

BLADEOS™

# ISCLI Reference

BNT Layer 2/3 GbE Switch Module for IBM BladeCenter®

Version 5.1

---

Part Number: BMD00101, December 2009

**BLADE**  
NETWORK TECHNOLOGIES

2350 Mission College Blvd.  
Suite 600  
Santa Clara, CA 95054  
[www.bladenetwork.net](http://www.bladenetwork.net)

Copyright © 2009 BLADE Network Technologies, Inc., 2350 Mission College Blvd., Suite 600, Santa Clara, California, 95054, USA. All rights reserved. Part Number: BMD00101.

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 ■ 11**

- Who Should Use This Book ■ 11
- How This Book Is Organized ■ 11
- Typographic Conventions ■ 12
- How to Get Help ■ 13

## **Chapter 1: ISCLI Basics ■ 15**

- Accessing the ISCLI ■ 15
- ISCLI Command Modes ■ 16
- Global Commands ■ 19
- Command Line Interface Shortcuts ■ 20
  - CLI List and Range Inputs ■ 20
  - Command Abbreviation ■ 21
  - Tab Completion ■ 21
- User Access Levels ■ 21
- Idle Timeout ■ 22

## **Chapter 2: Information Commands ■ 23**

- System Information ■ 25
  - SNMPv3 System Information ■ 26
    - SNMPv3 USM User Table Information ■ 28
    - SNMPv3 View Table Information ■ 29
    - SNMPv3 Access Table Information ■ 30
    - SNMPv3 Group Table Information ■ 31
    - SNMPv3 Community Table Information ■ 32
    - SNMPv3 Target Address Table Information ■ 33
    - SNMPv3 Target Parameters Table Information ■ 34
    - SNMPv3 Notify Table Information ■ 35
    - SNMPv3 Dump Information ■ 36
  - General System Information ■ 37

Show Recent Syslog Messages	■	39
User Status	■	40
Layer 2 Information	■	41
FDB Information	■	44
Show All FDB Information	■	45
Clearing Entries from the Forwarding Database	■	45
Link Aggregation Control Protocol Information	■	46
Link Aggregation Control Protocol	■	47
Layer 2 Failover Information	■	48
Layer 2 Failover information	■	49
Hot Links Information	■	50
LLDP Information	■	51
LLDP Remote Device Information	■	52
Unidirectional Link Detection Information	■	53
UDLD Port Information	■	53
OAM Discovery Information	■	54
OAM Port Information	■	54
802.1X Information	■	55
Spanning Tree Information	■	57
RSTP/MSTP/PVRST Information	■	60
Common Internal Spanning Tree Information	■	63
Trunk Group Information	■	65
VLAN Information	■	66
Layer 3 Information	■	68
IP Routing Information	■	70
Show All IP Route Information	■	71
ARP Information	■	73
Show All ARP Entry Information	■	74
ARP Address List Information	■	74
BGP Information	■	75
BGP Peer information	■	76
BGP Summary information	■	76
Dump BGP Information	■	77
OSPF Information	■	77
OSPF General Information	■	79
OSPF Interface Information	■	80
OSPF Database Information	■	80
OSPF Information Route Codes	■	82
Routing Information Protocol	■	83
RIP Routes Information	■	83

RIP Interface Information	■ 84
Interface Information	■ 84
IP Information	■ 85
IGMP Multicast Group Information	■ 86
IGMP Group Information	■ 88
IGMP Multicast Router Information	■ 89
VRRP Information	■ 90
Quality of Service Information	■ 91
802.1p Information	■ 92
Access Control List Information Commands	■ 93
Access Control List Information	■ 94
RMON Information Commands	■ 95
RMON History Information	■ 96
RMON Alarm Information	■ 97
RMON Event Information	■ 99
Link Status Information	■ 100
Port Information	■ 101
Port Transceiver Status	■ 102
Information Dump	■ 102

### **Chapter 3: Statistics Commands** ■ 103

Port Statistics	■ 104
802.1X Authenticator Statistics	■ 106
802.1X Authenticator Diagnostics	■ 107
Bridging Statistics	■ 110
Ethernet Statistics	■ 111
Interface Statistics	■ 114
Interface Protocol Statistics	■ 116
Link Statistics	■ 116
RMON Statistics	■ 117
Layer 2 Statistics	■ 120
FDB Statistics	■ 121
LACP Statistics	■ 122
Hotlinks Statistics	■ 123
LLDP Port Statistics	■ 124
OAM Statistics	■ 125
Layer 3 Statistics	■ 126
IPv4 Statistics	■ 130
Route Statistics	■ 133
ARP statistics	■ 133

DNS Statistics	■	134
ICMP Statistics	■	135
TCP Statistics	■	137
UDP Statistics	■	139
IGMP Statistics	■	140
OSPF Statistics	■	141
OSPF Global Statistics	■	142
VRRP Statistics	■	147
Routing Information Protocol Statistics	■	148
Management Processor Statistics	■	149
MP Packet Statistics	■	150
TCP Statistics	■	152
UDP Statistics	■	152
CPU Statistics	■	153
Access Control List Statistics	■	154
ACL Statistics	■	154
ACL Meter Statistics	■	155
SNMP Statistics	■	156
NTP Statistics	■	160
Statistics Dump	■	161
<b>Chapter 4: Configuration Commands</b>	<b>■</b>	<b>163</b>
Viewing and Saving Changes	■	164
System Configuration	■	165
System Host Log Configuration	■	167
SSH Server Configuration	■	169
RADIUS Server Configuration	■	171
TACACS+ Server Configuration	■	173
LDAP Server Configuration	■	177
NTP Server Configuration	■	179
System SNMP Configuration	■	181
SNMPv3 Configuration	■	183
User Security Model Configuration	■	185
SNMPv3 View Configuration	■	186
View-based Access Control Model Configuration	■	188
SNMPv3 Group Configuration	■	190
SNMPv3 Community Table Configuration	■	191
SNMPv3 Target Address Table Configuration	■	192
SNMPv3 Target Parameters Table Configuration	■	193
SNMPv3 Notify Table Configuration	■	195

System Access Configuration	■ 196
Management Network Configuration	■ 197
User Access Control Configuration	■ 198
System User ID Configuration	■ 199
Strong Password Configuration	■ 200
HTTPS Access Configuration	■ 202
Custom Daylight Savings Time Configuration	■ 203
sFlow Configuration	■ 204
sFlow Port Configuration	■ 205
Port Configuration	■ 206
Port Link Configuration	■ 208
Temporarily Disabling a Port	■ 209
UniDirectional Link Detection Configuration	■ 210
Port OAM Configuration	■ 211
ACL Port Configuration	■ 211
ACL Port Metering Commands	■ 212
Re-Marking Commands	■ 214
Re-Marking In-Profile Commands	■ 215
Update User Priority Commands	■ 215
Re-Marking Out-of-Profile Commands	■ 216
Port Spanning Tree Configuration	■ 216
Quality of Service Configuration	■ 218
802.1p Configuration	■ 218
DSCP Configuration	■ 219
Access Control Configuration	■ 220
Access Control List Configuration	■ 221
Ethernet Filtering Configuration	■ 222
IPv4 Filtering Configuration	■ 223
TCP/UDP Filtering Configuration	■ 225
Packet Format Filtering Configuration	■ 226
ACL Block Configuration	■ 227
ACL Group Configuration	■ 227
Port Mirroring	■ 228
Port-Mirroring Configuration	■ 229
Layer 2 Configuration	■ 230
802.1X Configuration	■ 231
802.1X Global Configuration	■ 232
802.1X Guest VLAN Configuration	■ 234
802.1X Port Configuration	■ 235
RSTP/MSTP/PVRST Configuration	■ 238

Common Internal Spanning Tree Configuration	■	239
CIST Bridge Configuration	■	240
CIST Port Configuration	■	241
Spanning Tree Configuration	■	243
Bridge Spanning Tree Configuration	■	244
Spanning Tree Port Configuration	■	245
Forwarding Database Configuration	■	247
Static FDB Configuration	■	248
LLDP Configuration	■	249
LLDP Port Configuration	■	251
LLDP Optional TLV configuration	■	251
Trunk Configuration	■	253
IP Trunk Hash Configuration	■	255
Layer 2 IP Trunk Hash Configuration	■	255
Link Aggregation Control Protocol Configuration	■	257
LACP Port Configuration	■	258
Layer 2 Failover Configuration	■	259
Failover Trigger Configuration	■	260
Auto Monitor Configuration	■	261
Failover Manual Monitor - Monitor Configuration	■	261
Failover Manual Monitor - Control Configuration	■	263
Hot Links Configuration	■	264
Hot Links Trigger Configuration	■	265
Hot Links Master Configuration	■	266
Hot Links Backup Configuration	■	267
VLAN Configuration	■	268
Protocol-Based VLAN Configuration	■	270
Private VLAN Configuration	■	272
VLAN Bandwidth Management Configuration	■	273
Layer 3 Configuration	■	275
IP Interface Configuration	■	277
Default Gateway Configuration	■	278
IPv4 Static Route Configuration	■	280
IP Multicast Route Configuration	■	281
ARP Configuration	■	283
ARP Static Configuration	■	283
IP Forwarding Configuration	■	284
Network Filter Configuration	■	285



Routing Map Configuration	■	286
IP Access List Configuration	■	288
Autonomous System Filter Path Configuration	■	289
Routing Information Protocol Configuration	■	290
Routing Information Protocol Interface Configuration	■	291
Open Shortest Path First Configuration	■	293
Area Index Configuration	■	295
OSPF Summary Range Configuration	■	297
OSPF Interface Configuration	■	298
OSPF Virtual Link Configuration	■	300
OSPF Host Entry Configuration	■	302
OSPF Route Redistribution Configuration.	■	303
OSPF MD5 Key Configuration	■	304
Border Gateway Protocol Configuration	■	305
BGP Peer Configuration	■	306
BGP Redistribution Configuration	■	309
BGP Aggregation Configuration	■	310
IGMP Configuration	■	311
IGMP Snooping Configuration	■	312
IGMPv3 Configuration	■	313
IGMP Relay Configuration	■	314
IGMP Relay Multicast Router Configuration	■	315
IGMP Static Multicast Router Configuration	■	316
IGMP Filtering Configuration	■	317
IGMP Filter Definition	■	318
IGMP Filtering Port Configuration	■	319
IGMP Advanced Configuration	■	319
Domain Name System Configuration	■	321
Bootstrap Protocol Relay Configuration	■	322
VRRP Configuration	■	323
Virtual Router Configuration	■	324
Virtual Router Priority Tracking Configuration	■	326
Virtual Router Group Configuration	■	328
Virtual Router Group Priority Tracking Configuration	■	330
VRRP Interface Configuration	■	331
VRRP Tracking Configuration	■	332
IP Loopback Interface Configuration	■	333
RMON History Configuration	■	334
RMON Event Configuration	■	335
RMON Alarm Configuration	■	336

- Configuration Dump ■ 338
- Saving the Active Switch Configuration ■ 338
- Restoring the Active Switch Configuration ■ 339

## Chapter 5: Operations Commands ■ 341

- Operations-Level Port Commands ■ 342
- Operations-Level Port 802.1X Commands ■ 343
- Operations-Level VRRP Commands ■ 344
- Operations-Level BGP Commands ■ 344
- Protected Mode Options ■ 345

## Chapter 6: Boot Options ■ 347

- Updating the Switch Software Image ■ 348
  - Loading New Software to Your Switch ■ 348
  - Selecting a Software Image to Run ■ 349
  - Uploading a Software Image from Your Switch ■ 350
- Selecting a Configuration Block ■ 350
- Resetting the Switch ■ 351
- Accessing the BLADEOS CLI ■ 352

## Chapter 7: Maintenance Commands ■ 353

- Forwarding Database Maintenance ■ 354
- Debugging Commands ■ 355
- ARP Cache Maintenance ■ 357
- IP Route Manipulation ■ 358
- LLDP Cache Manipulation ■ 359
- IGMP Groups Maintenance ■ 360
- IGMP Multicast Routers Maintenance ■ 361
- Uencode Flash Dump ■ 361
- TFTP or FTP System Dump Put ■ 362
- Clearing Dump Information ■ 362
- Unscheduled System Dumps ■ 363

## Index ■ 365

# Preface

---

The *BLADE OS 5.1 Command Reference* describes how to configure and use the BLADE OS 5.1 software with your BNT Layer 2/3 GbE 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 5.1 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
angle brackets < >	Indicates a variable to enter based on the description inside the brackets. Do not type the brackets when entering the command.  For example, if the command syntax is: <code>ping &lt;IP address&gt;</code>  you enter: <b>ping 192.32.10.12</b>
block body text	Indicates objects such as window names, dialog box names, and icons, as well as user interface objects such as buttons and tabs.
<b>bold fixed-width text</b>	Indicates command names, options, and text that you must enter.  Example: <b>show ip arp</b>
braces { }	Indicates 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.  For example, if the command syntax is: <b>show portchannel {&lt;1-13&gt; hash information}</b>  you would enter: <b>show portchannel &lt;1-13&gt;</b>  or: <b>show portchannel hash</b>  or: <b>show portchannel information</b>

**Table 1** Typographic Conventions

Typeface or Symbol	Meaning
brackets [ ]	<p>Indicates optional elements in syntax descriptions. Do not type the brackets when entering the command.</p> <p>For example, if the command syntax is:  <b>show ip ospf interface</b> [<i>&lt;1-128&gt;</i>]</p> <p>you would enter: <b>show ip ospf interface</b></p> <p>or: <b>show ip ospf interface</b> <i>&lt;1-128&gt;</i></p>
<i>italic text</i>	<p>Indicates variables in command syntax descriptions. Also indicates new terms and book titles.</p> <p>For example, if the command syntax is:  <b>show spanning-tree stp</b> <i>&lt;1-128&gt;</i></p> <p>then <i>&lt;1-128&gt;</i> represents a number between 1 and 128.</p>
plain fixed-width text	<p>Indicates command syntax and system output, for example, prompts and system messages.</p> <p>Example: <code>configure terminal</code></p>
vertical line	<p>Separates multiple choices for command keywords and arguments. Enter only one of the choices. Do not type the vertical line when entering the command.</p> <p>For example, if the command syntax is:  <b>show portchannel</b> {<i>&lt;1-13&gt;</i>   <b>hash</b>   <b>information</b>}</p> <p>then you would enter: <b>show portchannel</b> <i>&lt;1-13&gt;</i></p> <p>or: <b>show portchannel hash</b></p> <p>or: <b>show portchannel information</b></p>

## How to Get Help

If you need help, service, or technical assistance, see the “Getting help and technical assistance” appendix in the *BNT Layer 2/3 GbE Switch Module Installation Guide*.



## CHAPTER 1

# ISCLI Basics

---

Your GbE Switch Module (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: <b>exit</b> or <b>logout</b>
Privileged EXEC	Enter Privileged EXEC mode, from User EXEC mode: <b>enable</b>
Router#	Exit to User EXEC mode: <b>disable</b>  Quit ISCLI: <b>exit</b> or <b>logout</b>
Global Configuration	Enter Global Configuration mode, from Privileged EXEC mode: <b>configure terminal</b>
Router (config) #	Exit to Privileged EXEC: <b>end</b> or <b>exit</b>
Interface IP	Enter Interface IP Configuration mode, from Global Configuration mode: <b>interface ip</b> <interface number>
Router (config-ip) #	Exit to Global Configuration mode: <b>exit</b>  Exit to Privileged EXEC mode: <b>end</b>



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

Table 2 ISCLI Command Modes

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

## 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
<b>?</b>	Provides more information about a specific command or lists commands available at the current level.
<b>list</b>	Lists the commands available at the current level.
<b>exit</b>	Go up one level in the command mode structure. If already at the top level, exit from the command line interface and log out.
<b>copy running-config startup-config</b>	Write configuration changes to non-volatile flash memory.
<b>logout</b>	Exit from the command line interface and log out.
<b>ping</b>	<p>Use this command to verify station-to-station connectivity across the network. The format is as follows:</p> <pre><b>ping</b> {&lt;hostname&gt;   &lt;IP address&gt;} [&lt;tries (1-32)&gt; [&lt;msec delay&gt;]]</pre> <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>
<b>tracert</b>	<p>Use this command to identify the route used for station-to-station connectivity across the network. The format is as follows:</p> <pre><b>tracert</b> {&lt;hostname&gt;   &lt;IP address&gt;} [&lt;max-hops (1-32)&gt; [&lt;msec delay&gt;]]</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>Max-hops</i> (optional) is the maximum distance to trace (1-16 devices), and <i>msec delay</i> (optionally available if <i>max-hops</i> is specified) is the number of milliseconds for wait for the response.</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 {&lt;hostname&gt;   &lt;IP address&gt;} [&lt;port&gt;]</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:

# <code>vlan 1,3,4095</code>	(access VLANs 1, 3, and 4095)
# <code>vlan 1-20</code>	(access VLANs 1 through 20)
# <code>vlan 1-5,90-99,4090-4095</code>	(access multiple ranges)
# <code>vlan 1-5,19,20,4090-4095</code>	(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:

# <code>interface port 1-4</code>	(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 GbE Switch Module, 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 100](#).

---

**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 101](#).

---

**show transceiver**

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

**Command mode:** All

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

---

**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 25](#), 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 37](#).

---

#### **show logging messages**

Displays most recent syslog messages.

**Command mode:** All

For details, see [page 39](#).

---

#### **show access user**

Displays configured user names and their status.

**Command mode:** All except User EXEC

---

#### **show system flow-control**

Displays end-to-end flow control information.

**Command mode:** All except User EXEC

---

## 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 7** SNMPv3 commands

Command Syntax and Usage
<b>show snmp-server v3 user</b>  Displays User Security Model (USM) table information.  <b>Command mode:</b> All  To view the table, see <a href="#">page 28</a> .
<b>show snmp-server v3 view</b>  Displays information about view, subtrees, mask and type of view.  <b>Command mode:</b> All  To view a sample, see <a href="#">page 29</a> .
<b>show snmp-server v3 access</b>  Displays View-based Access Control information.  <b>Command mode:</b> All  To view a sample, see <a href="#">page 30</a> .
<b>show snmp-server v3 group</b>  Displays information about the group, including the security model, user name, and group name.  <b>Command mode:</b> All  To view a sample, see <a href="#">page 31</a> .

**Table 7** 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 32](#).

---

**show snmp-server v3 target-address**

Displays the Target Address table information.

**Command mode:** All

To view a sample, see [page 33](#).

---

**show snmp-server v3 target-parameters**

Displays the Target parameters table information.

**Command mode:** All

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

---

**show snmp-server v3 notify**

Displays the Notify table information.

**Command mode:** All

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

---

**show snmp-server v3**

Displays all the SNMPv3 information.

**Command mode:** All

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

---

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 8 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 9** 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 <code>view subtrees</code> is included or excluded from the MIB view.

## SNMPv3 Access Table Information

The access control sub system provides authorization services.

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

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

The following command displays SNMPv3 access information:

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

**Command mode:** All

Group Name	Model	Level	ReadV	WriteV	NotifyV
vlv2grp	snmpv1	noAuthNoPriv	iso	iso	vlv2only
admingrp	usm	authPriv	iso	iso	iso

Table 10 SNMPv3 Access Table Information

Field	Description
Group Name	Displays the name of group.
Model	Displays the security model used, for example, SNMPv1, or SNMPv2 or USM.
Level	Displays the minimum level of security required to gain rights of access. For example, noAuthNoPriv, authNoPriv, or authPriv.
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 11** 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 12** 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 13** 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 14 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 15** 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  Model  Level  ReadV  WriteV  NotifyV
-----
v1v2grp     snmpv1  noAuthNoPriv  iso     iso     v1v2only
admingrp    usm      authPriv  iso     iso     iso

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

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

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

snmpNotify Table:
Name      Tag
-----

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

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

```

## General System Information

The following command displays system information:

**show sys-info**

**Command mode:** All

```
System Information at 0:16:42 Wed Jan 3, 2009
Time zone: America/US/Pacific
Daylight Savings Time Status: Disabled

BNT Layer 2/3 GbE Switch Module

Switch has been up 5 days, 2 hours, 16 minutes and 42 seconds.
Last boot: 0:00:47 Wed Jan 3, 2009 (reset from console)

MAC address: 00:11:58:ad:a3:00 Management IP Address (if 128):
10.90.90.97
Software Version 5.1.0 (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.



## Layer 2 Information

---

**Table 16** Layer 2 Information Commands

---

### Command Syntax and Usage

---

#### **show dot1x information**

Displays 802.1X Information.

**Command mode:** All

For details, see [page 55](#).

---

#### **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 57](#).

---

**Table 16** 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 63](#).

---

**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 65](#).

---

**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 66](#).

---

**Table 16** Layer 2 Information Commands (continued)

---

**Command Syntax and Usage**

---

**show failover trigger** <1-8>

Displays Layer 2 Failover information.

**Command mode:** All

For details, see [page 48](#).

---

**show hotlinks information**

Displays Hot Links information.

**Command mode:** All

For details, see [page 50](#).

---

**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

---

## 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 17** 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, xxxxxxxxxxxx. 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 trunk** *<trunk number>*

Displays all FDB entries on a single trunk group.

**Command mode:** All

---

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

Displays all FDB entries on a single VLAN.

**Command mode:** All

---

**Table 17** FDB Information Commands (continued)**Command Syntax and Usage****show mac-address-table state {unknown|forward|trunk}**

Displays all FDB entries for a particular state.

**Command mode:** All**show mac-address-table**

Displays all entries in the Forwarding Database.

**Command mode:** AllFor more information, see [page 45](#).**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 354](#).

## Link Aggregation Control Protocol Information

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

**Table 18** LACP Information Commands

---

### Command Syntax and Usage

---

**show lacp aggregator** *<port alias or number>*

Displays detailed information about the LACP aggregator used by the selected port.

**Command mode:** All

---

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

Displays LACP information about the selected port.

**Command mode:** All

---

**show lacp information**

Displays a summary of LACP information.

**Command mode:** All

For details, see [page 47](#).

---

## 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 19** 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.

**Command mode:** All

For details, see [page 47](#).

---



## 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 20** 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 52](#).

---

**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 21** 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 22 OAM Discovery Information commands

---

Command Syntax and Usage

---

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

Displays OAM information about the selected port.

**Command mode:** All

---

**show oam**

Displays all OAM information.

**Command mode:** All

---

### OAM Port Information

The following command displays OAM information for the selected port:

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

**Command mode:** All

```
OAM information on port 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 23** 802.1X Parameter Descriptions

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



## Spanning Tree Information

The following command displays Spanning Tree information:

**show spanning-tree stp <1-/28> 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 60](#).

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

**Table 24** 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 25** 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 either 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 0		Port Hello EXT4 2		MaxAge 20		FwdDel 15	
Parameters:									
Priority 61440		Hello 2		MaxAge 20		FwdDel 15		Aging 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 26** 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 27** 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 27** 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 28** 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.

The following port-specific CIST information is also displayed:

**Table 29** CIST Parameter Descriptions

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



**Table 29** CIST Parameter Descriptions (continued)

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

## Trunk Group Information

The following command displays Trunk Group information:

**show portchannel information**

**Command mode:** All

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

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

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

## VLAN Information

Table 30 VLAN Information commands

Command Syntax and Usage

**show vlan** <VLAN number>

Displays general VLAN information.

**show vlan information**

Displays information about all VLANs, including:

- VLAN number and name
- Port membership
- Protocol VLAN status
- Private VLAN status
- Spanning Tree membership

The following command displays VLAN information:

**show vlan**

**Command mode:** All

VLAN	Name	Status	Bandwidth	MGT	Ports
1	Default VLAN	ena	ena	dis	INT1-INT14 EXT1-EXT6
10	VLAN 10	ena	ena	dis	INT1
11	VLAN 11	ena	ena	dis	EXT3
30	VLAN 30	ena	ena	dis	EXT4
4095	Mgmt VLAN	ena	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
- Bandwidth management status
- Management status of the VLAN
- Port membership of the VLAN
- Protocol-based VLAN information
- Private VLAN configuration

## Layer 3 Information

---

**Table 31** 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 71](#).

---

#### **show ip arp**

Displays Address Resolution Protocol (ARP) information.

**Command mode:** All

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

---

#### **show ip ospf information**

Displays the OSPF information.

**Command mode:** All

For details, see [page 77](#).

---

#### **show ip bgp information**

Displays Border Gateway Protocol (BGP) information.

**Command mode:** All

For details, see [page 77](#).

---

#### **show interface ip rip**

Displays RIP user's configuration.

**Command mode:** All

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

---

**Table 31** Layer 3 Information Commands (continued)

---

**Command Syntax and Usage**

---

**show ip information**

Displays IP Information. For details, see [page 70](#).

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 90](#).

---

**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 32** Route Information Commands

---

### Command Syntax and Usage

---

**show ip route address** *<IP address>*

Displays a single route by destination IP address.

**Command mode:** All

---

**show ip route gateway** *<IP address>*

Displays routes to a single gateway.

**Command mode:** All

---

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

Displays routes of a single type. For a description of IP routing types, see [Table 33 on page 71](#).

**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 34 on page 72](#).

**Command mode:** All

---

**show ip route interface** *<interface number>*

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 71](#).

---

## 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 33** 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 34** 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 GbE Switch Module.
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 36 on page 74](#)), VLAN and port for the address, and port referencing information.

**Table 35** 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 74](#).

---

**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 36** 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 37** BGP Peer Information Commands

---

### Command Syntax and Usage

---

#### **show ip bgp neighbor information**

Displays BGP peer information.

**Command mode:** All

See [page 76](#) 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 76](#) for a sample output.

---

#### **show ip bgp information**

Displays the BGP routing table.

**Command mode:** All

See [page 77](#) 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 0, TTL 1
  Remote AS: 0, Local AS: 0, Link type: IBGP
  Remote router ID: 0.0.0.0,   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: 0, Holdtime: 0, MinAdvTime: 60
  LastErrorCode: unknown(0), LastErrorSubcode: unspecified(0)
  Established state transitions: 0

4: 2.1.1.4          , version 0, TTL 1
  Remote AS: 0, Local AS: 0, Link type: IBGP
  Remote router ID: 0.0.0.0,   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: 0, Holdtime: 0, MinAdvTime: 60
  LastErrorCode: unknown(0), LastErrorSubcode: unspecified(0)
  Established state transitions: 0
```

BGP Summary information

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

**show ip bgp neighbor summary**

**Command mode:** All

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

## Dump BGP Information

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

**show ip bgp information**

**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 38** OSPF Information Commands

### Command Syntax and Usage

**show ip ospf general-information**

Displays general OSPF information.

**Command mode:** All

See [page 79](#) 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 80](#) for a sample output.

**Table 38** 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 82](#) 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 39** 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 39** 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 39** 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
```

## Routing Information Protocol

**Table 40** Routing Information Protocol Commands

---

### Command Syntax and Usage

---

#### **show ip rip routes**

Displays RIP routes.

**Command mode:** All

For more information, see [page 83](#).

---

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

Displays RIP user's configuration.

**Command mode:** All

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

---

### 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
```

## Interface Information

The following command displays interface information:

**show interface ip**

**Command mode:** All

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

For each interface, the following information is displayed:

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

## IP Information

The following command displays Layer 3 information:

**show layer3 information**

**Command mode:** All

```
IP information:
  AS number 0

Interface information:
  1: 201.201.27.2      255.255.255.0    201.201.27.255,  vlan 1, up
 128: 10.100.144.192  255.255.255.0    10.100.144.255,  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: 201.201.27.1,    vlan any, up active
 132: 10.100.144.190, vlan 4095, up active

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 41** 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 41** 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 GbE Switch Module 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 42 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 92](#).

---

## 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 43** 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 44** 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 45** ACL information commands

### Command Syntax and Usage

---

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

Displays ACL list information. For details, see [page 94](#).

**Command mode:** All

---

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

Displays ACL group information.

**Command mode:** All

---

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

Displays ACL block information.

**Command mode:** All

---

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

Displays ACL meter 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
  Actions     : Permit
No ACL groups configured.
```

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

Table 46 ACL Parameter Descriptions

Parameter	Description
Filter <i>x</i> profile	Indicates the ACL number.
Actions	Displays the configured action for the ACL.

# RMON Information Commands

---

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

**Table 47** RMON Information commands

Command Syntax and Usage	
<b>show rmon history</b>	Displays RMON History information. For details, see <a href="#">page 96</a> .
<b>Command mode:</b> All	
<b>show rmon alarm</b>	Displays RMON Alarm information. For details, see <a href="#">page 97</a> .
<b>Command mode:</b> All	
<b>show rmon event</b>	Displays RMON Event information. For details, see <a href="#">page 99</a> .
<b>Command mode:</b> All	
<b>show rmon</b>	Displays all RMON information.
<b>Command mode:</b> 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

The following table describes the RMON History Information parameters.

**Table 48** 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.



## RMON Alarm Information

The following command displays RMON Alarm information:

**show rmon alarm**

**Command mode:** All

RMON Alarm group configuration:							
Index	Interval	Type	rLimit	fLimit	rEvtIdx	fEvtIdx	last value
1	30	abs	10	0	1	0	0
2	900	abs	0	10	0	2	0
3	300	abs	10	20	0	0	0
4	1800	abs	10	0	1	0	0
5	1800	abs	10	0	1	0	0
8	1800	abs	10	0	1	0	56344540
10	1800	abs	10	0	1	0	0
11	1800	abs	10	0	1	0	0
15	1800	abs	10	0	1	0	0
18	1800	abs	10	0	1	0	0
100	1800	abs	10	0	1	0	0

  

Index	OID
1	1.3.6.1.2.1.2.2.1.10.257
2	1.3.6.1.2.1.2.2.1.11.258
3	1.3.6.1.2.1.2.2.1.12.259
4	1.3.6.1.2.1.2.2.1.13.260
5	1.3.6.1.2.1.2.2.1.14.261
8	1.3.6.1.2.1.2.2.1.10.280
10	1.3.6.1.2.1.2.2.1.15.262
11	1.3.6.1.2.1.2.2.1.16.263
15	1.3.6.1.2.1.2.2.1.19.266
18	1.3.6.1.2.1.2.2.1.10.279
100	1.3.6.1.2.1.2.2.1.17.264

The following table describes the RMON Alarm Information parameters.

**Table 49** 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.

**Table 49** RMON Alarm Parameter Descriptions (continued)

Parameter	Description
Type	<p>Displays the method of sampling the selected variable and calculating the value to be compared against the thresholds, as follows:</p> <ul style="list-style-type: none"> <li>□ <code>abs</code>—absolute value, the value of the selected variable is compared directly with the thresholds at the end of the sampling interval.</li> <li>□ <code>delta</code>—delta value, the value of the selected variable at the last sample is subtracted from the current value, and the difference compared with the thresholds.</li> </ul>
rLimit	Displays the rising threshold for the sampled statistic.
fLimit	Displays the falling threshold for the sampled statistic.
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.
Last value	Displays the last sampled value.
OID	Displays the MIB Object Identifier for each alarm index.

## RMON Event Information

The following command displays RMON Alarm information:

**show rmon alarm**

**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	
100	both	0D: 0H: 0M: 0S	Event_100	

The following table describes the RMON Event Information parameters.

**Table 50** 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: <i>none</i> , <i>log</i> , <i>trap</i> , <i>both</i> .
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.

## Link Status Information

The following command displays link information:

**show interface link**

**Command mode:** All except User EXEC

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	1000	any	yes	yes	up
EXT2	18	1000	any	yes	yes	up
EXT3	19	1000	any	yes	yes	up
EXT4	20	1000	any	yes	yes	up
EXT5	21	1000	any	yes	yes	up
EXT6	22	1000	any	yes	yes	up

**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 except User EXEC

Alias	Port	Tag	Fast	RMON	Lrn	Fld	PVID	NAME	VLAN(s)
INT1	1	y	n	d	e	e	1	INT1	1 4095
INT2	2	y	n	d	e	e	1	INT2	1 4095
INT3	3	y	n	d	e	e	1	INT3	1 4095
INT4	4	y	n	d	e	e	1	INT4	1 4095
INT5	5	y	n	d	e	e	1	INT5	1 4095
INT6	6	y	n	d	e	e	1	INT6	1 4095
INT7	7	y	n	d	e	e	1	INT7	1 4095
INT8	8	y	n	d	e	e	1	INT8	1 4095
INT9	9	y	n	d	e	e	1	INT9	1 4095
INT10	10	y	n	d	e	e	1	INT10	1 4095
INT11	11	y	n	d	e	e	1	INT11	1 4095
INT12	12	y	n	d	e	e	1	INT12	1 4095
INT13	13	y	n	d	e	e	1	INT13	1 4095
INT14	14	y	n	d	e	e	1	INT14	1 4095
MGT1	15	y	n	d	e	e	4095*	MGT1	4095
MGT2	16	y	n	d	e	e	4095*	MGT2	4095
EXT1	17	n	n	d	e	e	1	EXT1	1
EXT2	18	n	n	d	e	e	1	EXT2	1
EXT3	19	n	n	d	e	e	1	EXT3	1
EXT4	20	n	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)
- Whether the port has Port Fast Forwarding enabled (**F**ast)
- 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	FI-SFP	enabled	LOST	none
18 - EXT2	FI-SFP	enabled	LOST	none
19 - EXT3	FI-SFP	enabled	LOST	none
20 - EXT4	FI-SFP	enabled	LOST	none
21 - EXT5	FI-SFP	enabled	LOST	none
22 - EXT6	FI-SFP	enabled	LOST	none

## 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 51** 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 156](#) for sample output.

---

#### **show ntp counters**

Displays Network Time Protocol (NTP) Statistics.

**Command mode:** All

See [page 160](#) 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 161](#).

---

## Port Statistics

---

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

**Table 52** 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 106](#) for sample output.

---

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

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

**Command mode:** All

See [page 110](#) for sample output.

---

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

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

**Command mode:** All

See [page 111](#) for sample output.

---

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

Displays interface statistics for the port.

**Command mode:** All

See [page 114](#) for sample output.

---

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

Displays IP statistics for the port.

**Command mode:** All

See [page 116](#) for sample output.

---



**Table 52** Port Statistics Commands

---

**Command Syntax and Usage**

---

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

Displays link statistics for the port.

**Command mode:** AllSee [page 116](#) for sample output.

---

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

Displays Remote Monitoring (RMON) statistics for the port.

**Command mode:** AllSee [page 117](#) 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 53 802.1X 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 54** 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 54** 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 54** 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.

## 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 55** 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 56** 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 56** Ethernet Statistics for Port

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



Table 56 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

**Table 57** Interface Statistics for Port

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

**Table 57** Interface Statistics for Port

Statistics	Description
<code>ifInErrors</code>	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.
<code>ifOutOctets</code>	The total number of octets transmitted out of the interface, including framing characters.
<code>ifOutUcastPkts</code>	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.
<code>ifOutBroadcastPkts</code>	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> .
<code>ifOutMulticastPkts</code>	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> .
<code>ifOutFlowControlPkts</code>	The total number of flow control pause packets transmitted out of the interface.
<code>ifOutDiscards</code>	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.
<code>ifOutErrors</code>	For packet-oriented interfaces, the number of outbound packets that could not be transmitted because of errors. For character-oriented or fixed-length interfaces, the number of outbound transmission units that could not be transmitted because of errors.

## Interface Protocol Statistics

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

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

**Command mode:** All

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

**Table 58** 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 59** 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
etherStatsPkts640Octets:       0
etherStatsPkts1024to1518Octets: 0
```

**Table 60** RMON Statistics (/stats/port/rmon)

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 60** RMON Statistics (/stats/port/rmon)

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

**Table 60** RMON Statistics (/stats/port/rmon)

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

## Layer 2 Statistics

---

**Table 61** Layer 2 Statistics Commands

---

### Command Syntax and Usage

---

#### **show mac-address-table counters**

Displays FDB statistics.

**Command mode:** All

See [page 121](#) for sample output.

---

#### **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.

**Command mode:** All

See [page 122](#) for sample output.

---

#### **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.

**Command mode:** All except User EXEC

See [page 123](#) for sample output.

---

#### **clear hotlinks**

Clears all Hot Links statistics.

**Command mode:** All except User EXEC

---



**Table 61** Layer 2 Statistics Commands**Command Syntax and Usage****show interface port** *<port alias or number>* **lldp counters**

Displays LLDP statistics.

**Command mode:** All except User EXECSee [page 124](#) for sample output.**show oam counters**

Displays OAM statistics.

**Command mode:** All except User EXECSee [page 125](#) for sample output.**FDB Statistics**

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

**show mac-address-table counters****Command mode:** All

FDB statistics:			
current:	83	hiwat:	855

FDB statistics are described in the following table:

**Table 62** 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 63** 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 64** 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 65** LLDP port Statistics (/stats/l2/lldp)

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 66** 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.

**Command mode:** All

See [page 130](#) for sample output.

---

**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 ip route counters**

Displays route statistics.

**Command mode:** All

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

---

**show ip arp counters**

Displays Address Resolution Protocol (ARP) statistics.

**Command mode:** All

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

---

**show ip dns counters**

Displays Domain Name System (DNS) statistics.

**Command mode:** All

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

---

**Table 66** Layer 3 Statistics Commands

---

**Command Syntax and Usage**

---

**show ip icmp counters**

Displays ICMP statistics.

**Command mode:** All

See [page 135](#) for sample output.

---

**show ip tcp counters**

Displays TCP statistics.

**Command mode:** All

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

---

**show ip udp counters**

Displays UDP statistics.

**Command mode:** All

See [page 139](#) for sample output.

---

**show ip ospf counters**

Displays OSPF statistics.

**Command mode:** All

See [page 142](#) for sample output.

---

**show ip igmp counters**

Displays IGMP statistics.

**Command mode:** All

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

---

**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 66** 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:

**Command mode:** All

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

---

**show ip rip counters**

Displays Routing Information Protocol (RIP) statistics.

**Command mode:** All

See [page 148](#) for sample output.

---

**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 66** 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 67 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 67 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 67** 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).

## Route Statistics

The following command displays route statistics:

**show ip route counters**

**Command mode:** All

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

**Table 68** 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 69** ARP Statistics

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

## DNS Statistics

The following command displays Domain Name System statistics.

**show ip dns counters**

**Command mode:** All

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

**Table 70** DNS Statistics (/stats/dns)

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

## ICMP Statistics

The following command displays ICMP statistics:

**show ip icmp counters**

**Command mode:** All

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

**Table 71** 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 71** 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 72** TCP Statistics

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

**Table 72** 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 73** 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 74** 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 75 OSPF Statistics Commands

---

Command Syntax and Usage

---

**show ip ospf counters**

Displays OSPF statistics.

**Command mode:** All

See [page 142](#) 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 except User EXEC

```

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 76** OSPF General Statistics

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

Statistic	Description
<b>Nbr Change Stats:</b>	
hello	The sum total of all Hello packets received from neighbors on all OSPF areas and interfaces.
Start	The sum total number of neighbors in this state (that is, an indication that Hello packets should now be sent to the neighbor at intervals of <code>HelloInterval</code> seconds.) across all OSPF areas and interfaces.
n2way	The sum total number of bidirectional communication establishment between this router and other neighboring routers.
adjoint ok	The sum total number of decisions to be made (again) as to whether an adjacency should be established/maintained with the neighbor across all OSPF areas and interfaces.
negotiation done	The sum total number of neighbors in this state wherein the Master/slave relationship has been negotiated, and sequence numbers have been exchanged, across all OSPF areas and interfaces.
exchange done	The sum total number of neighbors in this state (that is, in an adjacency's final state) having transmitted a full sequence of Database Description packets, across all OSPF areas and interfaces.
bad requests	The sum total number of Link State Requests which have been received for a link state advertisement not contained in the database across all interfaces and OSPF areas.
bad sequence	<p>The sum total number of Database Description packets which have been received that either:</p> <ul style="list-style-type: none"> <li>a. Has an unexpected DD sequence number</li> <li>b. Unexpectedly has the init bit set</li> <li>c. Has an options field differing from the last Options field received in a Database Description packet.</li> </ul> <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 76** 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.
<b>Intf Change Stats:</b>	
hello	The sum total number of Hello packets sent on all interfaces and areas.
down	The sum total number of interfaces down in all OSPF areas.
loop	The sum total of interfaces no longer connected to the attached network across all OSPF areas and interfaces.
unloop	The sum total number of interfaces, connected to the attached network in all OSPF areas.
wait timer	The sum total number of times the Wait Timer has been fired, indicating the end of the waiting period that is required before electing a (Backup) Designated Router across all OSPF areas and interfaces.
backup	The sum total number of Backup Designated Routers on the attached network for all OSPF areas and interfaces.
nbr change	The sum total number of changes in the set of bidirectional neighbors associated with any interface across all OSPF areas.

**Table 76** OSPF General Statistics

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

## 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 77** 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 78** 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 150](#).

---

### **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 152](#).

---

### **show mp udp-block**

Displays all UDP control blocks that are in use.

**Command mode:** All

To view a sample output, see [page 152](#).

---

### **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 153](#).

---

## 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 79** Packet Statistics (/stats/mp/pkt)

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.
<b>small packet buffers</b>	
current	Total number of packet allocations with size less than 128 bytes from the packet buffer pool by the TCP/IP protocol stack.
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 79** Packet Statistics (/stats/mp/pkt)

Statistics	Description
hi-water time	Time stamp that indicates when the hi-watermark was reached.
<b>medium packet buffers</b>	
current	Total number of packet allocations with size between 128 to 1536 bytes from the packet buffer pool by the TCP/IP protocol stack.
hi-watermark	The highest number of packet allocation with size between 128 to 1536 bytes from the packet buffer pool by the TCP/IP protocol stack.
hi-water time	Time stamp that indicates when the hi-watermark was reached.
<b>jumbo packet buffers</b>	
current	Total number of packet allocations with more than 1536 bytes from the packet buffer pool by the TCP/IP protocol stack.
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 80 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 81** 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 82 ACL Statistics Commands

## Command Syntax and Usage

**show access-control list <1-4096> counters**

Displays the Access Control List Statistics for a specific ACL.

**Command mode:** All

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

Displays statistics for a specific ACL Meter.

**Command mode:** All

For details, see [page 155](#).

**show access-control counters**

Displays all ACL statistics.

**Command mode:** All except User EXEC

**clear access-control list**

Clears ACL statistics.

**Command mode:** All except User EXEC

**clear access-control meter counters**

Clears ACL metering statistics.

**Command mode:** All except User EXEC

## ACL Statistics

This option displays statistics for the selected ACL.

**show access-control <1-4096> counters**

**Command mode:** All

Hits for ACL 1, port EXT1:	26057515
Hits for ACL 2, port EXT1:	26057497

## ACL Meter Statistics

This option displays ACL meter statistics.

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

**Command mode:** All

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

# SNMP Statistics

The following command displays SNMP statistics:

**show snmp-server counters**

**Command mode:** All except User EXEC

SNMP statistics:			
snmpInPkts:	150097	snmpInBadVersions:	0
snmpInBadC'tyNames:	0	snmpInBadC'tyUses:	0
snmpInASNParseErrs:	0	snmpEnableAuthTraps:	0
snmpOutPkts:	150097	snmpInBadTypes:	0
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 83 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 83** 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><b>Note:</b> OSI's method of specifying abstract objects is called ASN.1 (Abstract Syntax Notation One, defined in X.208), and one set of rules for representing such objects as strings of ones and zeros is called the BER (Basic Encoding Rules, defined in X.209). ASN.1 is a flexible notation that allows one to define a variety of data types, from simple types such as integers and bit strings to structured types such as sets and sequences. BER describes how to represent or encode values of each ASN.1 type as a string of eight-bit octets.</p>
snmpEnableAuthTraps	An object to enable or disable the authentication traps generated by this entity (the switch).
snmpOutPkts	The total number of SNMP Messages which were passed from the SNMP protocol entity to the transport service.
snmpInBadTypes	The total number of SNMP Messages which failed ASN parsing.
snmpInTooBig	The total number of SNMP Protocol Data Units (PDUs) which were delivered to the SNMP protocol entity and for which the value of the error-status field is <i>too big</i> .
snmpInNoSuchNames	The total number of SNMP Protocol Data Units (PDUs) which were delivered to the SNMP protocol entity and for which the value of the error-status field is <i>noSuchName</i> .
snmpInBadValues	The total number of SNMP Protocol Data Units (PDUs) which were delivered to the SNMP protocol entity and for which the value of the error-status field is <i>badValue</i> .
snmpInReadOnly	The total number of valid SNMP Protocol Data Units (PDUs), which were delivered to the SNMP protocol entity and for which the value of the error-status field is <i>'read-Only'</i> . It should be noted that it is a protocol error to generate an SNMP PDU, which contains the value <i>'read-Only'</i> in the error-status field. As such, this object is provided as a means of detecting incorrect implementations of the SNMP.
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 83** 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 83** 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 server.
  Last update time: 18:04:16 Tue Jul 13, 2009
  Current system time: 18:55:49 Tue Jul 13, 2009
```



**Table 84** NTP Statistics

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

## 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 85** General Configuration Commands

---

### Command Syntax and Usage

---

#### **show running-config**

Dumps current configuration to a script file.

**Command mode:** All

For details, see [page 338](#).

---

#### **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 338](#).

---

#### **copy running-config startup-config**

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

**Command mode:** All

---

Table 85 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 339](#).

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 350](#).

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

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

**Command mode:** Global configuration

---

**Table 86** System Configuration Commands

---

**Command Syntax and Usage**

---

**system flow-control end-to-end**

Enables or disables End-to-End flow control mode. The default value is **enabled**. If you change the flow-control mode, you must apply and save the changes, then reboot the switch before the change takes effect.

The GbE switch module has two switching chips connected by an internal high-capacity link (Higig). Over subscription of traffic across the Higig link is handled by one of the following flow control modes:

- ☐ End-to-End (E2E) Flow Control
- ☐ Ingress Back Pressure (IBP) across the Higig link

One of the modes should be enabled, and the other mode disabled. E2E flow control works best for most applications. E2E provides a higher throughput and better overall switch performance, but does not provide lossless flow control.

**Command mode:** Global configuration

---

**system flow-control higig-ibp**

Enables or disables Higig Ingress Back Pressure (IBP) flow control mode. The default value is **disabled**. If you change the flow-control mode, you must apply and save the changes, then reboot the switch before the change takes effect.

The GbE switch module has two switching chips connected by an internal high-capacity link (Higig). Over subscription of traffic across the Higig link is handled by one of the following flow control modes:

- ☐ End-to-End (E2E) Flow Control
- ☐ Ingress Back Pressure (IBP) across the Higig link

One of the modes should be enabled, and the other mode disabled. Applications that cannot tolerate packet loss might require IBP across the Higig link. Higig IPB achieves lossless operation, but it might result in a lower throughput.

**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

---

**Table 86** System Configuration Commands

---

**Command Syntax and Usage**

---

**[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

---

**show system**

Displays the current system parameters.

**Command mode:** All

---

## System Host Log Configuration

**Table 87** 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

---

Table 87 Host Log Configuration Commands

Command Syntax and Usage
<b>no logging console</b>  Disables delivering syslog messages to the console. When necessary, disabling <code>console</code> ensures the switch is not affected by syslog messages. It is enabled by default.  <b>Command mode:</b> Global configuration
<b>[no] logging log [&lt;feature&gt;]</b>  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 servers), or enable/disable syslog on all available features.  <b>Command mode:</b> Global configuration
<b>show logging</b>  Displays the current syslog settings.  <b>Command mode:</b> All



## SSH Server Configuration

For the GbE Switch Module, these commands enable Secure Shell access from any SSH client.

**Table 88** 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 88** SSH Server Configuration Commands

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

## RADIUS Server Configuration

**Table 89** 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 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 89** 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 logon password to an authentication server to determine whether access can be allowed to a given system. TACACS is an encryption protocol, and therefore less secure than TACACS+ and Remote Authentication Dial-In User Service (RADIUS) protocols. (Both TACACS and TACACS+ are described in RFC 1492.)

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

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

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

**Table 90** 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 90** 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 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 90** 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 90** 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 91** 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 91** LDAP Configuration commands

---

**Command Syntax and Usage**

---

**[no] ldap-server backdoor**

Enables or disables the LDAP backdoor for telnet. The `telnet` command also applies to SSH/SCP connections and the Browser-Based Interface (BBI). The default is `disabled`.

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

**Command mode:** Global configuration

---

**ldap-server enable**

Enables the LDAP server.

**Command mode:** Global configuration

---

**no ldap-server enable**

Disables the LDAP server.

**Command mode:** Global configuration

---

**show ldap-server**

Displays the current LDAP server parameters.

**Command mode:** All

---

## NTP 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 92** 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 92 NTP Configuration Commands

Command Syntax and Usage
<b>ntp enable</b> Enables the NTP synchronization service. <b>Command mode:</b> Global configuration
<b>no ntp enable</b> Disables the NTP synchronization service. <b>Command mode:</b> Global configuration
<b>show ntp</b> Displays the current NTP service settings. <b>Command mode:</b> 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 93** 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 93** 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 RFC2271 to RFC2276.

**Table 94** SNMPv3 Configuration Commands

Command Syntax and Usage
<b>snmp-server user</b> <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.  <b>Command mode:</b> Global configuration  To view command options, see <a href="#">page 185</a> .
<b>snmp-server view</b> <1-128>  This command allows you to create different MIB views.  <b>Command mode:</b> Global configuration  To view command options, see <a href="#">page 186</a> .
<b>snmp-server access</b> <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.  <b>Command mode:</b> Global configuration  To view command options, see <a href="#">page 188</a> .

**Table 94** 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 190](#).

---

**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 191](#).

---

**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 192](#).

---

**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 193](#).

---

**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 195](#).

---



**Table 94** 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 95** 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 95 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

Table 96 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 96** 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 97** 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 97** 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 98** 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 185](#):

**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 185](#).

**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 99** 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 185](#):

`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 100** 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>

Allows you to configure a transport address IP that can be used in the generation of SNMP 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 193](#):  
snmp-server target-parameters <1-16> name <1-32 characters>

**Command mode:** Global configuration

---



**Table 100** 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 101** 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 101 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 185) 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 102** 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 103** 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 103** System Access Configuration Commands

---

**Command Syntax and Usage**

---

**[no] access userbbi**

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 104** 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 104 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 105 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 105** 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 106** 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 106 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 107 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.

**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.

**Command mode:** Global configuration



**Table 107** Strong Password Configuration Commands

<b>Command Syntax and Usage</b>	
<b>access user strong-password faillog</b> <1-255>	
Configures the number of failed login attempts allowed before a security notification is logged.	
<b>Command mode:</b> Global configuration	
<b>show access user strong-password</b>	
Displays the current Strong Password configuration.	
<b>Command mode:</b> All except User EXEC	

## HTTPS Access Configuration

**Table 108** 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.

**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 109** 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)

**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)

**Command mode:** Global configuration

---

**system custom-dst enable**

Enables the Custom Daylight Savings Time settings.

**Command mode:** Global configuration

---

Table 109 Custom DST Configuration Commands

Command Syntax and Usage
<b>no system custom-dst enable</b> Disables the Custom Daylight Savings Time settings. <b>Command mode:</b> Global configuration
<b>show custom-dst</b> Displays the current Custom DST configuration. <b>Command mode:</b> All except User EXEC

sFlow Configuration

sFlow is a sampling method used for monitoring high speed switched networks. Use these commands to configure the sFlow agent on the switch.

Table 110 sFlow Configuration commands

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

## sFlow Port Configuration

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

**Table 111** sFlow Port Configuration commands

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

# Port Configuration

Use the Port Configuration commands to configure settings for switch ports (INTx) and (EXTx).

**Table 112** 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] rmon**

Enables or disables Remote Monitoring for the port. RMON must be enabled for any RMON configurations to function.

**Command mode:** Interface port

---

**[no] dscp-marking**

Enables or disables DSCP re-marking on a port.

**Command mode:** Interface port

---

**[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

---

**Table 112** Port Configuration Commands

---

**Command Syntax and Usage**

---

**[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] broadcast-threshold <0-262143>**

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

**Command mode:** Interface port

---

**[no] multicast-threshold <0-262143>**

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

**Command mode:** Interface port

---

**[no] dest-lookup-threshold <0-262143>**

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

**Command mode:** Interface port

---

Table 112 Port Configuration Commands

Command Syntax and Usage
<b>no shutdown</b>  Enables the port.  <b>Command mode:</b> Interface port
<b>shutdown</b>  Disables the port. (To temporarily disable a port without changing its configuration attributes, refer to <a href="#">“Temporarily Disabling a Port” on page 209.</a> )  <b>Command mode:</b> Interface port
<b>show interface port</b> <i>&lt;port alias or number&gt;</i>  Displays current port parameters.  <b>Command mode:</b> All

## Port Link Configuration

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

Table 113 Port Link Configuration Commands

Command Syntax and Usage
<b>speed</b> {10 100 1000 10000 auto}  Sets the link speed. Some options are not valid on all ports. The choices include: <ul style="list-style-type: none"><li><input type="checkbox"/> 10 Mbps</li><li><input type="checkbox"/> 100 Mbps</li><li><input type="checkbox"/> 1000 Mbps</li><li><input type="checkbox"/> 10000 Mps</li><li><input type="checkbox"/> any (auto negotiate port speed)</li></ul> <b>Command mode:</b> Interface port
<b>duplex</b> {full half any}  Sets the operating mode. The choices include: <ul style="list-style-type: none"><li><input type="checkbox"/> “Any,” for auto negotiation (default)</li><li><input type="checkbox"/> Half-duplex</li><li><input type="checkbox"/> Full-duplex</li></ul> <b>Command mode:</b> Interface port



Table 113 Port Link Configuration Commands

Command Syntax and Usage

**[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.

**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 GbE Switch Module is reset. See the [“Operations Commands” on page 341](#) for other operations-level commands.

## UniDirectional Link Detection Configuration

UDLD commands are described in the following table.

**Table 114** Port UDLD Configuration commands

Command Syntax and Usage
<div><div>[no] udld</div><div>Enables or disables UDLD on the port.</div><div>Command mode: Interface port</div></div>
<div><div>[no] udld aggressive</div><div>Configures the UDLD mode for the selected port, as follows:</div><div><div><div><input type="checkbox"/> Normal:</div><div>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.</div></div><div><div><input type="checkbox"/> Aggressive:</div><div>In addition to the normal mode, the aggressive mode disables the port if the neighbor stops sending UDLD probes for 7 seconds.</div></div></div><div>Command mode: Interface port</div></div>
<div><div>show udld</div><div>Displays current port UDLD parameters.</div><div>Command mode: All</div></div>

## 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 115** Port OAM Configuration commands

---

### Command Syntax and Usage

---

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

Configures the OAM discovery mode, as follows:

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

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

**Command mode:** Interface port

---

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

Disables OAM discovery on the port.

**Command mode:** Interface port

---

#### **show oam**

Displays current port OAM parameters.

**Command mode:** All

---

## ACL Port Configuration

**Table 116** ACL/QoS Configuration Commands

---

### Command Syntax and Usage

---

#### **access-control list <1-4096>**

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 <1-4096>**

Deletes the specified ACL list from the port.

**Command mode:** Interface port

---

Table 116 ACL/QoS Configuration Commands

Command Syntax and Usage

**access-control block** <1-4096>

Adds the specified ACL Block to the port. You can add multiple ACL Blocks to a port.

**Command mode:** Interface port

**no access-control block** <1-4096>

Deletes the specified ACL Block from the port.

**Command mode:** Interface port

**access-control group** <1-4096>

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** <1-4096>

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

ACL Port Metering Commands

These commands define the Access Control profile for the selected ACL group on the port.

Table 117 Metering Command Options

Command Syntax and Usage

**access-control meter** <1-127> **committed-rate** <1000-1000000>

Configures the committed rate, in Kilobits per second. The committed rate must be a multiple of 64.

**Command mode:** Interface port

**access-control meter** <1-127> **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:** Interface port

**Table 117** Metering Command Options**Command Syntax and Usage**


---

**[no] access-control meter** <1-127> **enable**

Enables or disables ACL Metering on the port.

**Command mode:** Interface port

---

**access-control meter** <1-127> **action** {drop|pass}

Configures the ACL Meter to either drop or pass out-of-profile traffic.

**Command mode:** Interface port

---

**access-control meter** <1-127> {list|block|group} <1-4096>

Adds an ACL, ACL Block, or ACL Group to the ACL Meter on this port.

**Command mode:** Interface port

---

**no access-control meter** <1-127> {list|block|group} <1-4096>

Removes an ACL, ACL Block, or ACL Group from the ACL Meter on this port.

**Command mode:** Interface port

---

**default access-control meter** <1-127>

Reset ACL Metering parameters to their default values.

**Command mode:** Interface port

---

**show interface port** {<port alias or number>}

Displays current port configuration parameters.

**Command mode:** All

---

Re-Marking Commands

You can choose to re-mark IP header data for the selected ACL Group on the port. 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 118 Re-Mark Command Options

Command Syntax and Usage	
<b>access-control re-mark</b> <i>&lt;1-127&gt;</i> { <b>list group block</b> } <i>&lt;1-4096&gt;</i>	Assign an ACL, ACL Block, or ACL Group for DSCP remarking on this port.  <b>Command mode:</b> Interface port
<b>no access-control re-mark</b> <i>&lt;1-127&gt;</i> { <b>list block group</b> } <i>&lt;1-4096&gt;</i>	Removes an ACL, ACL Block, or ACL Group from DSCP remarking on this port.  <b>Command mode:</b> Interface port
<b>default access-control re-mark</b> <i>&lt;1-127&gt;</i>	Resets ACL Re-Mark parameters to their default values.  <b>Command mode:</b> Interface port
<b>show interface port</b> { <i>&lt;port alias or number&gt;</i> }	Displays current port configuration parameters.  <b>Command mode:</b> All

## Re-Marking In-Profile Commands

**Table 119** Re-Mark In-Profile Commands

---

### Command Syntax and Usage

---

**access-control re-mark** <1-127> **in-profile dscp** <0-63>

Sets the DiffServ Code Point (DSCP) of In-Profile packets to the selected value.

**Command mode:** Interface port

---

**default access-control re-mark** <1-127>

Resets the update DSCP parameters to their default values.

**Command mode:** Interface port

---

**show interface port** {<port alias or number>}

Displays current port configuration parameters.

**Command mode:** All

---

## Update User Priority Commands

**Table 120** User Priority Commands

---

### Command Syntax and Usage

---

**access-control re-mark** <1-127> **dot1p** <0-7>

Defines 802.1p value. The value is the priority bits information in the packet structure.

**Command mode:** Interface port

---

**[no] access-control re-mark** <1-127> **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:** Interface port

---

**default access-control re-mark** <1-127>

Resets UP1P settings to their default values.

**Command mode:** Interface port

---

**show interface port** {<port alias or number>}

Displays current port configuration parameters.

**Command mode:** All

---

## Re-Marking Out-of-Profile Commands

Table 121 Out-of-Profile Commands

Command Syntax and Usage
<b>access-control re-mark</b> <1-127> <b>out-profile dscp</b> <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.  <b>Command mode:</b> Interface port
<b>default access-control re-mark</b> <1-127>  Resets the update DSCP parameters for Out-of-Profile packets to their default values.  <b>Command mode:</b> Interface port
<b>show interface port</b> {<port alias or number>}  Displays current port configuration parameters.  <b>Command mode:</b> All

## Port Spanning Tree Configuration

Table 122 Port STP Options

Command Syntax and Usage
<b>[no] spanning-tree edge</b>  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).  <b>Command mode:</b> Interface port



**Table 122** Port STP Options

---

**Command Syntax and Usage**

---

**[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).

**Command mode:** Interface port

---

**show interface port {<port alias or number>}**

Displays current port configuration parameters.

**Command mode:** All

---

# 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 123 802.1p 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

---

**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.

**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 124** 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

---

**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.

**Table 125** General ACL Configuration Commands

---

**Command Syntax and Usage**

---

**[no] access-control list** <1-4096>

Configures an Access Control List.

**Command mode:** Global configuration

To view command options, see [page 221](#).

---

**[no] access-control group** <1-4096>

Configures an ACL Group.

**Command mode:** Global configuration

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

---

**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 126** ACL Configuration Commands

---

### Command Syntax and Usage

---

**[no] access-control list <1-4096> egress-port <port alias or number>**

Configures the ACL to function on egress packets.

**Command mode:** Global configuration

---

**access-control list <1-4096> 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 <1-4096> statistics**

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

**Command mode:** All except User EXEC

---

**default access-control list <1-4096>**

Resets the ACL parameters to their default values.

**Command mode:** Global configuration

---

**show access-control list <1-4096>**

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 127** Ethernet Filtering Configuration Commands

---

### Command Syntax and Usage

---

**[no] access-control list <1-4096> ethernet source-mac-address**  
*<MAC address> <MAC mask>*

Defines the source MAC address for this ACL.

**Command mode:** Global configuration

---

**[no] access-control list <1-4096> ethernet destination-mac-address**  
*<MAC address> <MAC mask>*

Defines the destination MAC address for this ACL.

**Command mode:** Global configuration

---

**[no] access-control list <1-4096> ethernet vlan <VLAN ID> <VLAN mask>**

Defines a VLAN number and mask for this ACL.

**Command mode:** Global configuration

---

**[no] access-control list <1-4096> ethernet ethernet-type**  
*{arp|ip|ipv6|mpls|rarp|any|<other (0xXXXX)>}*

Defines the Ethernet type for this ACL.

**Command mode:** Global configuration

---

**[no] access-control list <1-4096> ethernet priority <0-7>**

Defines the Ethernet priority value for the ACL.

**Command mode:** Global configuration

---

**default access-control list <1-4096> ethernet**

Resets Ethernet parameters for the ACL to their default values.

**Command mode:** Global configuration

---

**Table 127** Ethernet Filtering Configuration Commands**Command Syntax and Usage**


---

**no access-control list** <1-4096> **ethernet**

Removes Ethernet parameters for the ACL.

**Command mode:** Global configuration

---

**show access-control list** <1-4096> **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 128** IP version 4 Filtering Configuration Commands**Command Syntax and Usage**


---

**[no] access-control list** <1-4096> **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** <1-4096> **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 128 IP version 4 Filtering Configuration Commands

Command Syntax and Usage

**[no] access-control list <1-4096> 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 <1-4096> 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 <1-4096> ipv4**

Resets the IPv4 parameters for the ACL to their default values.

**Command mode:** Global configuration

**show access-control list <1-4096> 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 129** TCP/UDP Filtering Configuration Commands

Command Syntax and Usage	
<b>[no] access-control list &lt;1-4096&gt; tcp-udp source-port &lt;1-65535&gt; &lt;mask (0xFFFF)&gt;</b>	
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:	
<b>Number</b>	<b>Name</b>
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
<b>Command mode:</b> Global configuration	
<b>[no] access-control list &lt;1-4096&gt; tcp-udp destination-port &lt;1-65535&gt; &lt;mask (0xFFFF)&gt;</b>	
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.	
<b>Command mode:</b> Global configuration	
<b>[no] access-control list &lt;1-4096&gt; tcp-udp flags &lt;flag (0x0-0x3f)&gt;</b>	
Defines a TCP/UDP flag for the ACL.	
<b>Command mode:</b> Global configuration	

**Table 129** TCP/UDP Filtering Configuration Commands**Command Syntax and Usage****default access-control list** <1-4096> **tcp-udp**

Resets the TCP/UDP parameters for the ACL to their default values.

**Command mode:** Global configuration**show access-control list** <1-4096> **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 130** Packet Format Filtering Configuration Commands**Command Syntax and Usage****access-control list** <1-4096> **packet-format ethernet** {**ethertype2** | **snap** | **llc**}

Defines the Ethernet format for the ACL.

**Command mode:** Global configuration**[no] access-control list** <1-4096> **packet-format tagged**

Defines the tagging format for the ACL.

**Command mode:** Global configuration**[no] access-control list** <1-4096> **packet-format ip** {**ipv4** | **ipv6**}

Defines the IP format for the ACL.

**Command mode:** Global configuration**default access-control list** <1-4096> **packet-format**

Resets Packet Format parameters for the ACL to their default values.

**Command mode:** Global configuration**show access-control list** <1-4096> **packet-format**

Displays the current Packet Format parameters for the ACL.

**Command mode:** All except User EXEC

## ACL Block Configuration

These commands allows you to compile one or more ACLs into an ACL Block. Each ACL in the ACL Block must fall within the same mask.

**Table 131** ACL Block Configuration Commands

---

### Command Syntax and Usage

---

**access-control block** <1-4096> <1-4096>

Adds the selected ACL to the ACL Block.

**Command mode:** Global configuration

---

**no access-control block** <1-4096> <1-4096>

Removes the selected ACL from the ACL Block.

**Command mode:** Global configuration

---

**show access-control block** <1-4096>

Displays the current ACL block parameters.

**Command mode:** Global configuration

---

## 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 132** ACL Group Configuration Commands

---

### Command Syntax and Usage

---

**access-control group** <1-4096> **list** <1-4096>

Adds the selected ACL to the ACL Group.

**Command mode:** Global configuration

---

**no access-control group** <1-4096> **list** <1-4096>

Removes the selected ACL from the ACL Group.

**Command mode:** Global configuration

---

**show access-control group** <1-4096>

Displays the current ACL group parameters.

**Command mode:** All except User EXEC

---

# Port Mirroring

---

Port mirroring is disabled by default. For more information about port mirroring on the GbESM, see “Appendix A: Troubleshooting” in the *BLADEOS 5.1 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 133** 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 134 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 135** 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 268](#).

---

**[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] spanning-tree bpdu-guard**

Enables or disables BPDU guard, to avoid spanning-tree loops on ports with Port Fast Forwarding enabled.

**Command mode:** Global configuration

---

Table 135 Layer 2 Configuration Commands

Command Syntax and Usage

**[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 136 802.1x 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 137** 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

---

**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

---



**Table 137** 802.1X Global Configuration Commands

---

**Command Syntax and Usage**

---

**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

---

**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 138** 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 139** 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 139** 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

**default dot1x**

Resets the 802.1X port parameters to their default values.

**Command mode:** Interface port

Table 139 802.1X Port Commands

Command Syntax and Usage	
<b>dot1x apply-global</b>	Applies current global 802.1X configuration parameters to the port. <b>Command mode:</b> Interface port
<b>show interface port</b> <i>&lt;port alias or number&gt;</i> <b>dot1x</b>	Displays current 802.1X port parameters. <b>Command mode:</b> 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. MSTP is turned off by default.

---

**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 140** 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 140** 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 141](#) 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 141** 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 142** CIST Bridge Configuration Commands

Command Syntax and Usage
<b>spanning-tree mstp cist-bridge priority &lt;0-65535&gt;</b>  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.  <b>Command mode:</b> Global configuration
<b>spanning-tree mstp cist-bridge maximum-age &lt;6-40&gt;</b>  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.  <b>Command mode:</b> Global configuration
<b>spanning-tree mstp cist-bridge forward-delay &lt;4-30&gt;</b>  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.  <b>Command mode:</b> Global configuration
<b>show spanning-tree mstp cist</b>  Displays the current CIST bridge configuration.  <b>Command mode:</b> 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 143** CIST Port Configuration Commands

---

### Command Syntax and Usage

---

**spanning-tree mstp cist interface-priority** <0-240>

Configures the CIST port priority. The port priority helps determine which bridge port becomes the designated port. In a network topology that has multiple bridge ports connected to a single segment, the port with the lowest port priority becomes the designated port for the segment.

The range is 0 to 240, in steps of 16 (0, 16, 32...), and the default is 128.

**Command mode:** Interface port

---

**spanning-tree mstp cist path-cost** <0-200000000>

Configures the CIST port path cost. The port path cost is used to help determine the designated port for a segment. Port path cost is based on the port speed, and is calculated as follows:

- 100Mbps = 200000
- 1Gbps = 20000
- 10Gbps = 2000

The default value of 0 (zero) indicates that the default path cost will be computed for an auto negotiated link speed.

**Command mode:** Interface port

---

**spanning-tree mstp cist hello** <1-10>

Configures the CIST port Hello time. The Hello time specifies how often the root bridge transmits a configuration bridge protocol data unit (BPDU). Any bridge that is not the root bridge uses the root bridge Hello value. The range is 1 to 10 seconds, and the default is 2 seconds.

**Command mode:** Interface port

---

**Table 143** 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 144** 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 an external 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 an external 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 145** 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 145** 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

The **port** option of STG is turned on by default.

**Table 146** 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...) and the default is 128.

**Command mode:** Interface port

---

**spanning-tree stp** <STG number> **path-cost** <1-65535, 0 for default>

Configures the port path cost. The port path cost is used to help determine the designated port for a segment. Port path cost is based on the port speed, and is calculated as follows:

- 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** <STG number> **link** {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** <STG number> **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 146 Spanning Tree Port Commands

Command Syntax and Usage
<b>spanning-tree stp</b> <i>&lt;STG number&gt;</i> <b>enable</b> Enables STG on the port. <b>Command mode:</b> Interface port
<b>no spanning-tree stp</b> <i>&lt;STG number&gt;</i> <b>enable</b> Disables STG on the port. <b>Command mode:</b> Interface port
<b>show interface port</b> <i>&lt;port alias or number&gt;</i> <b>spanning-tree stp</b> <i>&lt;STG number&gt;</i> Displays the current STG port parameters. <b>Command mode:</b> All

## Forwarding Database Configuration

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

Table 147 FDB configuration commands

Command Syntax and Usage
<b>mac-address-table aging</b> <i>&lt;0-65535&gt;</i> Configures the aging value for FDB entries, in seconds. The default value is 300. <b>Command mode:</b> Global configuration
<b>[no] mac-address-table learning</b> Enables or disables FDB learning. The default value is enabled. <b>Command mode:</b> Global configuration

Table 147 FDB configuration commands

Command Syntax and Usage

[no] mac-address-table dropping

Enables or disables flooding of packets with unknown MAC addresses to all switch ports. The default value is `enabled`.

**Note:** If you disable FDB flooding, you must also disable FDB learning.

**Command mode:** Global configuration

show mac-address-table

Display current FDB configuration.

**Command mode:** All except User EXEC

**Note –** If you disable FDB learning and FDB flooding, manually add static MAC address entries for the management module, blade servers, and other connected devices. The static entries ensure that the GbESM retains connectivity to those devices.

Static FDB Configuration

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

Table 148 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



**Table 148** FDB configuration commands

---

**Command Syntax and Usage**

---

**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

---

## LLDP Configuration

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

**Table 149** 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 149 LLDP commands

Command Syntax and Usage	
<b>lldp reinit-delay</b> <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.	
<b>Command mode:</b> Global configuration	
<b>lldp enable</b>	
Globally turns LLDP on. The default setting is <b>on</b> .	
<b>Command mode:</b> Global configuration	
<b>no lldp enable</b>	
Globally turns LLDP off.	
<b>Command mode:</b> Global configuration	
<b>show lldp</b>	
Display current LLDP configuration.	
<b>Command mode:</b> All	

## LLDP Port Configuration

Use the following commands to configure LLDP port options.

**Table 150** 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 151** 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 151** 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 151** 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 GbE Switch Modules 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 13 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 152** Trunk Configuration Commands

Command Syntax and Usage	
<b>portchannel</b> <1-13> <b>member</b> <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 ( , ).	
<b>Command mode:</b> Global configuration	
<b>no portchannel</b> <1-13> <b>member</b> <port alias or number>	
Removes a physical port from the current trunk group.	
<b>Command mode:</b> Global configuration	
<b>[no] portchannel</b> <1-13> <b>enable</b>	
Enables or Disables the current trunk group.	
<b>Command mode:</b> Global configuration	
<b>no portchannel</b> <1-13>	
Removes the current trunk group configuration.	
<b>Command mode:</b> Global configuration	
<b>show portchannel</b> <1-13>	
Displays current trunk group parameters.	
<b>Command mode:</b> All	

## IP Trunk Hash Configuration

Use the following commands to configure IP trunk hash settings for the GbESM. The trunk hash settings affect both static trunks and LACP trunks.

**Table 153** IP Trunk Hash commands

---

### Command Syntax and Usage

---

#### **show portchannel hash**

Display current trunk hash configuration.

**Command mode:** All

---

## Layer 2 IP Trunk Hash Configuration

Trunk hash parameters are set globally for the GbESM. You can enable one or two 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 layer 2 IP trunk hash parameters for the GbESM.

**Table 154** Layer 2 IP Trunk Hash commands

---

### 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

---

**Table 154** Layer 2 IP Trunk Hash commands

---

**Command Syntax and Usage**

---

**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 Layer 2 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 155** 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

---

**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 156** 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 LACPDU.
- ❑ **passive**  
Turn LACP on and set this port to passive. Passive ports do not initiate LACPDU, but respond to LACPDU from active ports.

**Command mode:** Interface port

---

**lacp priority** <1-65535>

Sets the priority value for the selected port. Lower numbers provide higher priority. The default value is 32768.

**Command mode:** Interface port

---

**lacp key** <1-65535>

Set the admin key for this port. Only ports with the same *admin key* and *oper key* (operational state generated internally) can form a LACP trunk group.

**Command mode:** Interface port

---

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

Displays the current LACP configuration for this port.

**Command mode:** All

---

## Layer 2 Failover Configuration

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

**Table 157** 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 158** Failover Trigger Configuration Commands

<b>Command Syntax and Usage</b>	
<b>[no] failover trigger &lt;1-8&gt; enable</b>	
Enables or disables the Failover trigger.	
<b>Command mode:</b> Global configuration	
<b>no failover trigger &lt;1-8&gt;</b>	
Deletes the Failover trigger.	
<b>Command mode:</b> Global configuration	
<b>failover trigger &lt;1-8&gt; limit &lt;0-1024&gt;</b>	
Configures the minimum number of operational links allowed within each trigger before the trigger initiates a failover event. If you enter a value of zero (0), the switch triggers a failover event only when no links in the trigger are operational.	
<b>Command mode:</b> Global configuration	
<b>show failover trigger &lt;1-8&gt;</b>	
Displays the current failover trigger settings.	
<b>Command mode:</b> All except User EXEC	

## Auto Monitor Configuration

**Table 159** Auto Monitor Configuration Commands

---

### Command Syntax and Usage

---

**failover trigger** <1-8> **amon trunk** <trunk number>

Adds a trunk group to the Auto Monitor.

**Command mode:** Global configuration

---

**no failover trigger** <1-8> **amon trunk** <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 - Monitor Configuration

Use these commands to define the port link(s) to monitor. The Manual Monitor - Monitor configuration accepts only external uplink ports.

---

**Note** – AMON and MMON configurations are mutually exclusive.

---

**Table 160** Failover Manual Monitor - Monitor commands

---

### Command Syntax and Usage

---

**failover trigger** <1-8> **mmon monitor member** <port alias or number>

Adds the selected port to the Manual Monitor - Monitor.

**Command mode:** Global configuration

---

**Table 160** Failover Manual Monitor - Monitor 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 - Monitor.

**Command mode:** Global configuration

---

**failover trigger** <1-8> **mmon monitor portchannel** <trunk number>

Adds the selected trunk group to the Manual Monitor - Monitor.

**Command mode:** Global configuration

---

**no failover trigger** <1-8> **mmon monitor portchannel** <trunk number>

Removes the selected trunk group to the Manual Monitor - Monitor.

**Command mode:** Global configuration

---

**failover trigger** <1-8> **mmon monitor adminkey** <1-65535>

Adds an LACP admin key to the Manual Monitor - Monitor. LACP trunks formed with this admin key will be included in the Manual Monitor - Monitor.

**Command mode:** Global configuration

---

**no failover trigger** <1-8> **mmon monitor adminkey** <1-65535>

Removes an LACP admin key from the Manual Monitor - Monitor.

**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 161** 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.

**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.

**Command mode:** Global configuration

---

**failover trigger** <1-8> **mmon control portchannel** <trunk number>

Adds the selected trunk group to the Manual Monitor - Control.

**Command mode:** Global configuration

---

**no failover trigger** <1-8> **mmon control portchannel** <trunk number>

Removes the selected trunk group to the Manual Monitor - Control.

**Command mode:** Global configuration

---

**failover trigger** <1-8> **mmon control adminkey** <1-65535>

Adds an LACP admin key to the Manual Monitor - Monitor. LACP trunks formed with this admin key will be included in the Manual Monitor - Control.

**Command mode:** Global configuration

---

**no failover trigger** <1-8> **mmon control adminkey** <1-65535>

Removes an LACP admin key from the Manual Monitor - Control.

**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 5.1 Application Guide*.

**Table 162** Hot Links Configuration Commands

Command Syntax and Usage	
<b>[no] hotlinks bpdu</b>	<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><b>Command mode:</b> Global configuration</p>
<b>[no] hotlinks fdb-update</b>	<p>Enables or disables FDB Update, which allows the switch to send FDB and MAC update packets over the active interface.</p> <p>The default value is <code>disabled</code>.</p> <p><b>Command mode:</b> Global configuration</p>
<b>hotlinks enable</b>	<p>Globally enables Hot Links.</p> <p><b>Command mode:</b> Global configuration</p>
<b>no hotlinks enable</b>	<p>Globally disables Hot Links.</p> <p><b>Command mode:</b> Global configuration</p>
<b>show hotlinks</b>	<p>Displays current Hot Links parameters.</p> <p><b>Command mode:</b> All</p>



## Hot Links Trigger Configuration

**Table 163** Hot Links Trigger Configuration Commands

---

### Command Syntax and Usage

---

**hotlinks trigger** <1-5> **forward-delay** <0-3600>

Configures the Forward Delay interval, in seconds. The default value is 1.

**Command mode:** Global configuration

---

**hotlinks trigger** <1-5> **name** <1-32 characters>

Defines a name for the Hot Links trigger.

**Command mode:** Global configuration

---

[no] **hotlinks trigger** <1-5> **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** <1-5> **enable**

Enables or disables the Hot Links trigger.

**Command mode:** Global configuration

---

**no hotlinks trigger** <1-5>

Deletes the Hot Links trigger.

**Command mode:** Global configuration

---

**show hotlinks trigger** <1-25>

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 164** Hot Links Master Configuration Commands

Command Syntax and Usage	
<b>[no] hotlinks trigger &lt;1-5&gt; master port &lt;port alias or number&gt;</b>	
Adds the selected port to the Hot Links Master interface.	
<b>Command mode:</b> Global configuration	
<b>[no] hotlinks trigger &lt;1-5&gt; master portchannel &lt;0-16&gt;</b>	
Adds the selected trunk group to the Master interface.	
<b>Command mode:</b> Global configuration	
<b>[no] hotlinks trigger &lt;1-5&gt; master adminkey &lt;0-65535&gt;</b>	
Adds a LACP admin key to the Master interface. LACP trunks formed with this admin key will be included in the Master interface.	
<b>Command mode:</b> Global configuration	
<b>show hotlinks trigger &lt;1-5&gt;</b>	
Displays the current Hot Links settings.	
<b>Command mode:</b> All	

## Hot Links Backup Configuration

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

**Table 165** Hot Links Backup Configuration Commands

---

### Command Syntax and Usage

---

**[no] hotlinks trigger <1-5> backup port <port alias or number>**

Adds the selected port to the Hot Links Backup interface.

**Command mode:** Global configuration

---

**[no] hotlinks trigger <1-5> backup portchannel <0-16>**

Adds the selected trunk group to the Backup interface.

**Command mode:** Global configuration

---

**[no] hotlinks trigger <1-5> backup adminkey <0-65535>**

Adds a LACP admin key to the Backup interface. LACP trunks formed with this admin key will be included in the Backup interface.

**Command mode:** Global configuration

---

**show hotlinks trigger <1-5>**

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 166 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
member <port alias or number>	Adds port(s) to the VLAN membership. Command mode: VLAN
no member <port alias or number>	Removes port(s) from this VLAN. Command mode: VLAN

**Table 166** VLAN Configuration Commands

---

**Command Syntax and Usage**

---

**[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 167** 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 167** 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 168** 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 168 Private VLAN commands

Command Syntax and Usage
<b>private-vlan enable</b> Enables the private VLAN. <b>Command mode:</b> VLAN
<b>no private-vlan enable</b> Disables the Private VLAN. <b>Command mode:</b> VLAN
<b>show private-vlan [&lt;2-4094&gt;]</b> Displays current parameters for the selected Private VLAN(s). <b>Command mode:</b> VLAN

## VLAN Bandwidth Management Configuration

Use these commands to configure Bandwidth Management on the VLAN. For each internal port in the VLAN that has Bandwidth Management enabled, an Access Control List (ACL) is used to set the bandwidth parameters.

Table 169 VLAN Bandwidth Management commands

Command Syntax and Usage
<b>bandwidth rate &lt;64-14000000&gt;</b> Configures the traffic flow committed rate, in Kilobits per second. To calculate the traffic flow rate, multiply 64 kbps by the total number of ports in the VLAN. Acceptable rate values will be a multiple of the result. <b>Command mode:</b> VLAN
<b>bandwidth mbsize &lt;32-57344&gt;</b> Configures the maximum burst size, in Kilobits. To calculate the maximum burst size, multiply one of the following discreet values by the total number of ports in the VLAN: 32, 64, 128, 256, 512, 1024, 2048, 4096 <b>Command mode:</b> VLAN

Table 169 VLAN Bandwidth Management commands

Command Syntax and Usage	
<b>no bandwidth</b>	Disables Bandwidth Management on the VLAN.  <b>Command mode:</b> VLAN
<b>show vlan &lt;1-4094&gt; bandwidth</b>	Displays current bandwidth configuration for the VLAN.  <b>Command mode:</b> All

## Layer 3 Configuration

---

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

**Table 170** 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 277](#).

---

#### **route-map** {<1-32>}

Enter IP Route Map mode.

**Command mode:** Global configuration

To view command options, see [page 286](#).

---

#### **router rip**

Configures the Routing Interface Protocol.

**Command mode:** Global configuration

To view command options, see [page 290](#).

---

#### **router ospf**

Configures OSPF.

**Command mode:** Global configuration

To view command options, see [page 293](#).

---

#### **router bgp**

Configures Border Gateway Protocol.

**Command mode:** Global configuration

To view command options, see [page 305](#).

---

Table 170 Layer 3 Configuration Commands

Command Syntax and Usage	
<b>router vrrp</b>	Configures Virtual Router Redundancy. <b>Command mode:</b> Global configuration To view command options, see <a href="#">page 323</a> .
<b>ip router-id</b> <i>&lt;IP address&gt;</i>	Sets the router ID. <b>Command mode:</b> Global configuration
<b>show layer3</b>	Displays the current IP configuration. <b>Command mode:</b> 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 171** 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

---

**vlan** *<VLAN number>*

Configures the VLAN number for this interface. Each interface can belong to one VLAN.

**Command mode:** Interface IP

---

**[no] relay**

Enables or disables the BOOTP relay on this interface. It is enabled by default.

**Command mode:** Interface IP

---

**enable**

Enables this IP interface.

**Command mode:** Interface IP

---

**no enable**

Disables this IP interface.

**Command mode:** Interface IP

---

Table 171 IP Interface Configuration Commands

Command Syntax and Usage

**no interface ip** <interface number>

Removes this IP interface.

**Command mode:** Interface IP

**show interface ip** <interface number>

Displays the current interface settings.

**Command mode:** All

Default Gateway Configuration

The switch can be configured with up to 132 IPv4 gateways. Gateways 1–4 are reserved for default gateways. Gateway 132 is reserved for switch management.

This option is disabled by default.

Table 172 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

**Table 172** Default Gateway Commands**Command Syntax and Usage**


---

**ip gateway** <1-132> **vlan** <VLAN number>

Configures the VLAN to use for this default gateway.

**Note:** Gateway 1 and gateway 4 use VLAN 1, and cannot be changed.

**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

---

**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 173** 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.

**Note:** You may add multiple routes with the same IP address, but with different gateways. These routes become Equal Cost Multipath (ECMP) routes. The maximum number of gateways for each destination is five (5).

**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.

**Note:** The gateway IP address is optional. Include the gateway when you remove an ECMP route. If you do not include the gateway, then all ECMP paths for the route are deleted.

**Command mode:** Global configuration

---

**no ip route gateway** *<IP address>*

Clears all IP static routes that use this gateway.

**Note:** Use the gateway IP address to clear a single gateway for an ECMP route.

**Command mode:** Global configuration

---

**ip route interval** *<1-60>*

Configures the ping interval for ECMP health checks, in seconds. The default value is one second.

**Command mode:** Global configuration

---



**Table 173** IP Static Route Configuration Commands**Command Syntax and Usage****ip route retries** *<1-60>*

Configures the number of health check retries allowed before the switch declares that the gateway is down. The default value is 3.

**Command mode:** Global configuration

**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 174** 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 174 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 adminkey 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>  
**primary**|**backup**|**host**} [*<virtual router ID>* | **none**]

Removes a static multicast route. The destination address, VLAN, and LACP adminkey 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 175** ARP Configuration Commands

Command Syntax and Usage
<b>ip arp rearp</b> <i>&lt;2-120&gt;</i> Defines re-ARP period in minutes. You can set this duration between 2 and 120 minutes. <b>Command mode:</b> Global configuration
<b>show ip arp</b> Displays the current ARP configurations. <b>Command mode:</b> 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 176** ARP Static Configuration Commands

Command Syntax and Usage
<b>ip arp</b> <i>&lt;IP address&gt;</i> <i>&lt;MAC address&gt;</i> <b>vlan</b> <i>&lt;vlan number&gt;</i> <b>port</b> <i>&lt;port alias or number&gt;</i> Adds a permanent ARP entry. <b>Command mode:</b> Global configuration
<b>no ip arp</b> <i>&lt;IP address&gt;</i> Deletes a permanent ARP entry. <b>Command mode:</b> Global configuration

Table 176 ARP Static Configuration Commands

Command Syntax and Usage
<b>no ip arp all</b> Deletes all static ARP entries. <b>Command mode:</b> Global configuration
<b>show ip arp static</b> Displays current static ARP configuration. <b>Command mode:</b> All except User EXEC

IP Forwarding Configuration

Table 177 IP Forwarding Configuration Commands

Command Syntax and Usage
<b>[no] ip routing directed-broadcasts</b> Enables or disables forwarding directed broadcasts. The default setting is disabled. <b>Command mode:</b> Global configuration
<b>[no] ip routing no-icmp-redirect</b> Enables or disables ICMP re-directs. The default setting is disabled. <b>Command mode:</b> Global configuration
<b>ip routing</b> Enables IP forwarding (routing) on the GbESM. Forwarding is turned on by default. <b>Command mode:</b> Global configuration
<b>no ip routing</b> Disables IP forwarding (routing) on the GbESM. <b>Command mode:</b> Global configuration
<b>show ip routing</b> Displays the current IP forwarding settings. <b>Command mode:</b> All except User EXEC

## Network Filter Configuration

**Table 178** 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 179** 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 288](#).

---

**[no] as-path-list** <1-8>

Configures the Autonomous System (AS) Filter.

**Command mode:** Route map

For more information, see [page 289](#).

---

**[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 179** 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 180** 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 285 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 181** 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 182** Routing Information Protocol Commands

Command Syntax and Usage
<b>router rip</b> Enter Router RIP configuration mode. <b>Command mode:</b> Router RIP
<b>timers update &lt;1-120&gt;</b> Configures the time interval for sending for RIP table updates, in seconds. The default value is 30 seconds. <b>Command mode:</b> Router RIP
<b>enable</b> Globally turns RIP <b>on</b> . <b>Command mode:</b> Router RIP
<b>no enable</b> Globally turns RIP <b>off</b> . <b>Command mode:</b> Router RIP
<b>show ip rip</b> Displays the current RIP configuration. <b>Command mode:</b> 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 183** 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 183** 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

**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

## Open Shortest Path First Configuration

**Table 184** 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 297](#) to view command options.

---

#### **ip ospf** *<interface number>*

Configures the OSPF interface.

**Command mode:** Interface IP

See [page 298](#) 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 300](#) 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 302](#) to view command options.

---

**Table 184** 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 185** 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 185 Area Index Configuration Commands

Command Syntax and Usage

<b>area</b> <0-2> <b>spf-interval</b> <1-255>
Sets time interval between two successive SPF (shortest path first) calculations of the shortest path tree using the Dijkstra’s algorithm.
<b>Command mode:</b> Router OSPF
<b>area</b> <0-2> <b>enable</b>
Enables the OSPF area.
<b>Command mode:</b> Router OSPF
<b>no area</b> <0-2> <b>enable</b>
Disables the OSPF area.
<b>Command mode:</b> Router OSPF
<b>no area</b> <0-2>
Deletes the OSPF area.
<b>Command mode:</b> Router OSPF
<b>show ip ospf area</b> <0-2>
Displays the current OSPF configuration.
<b>Command mode:</b> All except User EXEC



## OSPF Summary Range Configuration

**Table 186** 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 187** OSPF Interface Configuration Commands

Command Syntax and Usage	
<b>ip ospf area</b> <0-2>	Configures the OSPF area index.  <b>Command mode:</b> Interface IP
<b>ip ospf priority</b> <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).  <b>Command mode:</b> Interface IP
<b>ip ospf cost</b> <1-65535>	Configures cost set for the selected path—preferred or backup. Usually the cost is inversely proportional to the bandwidth of the interface. Low cost indicates high bandwidth.  <b>Command mode:</b> Interface IP
<b>ip ospf hello-interval</b> <1-65535> <b>ip ospf hello-interval</b> <1-65535ms>	Configures the interval, in seconds or milliseconds, between the <code>hello</code> packets for the interfaces.  <b>Command mode:</b> Interface IP
<b>ip ospf dead-interval</b> <1-65535> <b>ip ospf dead-interval</b> <1-65535ms>	Configures the health parameters of a <code>hello</code> packet, in seconds or milliseconds, before declaring a silent router to be down.  <b>Command mode:</b> Interface IP
<b>ip ospf transit-delay</b> <1-3600>	Configures the transit delay in seconds.  <b>Command mode:</b> Interface IP

**Table 187** 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 187 OSPF Interface Configuration Commands

Command Syntax and Usage

**no ip ospf**

Deletes the OSPF interface.

**Command mode:** Interface IP

**show interface ip** *<interface number>* **ospf**

Displays the current settings for OSPF interface.

**Command mode:** All except User EXEC

OSPF Virtual Link Configuration

Table 188 OSPF Virtual Link Configuration Commands

Command Syntax and Usage

**area-virtual-link** *<1-3>* **area** *<0-2>*

Configures the OSPF area index for the virtual link.

**Command mode:** Router OSPF

**area-virtual-link** *<1-3>* **hello-interval** *<1-65535>*

**area-virtual-link** *<1-3>* **hello-interval** *<1-65535ms>*

Configures the authentication parameters of a hello packet, in seconds or milliseconds.

**Command mode:** Router OSPF

**area-virtual-link** *<1-3>* **dead-interval** *<1-65535>*

**area-virtual-link** *<1-3>* **dead-interval** *<1-65535ms>*

Configures the health parameters of a hello packet, in seconds or milliseconds. The default value is 60 seconds.

**Command mode:** Router OSPF

**area-virtual-link** *<1-3>* **transit-delay** *<1-3600>*

Configures the delay in transit, in seconds. Default is one second.

**Command mode:** Router OSPF

**area-virtual-link** *<1-3>* **retransmit-interval** *<1-3600>*

Configures the retransmit interval, in seconds. Default is five seconds.

**Command mode:** Router OSPF

**Table 188** OSPF Virtual Link Configuration Commands**Command Syntax and Usage**


---

**area-virtual-link** <1-3> **neighbor-router** <IP address>

Configures the router ID of the virtual neighbor. Default is 0.0.0.0.

**Command mode:** Router OSPF

---

[no] **area-virtual-link** <1-3> **key** <key string>

Configures the password (up to eight characters) for each virtual link. Default is none.

**Command mode:** Router OSPF

---

**area-virtual-link** <1-3> **message-digest-key** <1-255>

Sets MD5 key ID for each virtual link. Default 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 189** OSPF Host Entry Configuration Commands

Command Syntax and Usage	
<b>host</b> <1-128> <b>address</b> <IP address>	
Configures the base IP address for the host entry.	
<b>Command mode:</b> Router OSPF	
<b>host</b> <1-128> <b>area</b> <0-2>	
Configures the area index of the host.	
<b>Command mode:</b> Router OSPF	
<b>host</b> <1-128> <b>cost</b> <1-65535>	
Configures the cost value of the host.	
<b>Command mode:</b> Router OSPF	
<b>host</b> <1-128> <b>enable</b>	
Enables OSPF host entry.	
<b>Command mode:</b> Router OSPF	
<b>no host</b> <1-128> <b>enable</b>	
Disables OSPF host entry.	
<b>Command mode:</b> Router OSPF	
<b>no host</b> <1-128>	
Deletes OSPF host entry.	
<b>Command mode:</b> Router OSPF	
<b>show ip ospf host</b> <1-128>	
Displays the current OSPF host entries.	
<b>Command mode:</b> All except User EXEC	

## OSPF Route Redistribution Configuration.

**Table 190** 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 191** OSPF MD5 Key commands

Command Syntax and Usage	
<b>message-digest-key</b> <1-255> <b>md5-key</b> <1-16 characters>	
Sets the authentication key for this OSPF packet.	
<b>Command mode:</b> Router OSPF	
<b>no message-digest-key</b> <1-255>	
Deletes the authentication key for this OSPF packet.	
<b>Command mode:</b> Router OSPF	
<b>show ip ospf message-digest-key</b> <1-255>	
Displays the current MD5 key configuration.	
<b>Command mode:</b> 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 GbE Switch Module 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 192** 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 306](#).

---

#### **as <0-65535>**

Set Autonomous System number.

**Command mode:** Router BGP

---

**Table 192** 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 193** 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 193** 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.

**Command mode:** Router BGP

---

**neighbor** <1-16> **retry-interval** <1-65535>

Sets connection retry interval, in seconds.

**Command mode:** Router BGP

---

**neighbor** <1-16> **route-origination-interval** <1-65535>

Sets the minimum time between route originations, in 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 193** 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 194** 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 194 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 195 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 195** 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 196 describes the commands used to configure basic IGMP parameters.

**Table 196** IGMP Configuration Commands

---

**Command Syntax and Usage**

---

**ip igmp enable**

Globally turns IGMP on.

**Command mode:** Global configuration

---

**no ip igmp**

Globally turns IGMP off.

**Command mode:** Global configuration

---

**[no] ip igmp aggregate**

Enables or disables IGMP Membership Report aggregation.

**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 197 describes the commands used to configure IGMP Snooping.

Table 197 IGMP Snooping Configuration Commands

Command Syntax and Usage
<b>ip igmp snoop enable</b> Enables IGMP Snooping. <b>Command mode:</b> Global configuration
<b>no ip igmp snoop enable</b> Disables IGMP Snooping. <b>Command mode:</b> Global configuration
<b>ip igmp snoop mrouter-timeout &lt;1-600&gt;</b> 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. <b>Command mode:</b> Global configuration
<b>[no] ip igmp aggregate</b> Enables or disables IGMP Membership Report aggregation. <b>Command mode:</b> Global configuration
<b>ip igmp snoop source-ip &lt;IP address&gt;</b> Configures the source IP address used as a proxy for IGMP Group Specific Queries. <b>Command mode:</b> Global configuration
<b>ip igmp snoop vlan &lt;VLAN number&gt;</b> Adds the selected VLAN(s) to IGMP Snooping. <b>Command mode:</b> Global configuration



**Table 197** IGMP Snooping Configuration Commands

---

**Command Syntax and Usage**

---

**no ip igmp snoop vlan** *<VLAN number>*

Removes the selected VLAN(s) from IGMP Snooping.

**Command mode:** Global configuration

---

**no ip igmp snoop vlan all**

Removes all VLANs from IGMP Snooping.

**Command mode:** Global configuration

---

**show ip igmp snoop**

Displays the current IGMP Snooping parameters.

**Command mode:** All

---

## IGMPv3 Configuration

Table 201 describes the commands used to configure IGMP version 3.

**Table 198** 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.

**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

---

Table 198 IGMP version 3 Configuration Commands

Command Syntax and Usage	
<b>ip igmp snoop igmpv3 enable</b>	Enables IGMP version 3. The default value is <b>enabled</b> .
<b>Command mode:</b> Global configuration	
<b>no ip igmp snoop igmpv3 enable</b>	Disables IGMP version 3.
<b>Command mode:</b> Global configuration	
<b>show ip igmp snoop igmpv3</b>	Displays the current IGMP v3 Snooping configuration.
<b>Command mode:</b> All except User EXEC	

## IGMP Relay Configuration

When you configure IGMP Relay, also configure the IGMP Relay multicast routers.

Table 201 describes the commands used to configure IGMP Relay.

Table 199 IGMP Relay Configuration Commands

Command Syntax and Usage	
<b>ip igmp relay enable</b>	Enables IGMP Relay.
<b>Command mode:</b> Global configuration	
<b>no ip igmp relay enable</b>	Disables IGMP Relay.
<b>Command mode:</b> Global configuration	
<b>ip igmp relay vlan &lt;VLAN number&gt;</b>	Adds the VLAN to the list of IGMP Relay VLANs.
<b>Command mode:</b> Global configuration	
<b>no ip igmp relay vlan &lt;VLAN number&gt;</b>	Removes the VLAN from the list of IGMP Relay VLANs.
<b>Command mode:</b> Global configuration	

**Table 199** IGMP Relay Configuration Commands

---

**Command Syntax and Usage**

---

**ip igmp relay report** <0-150>

Configures the interval between unsolicited Join reports sent by the switch, in seconds.

The default value is 10.

**Command mode:** Global configuration

---

**show ip igmp relay**

Displays the current IGMP Relay configuration.

**Command mode:** All except User EXEC

---

## IGMP Relay Multicast Router Configuration

[Table 201](#) describes the commands used to configure multicast routers for IGMP Relay.

**Table 200** 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> **version** <1-2>

Configures the IGMP version (1 or 2) of the multicast router.

**Command mode:** Global configuration

---

Table 200 IGMP Relay Mrouter Configuration Commands

Command Syntax and Usage
<b>ip igmp relay mrouter &lt;1-2&gt; enable</b> Enables the multicast router. <b>Command mode:</b> Global configuration
<b>no ip igmp relay mrouter &lt;1-2&gt; enable</b> Disables the multicast router. <b>Command mode:</b> Global configuration
<b>no ip igmp relay mrouter &lt;1-2&gt;</b> Deletes the multicast router from IGMP Relay. <b>Command mode:</b> Global configuration

IGMP Static Multicast Router Configuration

Table 201 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 201 IGMP Static Multicast Router Configuration Commands

Command Syntax and Usage
<b>ip igmp mrouter &lt;port alias or number&gt; &lt;VLAN number&gt; &lt;version (1-3)&gt;</b> 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. <b>Command mode:</b> Global configuration
<b>no ip igmp mrouter &lt;port alias or number&gt; &lt;VLAN number&gt; &lt;version (1-3)&gt;</b> Removes a static multicast router from the selected port/VLAN combination. <b>Command mode:</b> Global configuration

**Table 201** 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 202](#) describes the commands used to configure an IGMP filter.

**Table 202** 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 318](#).

---

**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 203 describes the commands used to define an IGMP filter.

Table 203 IGMP Filter Definition Commands

Command Syntax and Usage	
<b>ip igmp profile</b> <1-16> <b>range</b> <IP address 1> <IP address 2>	
Configures the range of IP multicast addresses for this filter.	
<b>Command mode:</b> Global configuration	
<b>ip igmp profile</b> <1-16> <b>action</b> {allow deny}	
Allows or denies multicast traffic for the IP multicast addresses specified.	
<b>Command mode:</b> Global configuration	
<b>ip igmp profile</b> <1-16> <b>enable</b>	
Enables this IGMP filter.	
<b>Command mode:</b> Global configuration	
<b>no ip igmp profile</b> <1-16> <b>enable</b>	
Disables this IGMP filter.	
<b>Command mode:</b> Global configuration	
<b>no ip igmp profile</b> <1-16>	
Deletes this filter's parameter definitions.	
<b>Command mode:</b> Global configuration	
<b>show ip igmp profile</b> <1-16>	
Displays the current IGMP filter.	
<b>Command mode:</b> All	

## IGMP Filtering Port Configuration

Table 204 describes the commands used to configure a port for IGMP filtering.

**Table 204** 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 201 describes the commands used to configure advanced IGMP parameters.

**Table 205** 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 205** 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 206** 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 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 207** Bootstrap Protocol Relay Configuration Commands

Command Syntax and Usage	
<b>[no] ip bootp-relay {server1 server2} &lt;IP address&gt;</b>	
Sets the IP address of the first or second BOOTP server.	
<b>Command mode:</b> Global configuration	
<b>ip bootp-relay enable</b>	
Globally turns on BOOTP relay.	
<b>Command mode:</b> Global configuration	
<b>no ip bootp-relay enable</b>	
Globally turns off BOOTP relay.	
<b>Command mode:</b> 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 5.1 Application Guide*.

**Table 208** 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 209** VRRP Virtual Router Configuration Commands

Command Syntax and Usage
<b>virtual-router</b> <1-250> <b>virtual-router-id</b> <1-128>  Defines the virtual router ID (VRID). This is used in conjunction with the [no] <b>virtual-router</b> <VRID> <b>address</b> <IP address> command below to define a virtual router on this switch. To create a pool of VRRP-enabled routing devices which can provide redundancy to each other, each participating VRRP device must be configured with the same virtual router.  The VRID for standard virtual routers (where the virtual router IP address is not the same as any virtual server) can be any integer between 1 and 128. The default value is 1.  All VRID values must be unique within the VLAN to which the virtual router's IP interface belongs.  <b>Command mode:</b> Router VRRP
[no] <b>virtual-router</b> <1-250> <b>address</b> <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.  <b>Command mode:</b> Router VRRP
<b>virtual-router</b> <1-250> <b>interface</b> <interface number>  Selects a switch IP interface. If the IP interface has the same IP address as the <b>addr</b> 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 <b>preem</b> option below is disabled. The default value is 1.  <b>Command mode:</b> Router VRRP

**Table 209** VRRP Virtual Router Configuration Commands

---

**Command Syntax and Usage**

---

**virtual-router** <1-250> **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** <1-250> **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** <1-250> **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** <1-250> **enable**

Enables this virtual router.

**Command mode:** Router VRRP

---

**no** **virtual-router** <1-250> **enable**

Disables this virtual router.

**Command mode:** Router VRRP

---

Table 209 VRRP Virtual Router Configuration Commands

Command Syntax and Usage

**no virtual-router** <1-250>

Deletes this virtual router from the switch configuration.

**Command mode:** Router VRRP

**show ip vrrp virtual-router** <1-250>

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 210** VRRP Priority Tracking Configuration Commands

---

**Command Syntax and Usage**

---

---

**[no] virtual-router <1-250> 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 <1-250> 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 <1-250> 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 <1-250> 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 211 VRRP Virtual Router Group Configuration Commands

### Command Syntax and Usage

**group virtual-router-id** <1-128>

Defines the virtual router ID (VRID).

The VRID for standard virtual routers (where the virtual router IP address is not the same as any virtual server) can be any integer between 1 and 128. All VRID values must be unique within the VLAN to which the virtual router’s IP interface (see *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 211** 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 212** 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 213** 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 326](#)), the priority level for the virtual router is increased by a defined amount.

**Table 214** 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 326](#)) are enabled.

---

## 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 215** IP Loopback Interface commands

---

### Command Syntax and Usage

---

**interface loopback** *<1-5>*

Enter Interface loopback mode.

**Command mode:** Global configuration

---

**no interface loopback** *<1-5>*

Deletes the selected loopback interface.

**Command mode:** Global configuration

---

**ip address** *<IP address>*

Defines the loopback interface IP address.

**Command mode:** Interface loopback

---

**ip netmask** *<subnet mask>*

Defines the loopback interface subnet mask.

**Command mode:** Interface loopback

---

**enable**

Enables the loopback interface.

**Command mode:** Interface loopback

---

**no enable**

Disables the loopback interface.

**Command mode:** Interface loopback

---

**show interface loopback** *<1-5>*

Displays the current IP loopback interface parameters.

---

# 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 334](#)
- [“RMON Event Configuration” on page 335](#)
- [“RMON Alarm Configuration” on page 336](#)

## RMON History Configuration

[Table 216](#) describes the RMON History commands.

**Table 216** 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 216** 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 217 describes the RMON Event commands.

**Table 217** 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 217 RMON Event commands

Command Syntax and Usage
<b>no rmon event</b> <1-65535> Deletes the selected RMON Event index. <b>Command mode:</b> Global configuration
<b>show rmon event</b> Displays the current RMON Event parameters. <b>Command mode:</b> 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 218 describes the RMON Alarm commands.

Table 218 RMON Alarm commands

Command Syntax and Usage
<b>rmon alarm</b> <1-65535> <b>oid</b> <1-127 characters> Configures an alarm MIB Object Identifier. <b>Command mode:</b> Global configuration
<b>rmon alarm</b> <1-65535> <b>interval</b> <1-65535> Configures the time interval over which data is sampled and compared with the rising and falling thresholds. The default value is 1800. <b>Command mode:</b> Global configuration
<b>rmon alarm</b> <1-65535> <b>sample abs delta</b> Configures the method of sampling the selected variable and calculating the value to be compared against the thresholds, as follows: <ul style="list-style-type: none"><li>abs—absolute value, the value of the selected variable is compared directly with the thresholds at the end of the sampling interval.</li><li>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.</li></ul> <b>Command mode:</b> Global configuration



**Table 218** 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

---

## 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 339](#).

## 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 219** 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 220** 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

---

**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 221** 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 222 Virtual Router Redundancy Operations Commands

## Command Syntax and Usage

**router vrrp backup** *<virtual router number (1-128)>*

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 223 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 224** 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 224 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

---

## 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.

## Updating the Switch Software Image

---

The switch software image is the executable code running on the GbE Switch Module. 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 1.5.1
that was downloaded at 0:23:39 Thu Jan 1, 2009.
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 GbE Switch Module, 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 GbE Switch Module 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 GbE Switch Module 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.



## 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 GbE Switch Module 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 225** 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 361](#).

---

#### **copy flash-dump tftp**

Saves the system dump information via TFTP.

**Command mode:** All except User EXEC

For details, see [page 362](#).

---

#### **copy flash-dump ftp**

Saves the system dump information via FTP.

**Command mode:** All except User EXEC

---

Table 225 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 226 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 226** 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

---

**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 227** 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 228** 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 73](#).

---

# IP Route Manipulation

Table 229 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 33 on page 71](#)

**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 34 on page 72](#)

**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 70](#).

## LLDP Cache Manipulation

---

Table 230 describes the LLDP cache manipulation commands.

**Table 230** 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 231 describes the IGMP group maintenance commands.

**Table 231** IGMP Multicast Group Maintenance Commands

---

### Command Syntax and Usage

---

**show ip igmp groups address** *<IP address>*

Displays a single IGMP multicast group by its IP address.

**Command mode:** All

---

**show ip igmp groups vlan** *<VLAN number>*

Displays all IGMP multicast groups on a single VLAN.

**Command mode:** All

---

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

Displays all IGMP multicast groups on selected ports.

**Command mode:** All

---

**show ip igmp groups portchannel** *<trunk number>*

Displays all IGMP multicast groups on a single trunk group.

**Command mode:** All

---

**show ip igmp groups detail** *<IP address>*

Displays detailed information about a single IGMP multicast group.

**Command mode:** All

---

**show ip igmp groups**

Displays information for all multicast groups.

**Command mode:** All

---

**clear ip igmp groups**

Clears the IGMP group table.

**Command mode:** All except User EXEC

---



## IGMP Multicast Routers Maintenance

The following table describes the maintenance commands for IGMP multicast routers (Mrouters).

**Table 232** IGMP Multicast Router Maintenance Commands

---

### Command Syntax and Usage

---

**show ip igmp mrouter vlan** *<VLAN number>*

Displays IGMP Mrouter information for a single VLAN.

**Command mode:** All

---

**show ip igmp mrouter**

Displays information for all Mrouters.

**Command mode:** All

---

**clear ip igmp mrouter**

Clears the IGMP Mrouter port table.

**Command mode:** All except User EXEC

---

## Uencode Flash Dump

Using this command, dump information is presented in uencoded format. This format makes it easy to capture the dump information as a file or a string of characters.

If you want to capture dump information to a file, set your communication software on your workstation to capture session data prior to issuing the `show flash-dump-uencode` command. This will ensure that you do not lose any information. Once entered, the `show flash-dump-uencode` command will cause approximately 23,300 lines of data to be displayed on your screen and copied into the file.

Using the `show flash-dump-uencode` command, dump information can be read multiple times. The command does not cause the information to be updated or cleared from flash memory.

---

**Note** – Dump information is not cleared automatically. In order for any subsequent dump information to be written to flash memory, you must manually clear the dump region. For more information on clearing the dump region, see [page 362](#).

---

To access dump information, enter:

Router# <b>show flash-dump-uencode</b>
----------------------------------------

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, 2009. 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

---

## Symbols

## Numerics

802.1p information ..... 92

## A

abbreviating commands (CLI) ..... 21

access control

    user ..... 198

Access Control Lists ..... 220

ACL configuration ..... 220

ACL Port commands ..... 211

ACL statistics ..... 154

active configuration block ..... 164, 350

active IP interface ..... 330

active port

    VLAN ..... 330

active switch configuration

    gtcfg ..... 339

    ptcfg ..... 338

    restoring ..... 339

active switch, saving and loading configuration .... 339

addr

    IP route tag ..... 72

administrator account ..... 22

aging

    STP information ..... 58, 61

autonomous system filter action ..... 289

autonomous system filter path

    action ..... 289

    as ..... 289

    aspath ..... 289

## B

backup configuration block ..... 350

Bandwidth Management ..... 273

## BGP

    configuration ..... 305

    eBGP ..... 305

    filters, aggregation configuration ..... 310

    iBGP ..... 305

    in route ..... 308

    IP address, border router ..... 306

    IP route tag ..... 72

    keep-alive time ..... 307

    peer ..... 305

    peer configuration ..... 306

    redistribution configuration ..... 309

    remote autonomous system ..... 306

    router hops ..... 307

BLOCKING (port state) ..... 59

Boot options ..... 347

bootstrap protocol ..... 322

Border Gateway Protocol ..... 72

    configuration ..... 305

Border Gateway Protocol (BGP)

    operations-level options ..... 344

BPDU. *See Bridge Protocol Data Unit.*

bridge priority ..... 58, 64

Bridge Protocol Data Unit (BPDU) ..... 58, 64

    STP transmission frequency ..... 244

Bridge Spanning-Tree parameters ..... 244

broadcast

    IP route tag ..... 72

    IP route type ..... 71

## C

capture dump information to a file ..... 361

Cisco Ether Channel ..... 253

CIST information ..... 63

clear

    dump information ..... 362

command (help) ..... 19

commands	
abbreviations .....	21
conventions used in this manual .....	12
shortcuts .....	20
tab completion .....	21
commands, NNCLI	
modes .....	16
configuration	
802.1x .....	231
CIST .....	239
default gateway interval, for health checks .....	278
default gateway IP address .....	278
dump command .....	338
failover .....	259
flow control .....	209
IGMP .....	311
IP static route .....	280
port link speed .....	208
port mirroring .....	228
port trunking .....	253
RIP .....	290
save changes .....	164
SNMP .....	181
switch IP address .....	277
TACACS+ .....	173
VLAN default (PVID) .....	206
VLAN IP interface .....	277
VLAN tagging .....	206
VRRP .....	323
configuration block	
active .....	350
backup .....	350
factory .....	351
selection .....	350
Configuration commands .....	163
configuring routing information protocol .....	291
COS queue information .....	92
cost	
STP information .....	59, 61, 64
STP port option .....	246
CPU statistics .....	153
CPU utilization .....	153

## D

daylight savings time .....	165
debugging .....	353
default gateway	
information .....	69
interval, for health checks .....	278
default password .....	22

delete	
FDB entry .....	355
direct (IP route type) .....	71
directed broadcasts .....	284
DISABLED (port state) .....	59
disconnect idle timeout .....	22
downloading software .....	348
DSCP .....	219
dump	
configuration command .....	338
maintenance .....	353
duplex mode	
link status .....	23, 100
dynamic routes .....	358

## E

End-to-End flow control .....	166
EtherChannel	
as used with port trunking .....	253
Etherchannel information .....	65

## F

factory configuration block .....	351
failover	
configuration .....	259
FDB statistics .....	121
fixed	
IP route tag .....	72
flag field .....	74
flow control .....	23, 100
configuring .....	209
forwarding configuration	
IP forwarding configuration .....	284
forwarding database (FDB) .....	353
delete entry .....	355
Forwarding Database Information .....	44
Forwarding Database maintenance .....	354
forwarding state (FWD) .....	45, 58, 64, 65
fwd (STP bridge option) .....	245
FwdDel (forward delay), bridge port .....	58, 61, 64

## G

gtcfg (TFTP load command) .....	339
---------------------------------	-----

## H

health checks	
default gateway interval, retries .....	278
retry, number of failed health checks .....	278

hello	
STP information .....	58, 61, 64
help.....	19
Hot Links configuration .....	264
hot-standby failover.....	328
hprompt	
system option .....	167
HTTPS.....	202

## I

ICMP statistics .....	135
idle timeout	
overview.....	22
IEEE standards	
802.1d .....	58, 243
802.1s .....	238
802.1w .....	238
802.1x .....	55, 57
IGMP Information .....	86
IGMP Relay.....	314
IGMP Snooping .....	312
IGMP statistics.....	140
image	
downloading .....	348
software, selecting .....	349
indirect (IP route type) .....	71
Information	
IGMP Multicast Router Information.....	360
Information commands .....	23
Ingress Back Pressure (IBP) flow control.....	166
Interface change stats .....	145
IP address	
ARP information .....	73
configuring default gateway .....	278
IP forwarding	
directed broadcasts.....	284
IP forwarding information .....	69
IP Information.....	69
IP interface	
active .....	330
configuring address.....	277
configuring VLANs .....	277
IP interfaces.....	71
information .....	69
IP route tag .....	72
priority increment value (ifs) for VRRP .....	332
IP network filter configuration .....	285
IP Route Manipulation .....	358
IP routing	
tag parameters .....	72

IP Static Route commands .....	280
IP statistics .....	130

## L

LACP .....	257
Layer 2 commands .....	41
Layer 3 commands .....	68
LDAP .....	177
LEARNING (port state).....	58, 59, 64
link	
speed, configuring .....	208
Link Aggregation Control Protocol .....	257
link status .....	23
command .....	100
duplex mode .....	23, 100
port speed .....	23, 100
Link Status Information .....	100
linkt (SNMP option) .....	182
LISTENING (port state) .....	59
LLDP	
configuration.....	249
information.....	51
LLDP TLV .....	251
local (IP route type).....	71
log	
syslog messages .....	168

## M

MAC (media access control) address.....	25, 38, 44, 73, 354
Maintenance commands.....	353
Management Processor (MP) .....	355
display MAC address .....	25, 38
manual style conventions .....	12
martian	
IP route tag (filtered).....	72
IP route type (filtered out).....	71
mation.....	65
MaxAge (STP information).....	58, 61, 64
MD5 cryptographic authentication .....	295
MD5 key .....	299
media access control. <i>See</i> MAC address.	
meter	
ACL .....	212, 228
Miscellaneous Debug commands .....	355
monitor port.....	228
mp	
packet .....	150
MP. <i>See</i> Management Processor.	
Mrouter information .....	89

multicast	
IP route type.....	71
multiple management VLANs .....	269
Multiple Spanning Tree	
configuration.....	238
mxage (STP bridge option).....	244

## N

nbr change statistics.....	144
NNCLI commands	
modes .....	16
notice .....	165
NTP synchronization .....	180

## O

OAM Discovery	
information .....	54
online help.....	19
Operations commands.....	341
operations-level BGP options .....	344
Operations-Level Port Options.....	342, 343
operations-level VRRP options .....	344
ospf	
area index .....	295
authentication key .....	299
cost of the selected path .....	298
cost value of the host.....	302
dead, declaring a silent router to be down.....	298
dead, health parameter of a hello packet.....	300
export.....	303
fixed routes .....	305
hello, authentication parameter of a hello packet.....	300
host entry configuration .....	302
host routes .....	293
interface .....	293
interface configuration.....	298
link state database .....	294
Not-So-Stubby Area.....	295
priority value of the switch interface.....	298
range number .....	293
route redistribution configuration.....	303
spf, shortest path first .....	296
stub area .....	295
summary range configuration .....	297
transit area .....	295
transit delay .....	298
type.....	295

virtual link .....	293
virtual link configuration .....	300
virtual neighbor, router ID .....	301
OSPF Database Information.....	80
OSPF General Information.....	79
OSPF Information .....	77
OSPF Information Route Codes.....	82

## P

parameters	
tag .....	72
type .....	71
Password	
user access control.....	198
password	
administrator account .....	22
default.....	22
user account.....	22
passwords.....	22
ping .....	19
poisoned reverse, as used with split horizon.....	291
Port configuration .....	206
port configuration.....	206
port mirroring	
configuration.....	228
Port number.....	100
port speed.....	23, 100
port states	
UNK (unknown) .....	45
port trunking	
description.....	253
port trunking configuration .....	253
ports	
disabling (temporarily) .....	209
information.....	101
membership of the VLAN .....	42, 67
priority .....	59, 64
VLAN ID.....	24, 101
preemption	
assuming VRRP master routing authority .....	326
prisrv	
primary radius server .....	171, 177
Private VLAN.....	272
Protected Mode.....	345
Protocol-based VLAN .....	270
ptcfg (TFTP save command) .....	338
PVID (port VLAN ID).....	24, 101



**Q**

QoS ..... 218

**R**

read community string (SNMP option) ..... 182  
 receive flow control ..... 209  
 reference ports ..... 45  
 re-mark ..... 214, 228  
 Remote Monitoring (RMON) ..... 334  
 retries  
     radius server ..... 171  
 retry  
     health checks for default gateway ..... 278  
 rip  
     IP route tag ..... 72  
 RIP Information ..... 84  
 RIP information ..... 83  
 RIP. *See Routing Information Protocol.*  
 RMON  
     information ..... 95  
 route statistics ..... 133  
 router hops ..... 307  
 routing information protocol  
     configuration ..... 291  
 Routing Information Protocol (RIP) ..... 72  
     options ..... 291  
     poisoned reverse ..... 291  
     split horizon ..... 291  
     version 1 parameters ..... 290, 291  
 RSTP information ..... 60  
 Rx/Tx statistics ..... 143

**S**

save (global command) ..... 164  
 secret  
     radius server ..... 171  
 Secure Shell ..... 169  
 shortcuts (CLI) ..... 20  
 snap traces  
     buffer ..... 356  
 SNMP options ..... 181  
 SNMP statistics ..... 156  
 SNMPv3 ..... 183  
 software  
     image ..... 348  
     image file and version ..... 25, 38  
 spanning tree  
     configuration ..... 243

Spanning-Tree Protocol ..... 65  
     bridge parameters ..... 244  
     bridge priority ..... 58, 64  
     port cost option ..... 246  
     root bridge ..... 58, 64, 244  
     switch reset effect ..... 351  
 split horizon ..... 291  
 state (STP information) ..... 59, 62, 64  
 static  
     IP route tag ..... 72  
 static route  
     rem ..... 280  
 statis route  
     add ..... 280  
 statistics  
     management processor ..... 149  
 Statistics commands ..... 103  
 subnets  
     IP interface ..... 277  
 switch  
     name and location ..... 25, 38  
     resetting ..... 351  
 system  
     contact (SNMP option) ..... 181  
     date and time ..... 25, 38  
     information ..... 38  
     location (SNMP option) ..... 181  
 System Information ..... 25  
 system options  
     hprompt ..... 167  
     tport ..... 196  
     wport ..... 196

**T**

tab completion (CLI) ..... 21  
 TCP statistics ..... 137, 152  
 Telnet  
     configuring switches using ..... 338  
 telnet  
     radius server ..... 172, 178  
 text conventions ..... 12  
 TFTP ..... 348  
     PUT and GET commands ..... 338  
 TFTP server ..... 338  
 timeout  
     radius server ..... 171  
 timeouts  
     idle connection ..... 22  
 timers kickoff ..... 146  
 TLV ..... 251

tnport	
system option .....	196
trace buffer .....	355
traceroute .....	19
transmit flow control .....	209
Trunk group information .....	65
trunk hash algorithm .....	255
type of area	
ospf .....	295
type parameters .....	71
typographic conventions, manual .....	12

## U

UCB statistics .....	152
UDLD	
information .....	53
UDP statistics .....	139
unknown (UNK) port state .....	45
Unscheduled System Dump .....	363
upgrade, switch software .....	348
user access control configuration .....	198
user account .....	22
Uencode Flash Dump .....	361

## V

virtual router	
description .....	324
tracking criteria .....	326
virtual router group configuration .....	328
virtual router group priority tracking .....	330
Virtual Router Redundancy Protocol (VRRP)	
authentication parameters for IP interfaces .....	331
operations-level options .....	344
priority tracking options .....	306, 310, 327
Virtual Router Redundancy Protocol configuration .....	323
virtual routers	
increasing priority level of .....	326
priority increment values (vrs) for VRRP .....	332
VLAN	
active port .....	330
configuration .....	268
VLAN tagging	
port configuration .....	206
port restrictions .....	269

VLANs	
ARP entry information .....	73
information .....	67
name .....	42, 67
port membership .....	42, 67
setting default number (PVID) .....	206
tagging .....	24, 101, 269
VLAN Number .....	67
VRRP	
interface configuration .....	331
master advertisements .....	325
tracking configuration .....	332
VRRP Information .....	90
VRRP master advertisements	
time interval .....	329
VRRP statistics .....	147

## W

watchdog timer .....	353
weights	
setting virtual router priority values .....	332
wport .....	196