>*

Stops the peer session.

Command Mode: Privileged EXEC

show ip bgp state

Displays the current BGP operational state.

Command Mode: Privileged EXEC

Protected Mode Options

Protected Mode is used to secure certain switch management options, so they cannot be changed by the management module.

Table 265 Protected Mode Options

Command Syntax and Usage

[no] protected-mode external-management

Enables exclusive local control of switch management. When Protected Mode is set to **on**, the management module cannot be used to disable external management on the switch. The default value is **enabled**.

Note: Due to current management module implementation, this setting cannot be disabled.

Command Mode: Global Configuration

[no] protected-mode external-ports

Enables exclusive local control of external ports. When Protected Mode is set to **on**, the management module cannot be used to disable external ports on the switch. The default value is **enabled**.

Note: Due to current management module implementation, this setting cannot be disabled.

Command Mode: Global Configuration

[no] protected-mode factory-default

Enables exclusive local control of factory default resets. When Protected Mode is set to **on**, the management module cannot be used to reset the switch software to factory default values. The default value is **enabled**.

Note: Due to current management module implementation, this setting cannot be disabled.

Command Mode: Global Configuration

[no] protected-mode management-vlan-interface

Enables exclusive local control of the management interface. When Protected Mode is set to **on**, the management module cannot be used to configure parameters for the management interface. The default value is **enabled**.

Note: Due to current management module implementation, this setting cannot be disabled.

Command Mode: Global Configuration

Table 265 Protected Mode Options

Command Syntax and Usage

protected-mode enable

Turns Protected Mode **on**. When Protected Mode is turned on, the switch takes exclusive local control of all enabled options.

Command Mode: Global Configuration

no protected-mode enable

Turns Protected Mode **off**. When Protected Mode is turned off, the switch relinquishes exclusive local control of all enabled options.

Command Mode: Global Configuration

show protected-mode

Displays the current Protected Mode configuration.

Command Mode: Global Configuration

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 266 VMware Operations Commands

Command Syntax and Usage

virt vmware pg [*<Port Group name>* *<host ID>* *<VSwitch name>* *<VLAN number>*
<shaping-enabled> *<average-Kbps>* *<burst-KB>* *<peak-Kbps>*]

Adds a Port Group to a VMware host. You are prompted for the following information:

- ☐ Port Group name
- ☐ VMware host ID (Use host UUID, host IP address, or host name.)
- ☐ Virtual Switch name
- ☐ VLAN ID of the Port Group
- ☐ Whether to enable the traffic-shaping profile (1 or 0). If you choose 1 (yes), you are prompted to enter the traffic shaping parameters.

Command Mode: Privileged EXEC

Table 266 VMware Operations Commands**Command Syntax and Usage**

virt vmware vsw *<host ID>* *<Virtual Switch name>*

Adds a Virtual Switch to a VMware host. Use one of the following identifiers to specify the host:

- ☐ UUID
- ☐ IP address
- ☐ Host name

Command Mode: Privileged EXEC

no virt vmware pg *<Port Group name>* *<host ID>*

Removes a Port Group from a VMware host. Use one of the following identifiers to specify the host:

- ☐ UUID
- ☐ IP address
- ☐ Host name

Command Mode: Privileged EXEC

no virt vmware vsw *<host ID>* *<Virtual Switch name>*

Removes a Virtual Switch from a VMware host. Use one of the following identifiers to specify the host:

- ☐ UUID
- ☐ IP address
- ☐ Host name

Command Mode: Privileged EXEC

Table 266 VMware Operations Commands

Command Syntax and Usage

virt vmware export *<VM profile name>* *<VMware host ID (one per line, 'null' to end)>*
<Virtual Switch name>

Exports a VM Profile to one or more VMware hosts. This command allows you to distribute a VM Profile to VMware hosts.

Use one of the following identifiers to specify each host:

- ☐ UUID
- ☐ IP address
- ☐ Host name

The switch displays a list of available Virtual Switches. You may enter a Virtual Switch name from the list, or enter a new name to create a new Virtual Switch.

Command Mode: Privileged EXEC

virt vmware scan

Performs a scan of the VM Agent, and updates VM information.

Command Mode: Privileged EXEC

virt vmware vmacpg *<VNIC MAC address>* *<Port Group name>*

Changes a VNIC's configured Port Group.

Command Mode: Privileged EXEC

virt vmware updpkg *<Port Group name>* *<host ID>* *<VLAN number>*

Updates a VMware host's Port Group parameters.

Command Mode: Privileged EXEC

CHAPTER 6

Boot Options

To use the Boot Options commands, you must be logged in to the switch as the administrator. The Boot Options commands provide options for:

- Selecting a switch software image to be used when the switch is next reset
- Selecting a configuration block to be used when the switch is next reset
- Downloading or uploading a new software image to the switch via FTP/TFTP

In addition to the Boot commands, you can use a Web browser or SNMP to work with switch image and configuration files. To use SNMP, refer to “Working with Switch Images and Configuration Files” in the *Command Reference*.

The boot options are discussed in the following sections.

Stacking Boot Options

The Stacking Boot options are used to define the role of the switch in a stack: either as the Master that controls the stack, or as a participating Member switch. Options are available for loading stack software to individual Member switches, and to configure the VLAN that is reserved for inter-switch stacking communications.

You must enable Stacking and reset the switch to enter Stacking mode. When the switch enters Stacking mode, the Stacking configuration menu appears. For more information, see “[Stacking Configuration Menu](#)” on page 270.

Table 267 lists the Boot Stacking command options.

Table 267 Boot Stacking Options

Command Syntax and Usage

boot stack mode [master|member]

Configures the Stacking mode for the selected switch.

Command mode: Global configuration

boot stack higig-trunk <list of ports>

Configures the ports used to connect the switch to the stack. Enter only 10Gb external ports (EXT1, EXT2, EXT3).

Command mode: Global configuration

boot stack vlan <VLAN number>

Configures the VLAN used for Stacking control communication.

Command mode: Global configuration

default boot stack [master|backup|<csnum (1-6)>|all]

Resets the Stacking boot parameters to their default values.

Command mode: Global configuration

boot stack push-image {image1|image2|boot}

Pushes the selected software file from the master to the selected switch.

Command mode: Global configuration

boot stack enable

Enables the switch stack.

Command mode: Global configuration

no boot stack enable

Disables the switch stack.

Command mode: Global configuration

show boot stack [master|backup|<csnum (1-6)>|all]

Displays current Stacking boot parameters.

Command mode: All

When in stacking mode, the following stand-alone features are not supported:

- Active Multi-Path Protocol (AMP)
- SFD
- sFlow port monitoring
- Uni-Directional Link Detection (UDLD)
- Port flood blocking
- BCM rate control
- Link Layer Detection Protocol (LLDP)
- Private VLANs
- RIP
- OSPF and OSPFv3
- IPv6
- Virtual Router Redundancy Protocol (VRRP)
- Loopback Interfaces
- Router IDs
- Route maps
- Border Gateway Protocol (BGP)
- MAC address notification
- Static MAC address adding
- Static multicast
- Static routes
- MSTP and RSTP settings for CIST, Name, Rev, and Maxhop
- IGMP Relay and IGMPv3
- Virtual NICs

Switch menus and commands for unsupported features may be unavailable, or may have no effect on switch operation.

Scheduled Reboot

This feature allows you to schedule a reboot to occur at a particular time in the future. This feature is particularly helpful if the user needs to perform switch upgrades during off-peak hours. You can set the reboot time, cancel a previously scheduled reboot, and check the time of the currently set reboot schedule.

Table 268 Boot Scheduling Options

Command Syntax and Usage

boot schedule *<day of week>* *<time of day>*

Defines the reboot schedule. Enter the day of the week, followed by the time of day (in hh:mm format). For example:

boot schedule monday 11:30

Command mode: Global configuration

no boot schedule

Cancels the next pending scheduled reboot.

Command mode: Global configuration

show boot

Displays the current reboot scheduling parameters.

Command mode: All

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 269 Netboot Options (/boot/netboot)

Command Syntax and Usage

boot netboot enable

Enables Netboot. When enabled, the switch boots into factory-default configuration, and attempts to download a new configuration file.

Command mode: Global configuration

no boot netboot enable

Disables Netboot.

Command mode: Global configuration

[no] boot netboot tftp <IP address>

Configures the IP address of the TFTP server used for manual configuration. This server is used if DHCP is not enabled, or if the DHCP server does not return the required information.

Command mode: Global configuration

[no] boot netboot cfgfile <1-31 characters>

Defines the file path for the configuration file on the TFTP server. For example:

/directory/sub/config.cfg

Command mode: Global configuration

show boot

Displays the current Netboot parameters.

Command mode: All

Updating the Switch Software Image

The switch software image is the executable code running on the 1/10Gb Uplink ESM. A version of the image ships with the switch, and comes pre-installed on the device. As new versions of the image are released, you can upgrade the software running on your switch. To get the latest version of software available for your GbESM, go to:

<http://www-304.ibm.com/jct01004c/systems/support>

Click on software updates. Use the following command to determine the current software version:

show boot

Upgrading the software image on your switch requires the following:

- Loading the new image onto a FTP or TFTP server on your network
- Transferring the new image from the FTP or TFTP server to your switch
- Selecting the new software image to be loaded into switch memory the next time the switch is reset

Loading New Software to Your Switch

The switch can store up to two different software images, called `image1` and `image2`, as well as boot software, called `boot`. When you load new software, you must specify where it should be placed: either into `image1`, `image2`, or `boot`.

For example, if your active image is currently loaded into `image1`, you would probably load the new image software into `image2`. This lets you test the new software and reload the original active image (stored in `image1`), if needed.

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}
```

Select a port, or press <Enter> to use the default (management port).

2. Enter the hostname or IP address of the FTP or TFTP server.

```
Address or name of remote host: <IP address or hostname>
```

3. Enter the name of the new software file on the server.

```
Source file name: <filename>
```

The exact form of the name will vary by server. However, the file location is normally relative to the FTP or TFTP directory (usually `tftpboot`).

4. Enter your username and password for the server, if applicable.

```
User name: {<username>|<Enter>}
```

5. The system prompts you to confirm your request.

You should next select a software image to run, as described below.

Selecting a Software Image to Run

You can select which software image (`image1` or `image2`) you want to run in switch memory for the next reboot.

1. In Global Configuration mode, enter:

```
Router(config)# boot image {image1|image2}
```

2. Enter the name of the image you want the switch to use upon the next boot.

The system informs you of which image set to be loaded at the next reset:

```
Next boot will use switch software image1 instead of image2.
```

Uploading a Software Image from Your Switch

You can upload a software image from the switch to a FTP or TFTP server.

1. In Privileged EXEC mode, enter:

```
Router# copy {image1|image2|boot-image} {ftp|tftp}
```

Select a port, or press <Enter> to use the default (management port).

2. Enter the name or the IP address of the FTP or TFTP server:

```
Address or name of remote host: <IP address or hostname>
```

3. Enter the name of the file into which the image will be uploaded on the FTP or TFTP server:

```
Destination file name: <filename>
```

4. Enter your username and password for the server, if applicable.

```
User name: {<username>|<Enter>}
```

5. The system then requests confirmation of what you have entered. To have the file uploaded, enter **y**.

```
image2 currently contains Software Version 6.3.0
that was downloaded at 0:23:39 Thu Jan 1, 2010
Upload will transfer image2 (2788535 bytes) to file "image1"
on FTP/TFTP server 1.90.90.95.
Confirm upload operation (y/n) ? y
```


Selecting a Configuration Block

When you make configuration changes to the 1/10Gb Uplink ESM, 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 1/10Gb Uplink ESM 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 1/10Gb Uplink ESM is moved to a network environment where it will be re-configured for a different purpose.

In Global Configuration mode, use the following command to set which configuration block you want the switch to load the next time it is reset:

```
Router (config)# boot configuration-block {active|backup|factory}
```

Resetting the Switch

You can reset the switch to make your software image file and configuration block changes occur.

Note – Resetting the switch causes the Spanning Tree Group to restart. This process can be lengthy, depending on the topology of your network.

Enter the following command to reset (reload) the switch:

```
>> Router# reload
```

You are prompted to confirm your request.

```
Reset will use software "image2" and the active config block.  
>> Note that this will RESTART the Spanning Tree,  
>> which will likely cause an interruption in network service.  
Confirm reload (y/n) ?
```

Accessing the BLADEOS CLI

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

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

The default command-line interface for the GbESM is the BLADEOS CLI. To access the ISCLI, enter the following command and reset the GbESM:

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

Users can select the CLI mode upon login, if the following ISCLI command is enabled:

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

Only an administrator connected through the CLI can view and enable the `prompt` command. When `prompt` is enabled, the first user to log in can select the CLI mode. Subsequent users must use the selected CLI mode, until all users have logged out.

Using the Boot Management Menu

The Boot Management menu allows you to switch the software image, reset the switch to factory defaults, or to recover from a failed software download.

You can interrupt the boot process and enter the Boot Management menu from the serial console port. When the system displays Memory Test, press **<Shift B>**. The Boot Management menu appears.

```
Resetting the System ...
Memory Test .....

Boot Management Menu
1 - Change booting image
2 - Change configuration block
3 - Xmodem download
4 - Exit

Please choose your menu option: 1
Current boot image is 1. Enter image to boot: 1 or 2: 2
Booting from image 2
```

The Boot Management menu allows you to perform the following actions:

- To change the booting image, press 1 and follow the screen prompts.
- To change the configuration block, press 2, and follow the screen prompts.
- To perform an Xmodem download, press 3 and follow the screen prompts.
- To exit the Boot Management menu, press 4. The booting process continues.

Recovering from a Failed Upgrade

Use the following procedure to recover from a failed software upgrade.

1. Connect a PC to the serial port of the switch.
2. Open a terminal emulator program that supports XModem Download (for example, HyperTerminal, CRT, PuTTY) and select the following serial port characteristics:
 - Speed: 9600 bps
 - Data Bits: 8
 - Stop Bits: 1
 - Parity: None
 - Flow Control: None

3. Boot the switch and access the Boot Management menu by pressing <Shift B> while the Memory Test is in progress and the dots are being displayed.
4. Select 3 for Xmodem download. When you see the following message, change the Serial Port characteristics to 115200 bps:

```
## Switch baudrate to 115200 bps and press ENTER ...
```

5. Press <Enter> to set the system into download accept mode. When the readiness meter displays (a series of “C” characters), start XModem on your terminal emulator.
6. Select the Boot Image to download. The XModem initiates the file transfer. When the download is complete, a message similar to the following is displayed:

```
yzModem - CRC mode, 62494(SOH)/0(STX)/0(CAN) packets, 6 retries

Extracting images ... Do *NOT* power cycle the switch.

**** VMLINUX ****

Un-Protected 10 sectors

Erasing Flash..... done

Writing to Flash.....done

Protected 10 sectors

**** RAMDISK ****

Un-Protected 44 sectors

Erasing Flash..... done

Writing to Flash.....done

Protected 44 sectors

**** BOOT CODE ****

Un-Protected 8 sectors

Erasing Flash..... done

Writing to Flash.....done

Protected 8 sectors
```

7. When you see the following message, change the Serial Port characteristics to 9600 bps:

```
## Switch baudrate to 9600 bps and press ESC ...
```

8. Press the Escape key (<Esc>) to re-display the Boot Management menu.
9. Select 3 to start a new XModem Download. When you see the following message, change the Serial Port characteristics to 115200 bps:

```
## Switch baudrate to 115200 bps and press ENTER ...
```

10. Press <Enter> to continue the download.
11. Select the OS Image to download. The XModem initiates the file transfer. When the download is complete, a message similar to the following is displayed:

```
yzModem - CRC mode, 27186(SOH)/0(STX)/0(CAN) packets, 6 retries
Extracting images ... Do *NOT* power cycle the switch.
**** Switch OS ****

Please choose the Switch OS Image to upgrade [1|2|n] :
```

12. Select the image number to load the new image (1 or 2). It is recommended that you select 1. A message similar to the following is displayed:

```
Switch OS Image 1 ...
Un-Protected 27 sectors
Erasing Flash..... done
Writing to Flash.....done
Protected 27 sectors
```

13. When you see the following message, change the Serial Port characteristics to 9600 bps:

```
## Switch baudrate to 9600 bps and press ESC ...
```

14. Press the Escape key (<Esc>) to re-display the Boot Management menu.

Select 4 to exit and boot the new image.

CHAPTER 7

Maintenance Commands

The maintenance commands are used to manage dump information and forward database information. They also include debugging commands to help with troubleshooting.

Dump information contains internal switch state data that is written to flash memory on the 1/10Gb Uplink ESM 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 270 General Maintenance Commands

Command Syntax and Usage

show flash-dump-uuencode

Displays dump information in uuencoded format.

Command mode: All except User EXEC

For details, see [page 441](#).

copy flash-dump tftp

Saves the system dump information via TFTP.

Command mode: All except User EXEC

For details, see [page 442](#).

copy flash-dump ftp

Saves the system dump information via FTP.

Command mode: All except User EXEC

Table 270 General Maintenance Commands

Command Syntax and Usage

clear flash-dump

Clears dump information from flash memory.

Command mode: All except User EXEC

show tech-support

Dumps all GbESM information, statistics, and configuration. You can log the output (`tsdmp`) into a file.

Command mode: All except User EXEC

copy tech-support tftp

Redirects the technical support dump (`tsdmp`) to an external TFTP server.

Command mode: All except User EXEC

copy tech-support ftp

Redirects the technical support dump (`tsdmp`) to an external FTP server.

Command mode: All except User EXEC

Forwarding Database Maintenance

The Forwarding Database commands can be used to view information and to delete a MAC address from the forwarding database or to clear the entire forwarding database. This is helpful in identifying problems associated with MAC address learning and packet forwarding decisions.

Table 271 FDB Manipulation Commands

Command Syntax and Usage

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

Displays a single database entry by its MAC address. If not specified, you are prompted for the MAC address of the device. Enter the MAC address using one of the following formats:

- `xx:xx:xx:xx:xx:xx` (such as `08:00:20:12:34:56`)
- `xxxxxxxxxxxx` (such as `080020123456`)

Command mode: All except User EXEC

Table 271 FDB Manipulation Commands

Command Syntax and Usage

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

Displays all FDB entries for a particular port.

Command mode: All except User EXEC

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

Displays all FDB entries on a single VLAN.

Command mode: All except User EXEC

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

Displays all FDB entries of a particular state.

Command mode: All except User EXEC

show mac-address-table multicast

Displays all Multicast MAC entries in the FDB.

Command mode: All

no mac-address-table {*<MAC address>* | all}

Removes static FDB entries.

Command mode: All except User EXEC

clear mac-address-table

Clears the entire Forwarding Database from switch memory.

Command mode: All except User EXEC

Debugging Commands

The Miscellaneous Debug Commands display trace buffer information about events that can be helpful in understanding switch operation. You can view the following information using the debug commands:

- Events traced by the Management Processor (MP)
- Events traced to a buffer area when a reset occurs

If the switch resets for any reason, the MP trace buffer is saved into the snap trace buffer area. The output from these commands can be interpreted by Technical Support personnel.

Table 272 Miscellaneous Debug Commands

Command Syntax and Usage

debug debug-flags

This command sets the flags that are used for debugging purposes.

Command mode: All except User EXEC

debug mp-trace

Displays the Management Processor trace buffer. Header information similar to the following is shown:

MP trace buffer at 13:28:15 Fri May 25, 2001; mask: 0x2ffdf748

The buffer information is displayed after the header.

Command mode: All except User EXEC

debug mp-snap

Displays the Management Processor snap (or post-mortem) trace buffer. This buffer contains information traced at the time that a reset occurred.

Command mode: All except User EXEC

clear flash-config

Deletes all flash configuration blocks.

Command mode: All except User EXEC

ARP Cache Maintenance

Table 273 Address Resolution Protocol Maintenance Commands

Command Syntax and Usage

show ip arp find *<IP address>*

Shows a single ARP entry by IP address.

Command mode: All except User EXEC

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

Shows ARP entries on selected ports.

Command mode: All except User EXEC

show ip arp vlan *<VLAN number>*

Shows ARP entries on a single VLAN.

Command mode: All except User EXEC

show ip arp reply

Shows the list of IP addresses which the switch will respond to for ARP requests.

Command mode: All except User EXEC

show ip arp

Shows all ARP entries.

Command mode: All except User EXEC

clear ip arp-cache

Clears the entire ARP list from switch memory.

Command mode: All except User EXEC

Note – To display all or a portion of ARP entries currently held in the switch, you can also refer to “ARP Information” on [page 83](#).

IP Route Manipulation

Table 274 IP Route Manipulation Commands

Command Syntax and Usage

show ip route address *<IP address>*

Shows a single route by destination IP address.

Command mode: All except User EXEC

show ip route gateway *<IP address>*

Shows routes to a default gateway.

Command mode: All except User EXEC

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

Shows routes of a single type.

Command mode: All except User EXEC

For a description of IP routing types, see [Table 36 on page 81](#)

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

Shows routes of a single tag.

Command mode: All except User EXEC

For a description of IP routing tags, see [Table 37 on page 82](#)

show ip route interface *<IP interface>*

Shows routes on a single interface.

Command mode: All except User EXEC

show ip route

Shows all routes.

Command mode: All except User EXEC

clear ip route

Clears the route table from switch memory.

Command mode: All except User EXEC

Note – To display all routes, you can also refer to [“IP Routing Information” on page 80](#).

LLDP Cache Manipulation

Table 275 describes the LLDP cache manipulation commands.

Table 275 LLDP Cache Manipulation commands

Command Syntax and Usage

show lldp port *<port alias or number>*

Displays Link Layer Discovery Protocol (LLDP) port information.

Command mode: All

show lldp receive

Displays information about the LLDP receive state machine.

Command mode: All

show lldp transmit

Displays information about the LLDP transmit state machine.

Command mode: All

show lldp remote-device *<1-256>*

Displays information received from LLDP -capable devices.

Command mode: All

show lldp

Displays all LLDP information.

Command mode: All

clear lldp

Clears the LLDP cache.

Command mode: All

IGMP Groups Maintenance

Table 276 describes the IGMP group maintenance commands.

Table 276 IGMP Multicast Group Maintenance Commands

Command Syntax and Usage
show ip igmp groups address <i><IP address></i> Displays a single IGMP multicast group by its IP address. Command mode: All
show ip igmp groups vlan <i><VLAN number></i> Displays all IGMP multicast groups on a single VLAN. Command mode: All
show ip igmp groups interface port <i><port number or alias></i> Displays all IGMP multicast groups on selected ports. Command mode: All
show ip igmp groups portchannel <i><trunk number></i> Displays all IGMP multicast groups on a single trunk group. Command mode: All
show ip igmp groups detail <i><IP address></i> Displays detailed information about a single IGMP multicast group. Command mode: All
show ip igmp groups Displays information for all multicast groups. Command mode: All
clear ip igmp groups Clears the IGMP group table. Command mode: All except User EXEC

IGMP Multicast Routers Maintenance

The following table describes the maintenance commands for IGMP multicast routers (Mrouters).

Table 277 IGMP Multicast Router Maintenance Commands

Command Syntax and Usage
show ip igmp mrouter vlan <i><VLAN number></i> Displays IGMP Mrouter information for a single VLAN. Command mode: All
show ip igmp mrouter Displays information for all Mrouters. Command mode: All
clear ip igmp mrouter Clears the IGMP Mrouter port table. Command mode: All except User EXEC

IPv6 Neighbor Discovery Cache Manipulation

Table 278 describes the IPv6 Neighbor Discovery cache manipulation commands.

Table 278 IPv6 Neighbor Discovery cache manipulation commands

Command Syntax and Usage

show ipv6 neighbors find *<IPv6 address>*

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

Command mode: All

show ipv6 neighbors interface port *<port number or alias>*

Shows IPv6 Neighbor Discovery cache entries on a single port.

Command mode: All

show ipv6 neighbors vlan *<VLAN number>*

Shows IPv6 Neighbor Discovery cache entries on a single VLAN.

Command mode: All

show ipv6 neighbors

Shows all IPv6 Neighbor Discovery cache entries.

Command mode: All

clear ipv6 neighbors

Clears all IPv6 Neighbor Discovery cache entries from switch memory.

Command mode: All except User EXEC

IPv6 Route Maintenance

Table 278 describes the IPv6 route maintenance commands.

Table 279 IPv6 route maintenance commands

Command Syntax and Usage

show ipv6 route

Shows all IPv6 routes.

Command mode: All

clear ipv6 route

Clears all IPv6 routes.

Command mode: All except User EXEC

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 442](#).

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 or FTP System Dump Put

Use these commands to put (save) the system dump to a TFTP or FTP server.

Note – If the TFTP/FTP server is running SunOS or the Solaris operating system, the specified `copy flash-dump tftp` (or `ftp`) file must exist *prior* to executing the `copy flash-dump tftp` command (or `copy flash-dump ftp`), and must be writable (set with proper permission, and not locked by any application). The contents of the specified file will be replaced with the current dump data.

To save dump information via TFTP, enter:

```
Router# copy flash-dump tftp <server filename>
```

You are prompted for the TFTP server IP address or hostname, and the *filename* of the target dump file.

To save dump information via FTP, enter:

```
Router# copy flash-dump ftp <server filename>
```

You are prompted for the FTP server IP address or hostname, your *username* and *password*, and the *filename* of the target dump file.

Clearing Dump Information

To clear dump information from flash memory, enter:

```
Router# clear flash-dump
```

The switch clears the dump region of flash memory and displays the following message:

```
FLASH dump region cleared.
```

If the flash dump region is already clear, the switch displays the following message:

```
FLASH dump region is already clear.
```

Unscheduled System Dumps

If there is an unscheduled system dump to flash memory, the following message is displayed when you log on to the switch:

```
Note: A system dump exists in FLASH. The dump was saved
      at 13:43:22 Wednesday January 30, 2010. Use show flash-dump
      uuencode to
      extract the dump for analysis and clear flash-dump to
      clear the FLASH region. The region must be cleared
      before another dump can be saved.
```


Index

Numerics

802.1p information 111

A

abbreviating commands (CLI) 24
access control
 user 234
Access Control Lists 255
ACL configuration 255
ACL Port commands 248
ACL re-marking 266
ACL statistics 190
active configuration block 200, 425
active IP interface 376
Active Multipath Protocol 277
active port
 VLAN 376
active switch configuration
 gtcfg 408
 ptcfg 407
 restoring 408
active switch, saving and loading configuration 408
addr
 IP route tag 82
administrator account 25
aging
 STP information 68, 71
AMP configuration 277
autonomous system filter action 334
autonomous system filter path
 action 334
 as 334
 aspath 334

B

backup configuration block 425
BGP
 configuration 351
 eBGP 351
 filters, aggregation configuration 356
 iBGP 351
 in route 354
 IP address, border router 352
 IP route tag 82
 keep-alive time 353
 peer 351
 peer configuration 352
 redistribution configuration 355
 remote autonomous system 352
 router hops 353
BLOCKING (port state) 69
Boot Management menu 427
Boot options 417
bootstrap protocol 368
Border Gateway Protocol 82
 configuration 351
Border Gateway Protocol (BGP)
 operations-level options 412
BPDU. *See Bridge Protocol Data Unit.*
bridge priority 68, 74
Bridge Protocol Data Unit (BPDU) 68, 74
 STP transmission frequency 287
Bridge Spanning-Tree parameters 287
broadcast
 IP route tag 82
 IP route type 81

C

capture dump information to a file 441
Cisco Ether Channel 297
CIST information 73

clear	
dump information	442
command (help)	21
commands	
abbreviations	24
conventions used in this manual	14
shortcuts	23
tab completion	24
configuration	
802.1x	271
CIST	282
default gateway interval, for health checks	324
default gateway IP address	324
dump command	407
failover	303
flow control	246
IGMP	357
IP static route	325
port link speed	245
port mirroring	268
port trunking	297
RIP	335
save changes	200
SNMP	217
switch IP address	320
TACACS+	209
VLAN default (PVID)	242
VLAN IP interface	321
VLAN tagging	243
VRRP	369
configuration block	
active	425
backup	425
factory	425
selection	425
Configuration commands	199
configuring routing information protocol	336
COS queue information	111
cost	
STP information	69, 71, 74
STP port option	289
CPU statistics	189
CPU utilization	189

D

daylight savings time	201
debugging	431
default gateway	
information	79
interval, for health checks	324

default gateway, IPv6	379
default password	25
delete	
FDB entry	433
direct (IP route type)	81
directed broadcasts	329
DISABLED (port state)	69
disconnect idle timeout	25
downloading software	422
DSCP	254
dump	
configuration command	407
maintenance	431
duplex mode	
link status	27, 119
dynamic routes	436

E

Error disable and recovery	
system	203
error disable and recovery	
port	245
EtherChannel	
as used with port trunking	297
Etherchannel information	75

F

factory configuration block	425
failover	
configuration	303
FDB statistics	147
fixed	
IP route tag	82
flag field	84
flow control	27, 119
configuring	246
forwarding configuration	
IP forwarding configuration	329
forwarding database (FDB)	431
delete entry	433
Forwarding Database Information	54
Forwarding Database maintenance	432
forwarding state (FWD)	55, 68, 74, 75
fwd (STP bridge option)	288
FwdDel (forward delay), bridge port	68, 71, 74

G

gtcfg (TFTP load command)..... 408

H

health checks
 default gateway interval, retries 324
 retry, number of failed health checks 324
 hello
 STP information 68, 71, 74
 help..... 21
 Hot Links configuration 308
 hot-standby failover..... 374
 hprompt
 system option 202
 HTTPS..... 238

I

ICMP statistics 166
 idle timeout
 overview..... 25
 IEEE standards
 802.1d 68, 286
 802.1p 253
 802.1s 281
 802.1w 281
 802.1x 65, 67
 IGMP Information 105
 IGMP Relay..... 360
 IGMP Snooping 358
 IGMP statistics..... 171
 image
 downloading 422
 software, selecting 423
 indirect (IP route type)..... 81
 Information
 IGMP Multicast Router Information..... 438
 Information commands 27
 Interface change stats..... 176, 182
 IP address
 ARP information 83
 configuring default gateway 324
 IP forwarding
 directed broadcasts..... 329
 IP forwarding information 79
 IP Information..... 79, 104

IP interface
 active 376
 configuring address..... 320
 configuring VLANs 321
 IP interfaces..... 81
 information..... 79
 IP route tag 82
 priority increment value (ifs) for VRRP..... 378
 IP network filter configuration..... 330
 IP Route Manipulation..... 436
 IP routing
 tag parameters 82
 IP Static Route commands 325
 IP statistics 156
 IPv6 default gateway configuration..... 379
 IPv6 Neighbor Discovery..... 322
 IPv6 Neighbor Discovery cache..... 381
 IPv6 static route 380
 ISCLI command modes 18

L

LACP 301
 Layer 2 commands 49
 Layer 3 commands 78
 LDAP 213
 LEARNING (port state)..... 68, 69, 74
 Lightweight Directory Access Protocol 213
 link
 speed, configuring 245
 Link Aggregation Control Protocol..... 301
 link status 27
 command 119
 duplex mode 27, 119
 port speed 27, 119
 Link Status Information 119
 linkt (SNMP option)..... 218
 LISTENING (port state) 69
 LLDP
 configuration..... 293
 information..... 61
 LLDP TLV 295
 local (IP route type)..... 81
 log
 syslog messages 204

M

MAC	
multicast	292
MAC (media access control) address	29, 43, 54, 83, 432
Maintenance commands	431
Management Processor (MP)	433
display MAC address	29, 43
manual style conventions	14
martian	
IP route tag (filtered)	82
IP route type (filtered out)	81
mation	75
MaxAge (STP information)	68, 71, 74
MD5 cryptographic authentication	341
MD5 key	345
media access control. <i>See</i> MAC address.	
meter	
ACL	250, 264
Miscellaneous Debug commands	433
monitor port	268
mp	
packet	186
MP. <i>See</i> Management Processor.	
Mrouter information	108
multicast	
IP route type	81
multicast MAC	292
multiple management VLANs	313
Multiple Spanning Tree	
configuration	281
mxage (STP bridge option)	287

N

nbr change statistics	175, 181
Neighbor Discovery cache configuration	381
Neighbor Discovery, IPv6	322
notice	202
NTP synchronization	216

O

OAM Discovery	
information	64
online help	21
Operations commands	409
operations-level BGP options	412
Operations-Level Port Options	410, 411
operations-level VRRP options	412

ospf

area index	341
authentication key	345
cost of the selected path	344
cost value of the host	348
dead, declaring a silent router to be down	344, 389
dead, health parameter of a hello packet	346, 391
export	349
fixed routes	351
hello, authentication parameter of a hello packet	346, 390
host entry configuration	348
host routes	339
interface	339
interface configuration	344
link state database	340, 382
Not-So-Stubby Area	341, 384
priority value of the switch interface	344
range number	339
route redistribution configuration	349
spf, shortest path first	342
stub area	341, 384
summary range configuration	343
transit area	341, 384
transit delay	344
type	341, 384
virtual link	339
virtual link configuration	346
virtual neighbor, router ID	347, 391
OSPF Database Information	90
OSPF General Information	89
OSPF Information	87
OSPF Information Route Codes	92
OSPFv3	
configuration	382

P

parameters	
tag	82
type	81
Password	
user access control	234
password	
administrator account	25
default	25
user account	25
passwords	25
ping	22
poisoned reverse, as used with split horizon	336
Port configuration	242

port configuration	242
Port Error Disable and Recovery	245
port mirroring	
configuration	268
Port number	119
port speed	27, 119
port states	
UNK (unknown)	55
port trunking	
description	297
port trunking configuration	297
ports	
disabling (temporarily)	247
information	120
membership of the VLAN	50, 77
priority	69, 74
VLAN ID	28, 120
preemption	
assuming VRRP master routing authority	372
prisrv	
primary radius server	207, 213
Private VLAN	316
Protected Mode	413
Protocol-based VLAN	314
ptcfg (TFTP save command)	407
PVID (port VLAN ID)	28, 120

Q

QoS	253
-----------	-----

R

read community string (SNMP option)	218
receive flow control	246
reference ports	55
re-mark	266
Remote Monitoring (RMON)	396
retries	
radius server	207
retry	
health checks for default gateway	324
rip	
IP route tag	82
RIP Information	100
RIP information	99
RIP. <i>See Routing Information Protocol.</i>	
RMON	
configuration	396
information	114
route statistics	164

router hops	353
routing information protocol	
configuration	336
Routing Information Protocol (RIP)	82
options	336
poisoned reverse	336
split horizon	336
version 1 parameters	335, 336
RSTP information	70
Rx/Tx statistics	174, 180

S

save (global command)	200
secret	
radius server	207
Secure Shell	205
shortcuts (CLI)	23
snap traces	
buffer	434
SNMP	217
SNMP options	217
SNMP statistics	192
SNMPv3	219
software	
image	422
image file and version	29, 43
software upgrade	
recovery	427
spanning tree	
configuration	286
Spanning-Tree Protocol	75
bridge parameters	287
bridge priority	68, 74
port cost option	289
root bridge	68, 74, 287
switch reset effect	425
split horizon	336
Stacking	
boot options	417
configuration	251
state (STP information)	69, 72, 75
static	
IP route tag	82
static multicast MAC	292
static route	
rem	325
static route, IPv6	380
static route	
add	325

statistics	
management processor	185
Statistics commands	125
subnets	
IP interface	320
switch	
name and location	29, 43
resetting	425
system	
contact (SNMP option)	217
date and time	29, 43
information	43
location (SNMP option)	217
System Error Disable and Recovery	203
System Information	29
system options	
hprompt	202
tnport	232
wport	232

T

tab completion (CLI)	24
TACACS+	209
TCP statistics	168, 188
Telnet	
configuring switches using	407
telnet	
radius server	208, 214
text conventions	14
TFTP	422
PUT and GET commands	407
TFTP server	407
timeout	
radius server	207
timeouts	
idle connection	25
timers kickoff	177, 182
TLV	295
tnport	
system option	232
trace buffer	433
traceroute	22
transmit flow control	246
Trunk group information	75
trunk hash algorithm	299
type of area	
ospf	341, 384
type parameters	81
typographic conventions, manual	14

U

UCB statistics	188
UDLD	
information	63
UDP statistics	170
unknown (UNK) port state	55
Unscheduled System Dump	443
upgrade	
recover from failure	427
upgrade, switch software	422
user access control configuration	234
user account	25
Uencode Flash Dump	441

V

virtual router	
description	370
tracking criteria	372
virtual router group configuration	374
virtual router group priority tracking	376
Virtual Router Redundancy Protocol (VRRP)	
authentication parameters for IP interfaces	377
operations-level options	412
priority tracking options	352, 356, 373
Virtual Router Redundancy Protocol configuration	369
virtual routers	
increasing priority level of	372
priority increment values (vrs) for VRRP	378
virtualization	
configuration	400
information	122
VLAN	
active port	376
configuration	312
VLAN tagging	
port configuration	243
port restrictions	313
VLANs	
ARP entry information	83
information	77
name	50, 77
port membership	50, 77
setting default number (PVID)	242
tagging	28, 120, 313
VLAN Number	77

VM	
bandwidth management	401
group configuration.....	402
information	122
policy configuration	401
profile configuration.....	404
VMware configuration	406
VMware information.....	123
VMware operations.....	414
VRRP	
interface configuration.....	377
master advertisements	371
tracking configuration	378
VRRP Information	109
VRRP master advertisements	
time interval.....	375
VRRP statistics	183

W

watchdog timer	431
weights	
setting virtual router priority values	378
wport	232