



Alteon OSTM ISCLI Reference

Nortel 10Gb Ethernet Switch Module for IBM BladeCenter[®]
Version 1.0

Part Number: 42C4914, February 2007

Solutions by

NORTEL

BLADE
NETWORK
TECHNOLOGIES

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

Copyright © 2007 Blade Network Technologies, Inc., 2350 Mission College Blvd., Suite 600, Santa Clara, California, 95054, USA. All rights reserved. Part Number: 42C4914.

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.

Originated in the USA.

Alteon OS, and Alteon are trademarks of Nortel Networks, Inc. in the United States and certain other countries. Cisco[®] and EtherChannel[®] are registered trademarks of Cisco Systems, Inc. in the United States and certain other countries. Any other trademarks appearing in this manual are owned by their respective companies.

Contents

Preface 11

- Who Should Use This Book 12
- How This Book Is Organized 13
- Typographic Conventions 14
- How to Get Help 16

ISCLI Basics 17

- Accessing the ISCLI 17
- ISCLI command modes 18
- Global Commands 21
- Command Line Interface Shortcuts 23
 - Command Abbreviation 23
 - Tab Completion 23
- User Access Levels 24
- Idle Timeout 25

Information Commands 27

- System Information 28
 - SNMPv3 System Information 29
 - SNMPv3 USM User Table Information 30
 - SNMPv3 View Table Information 32
 - SNMPv3 Access Table Information 32
 - SNMPv3 Group Table Information 34
 - SNMPv3 Community Table Information 34
 - SNMPv3 Target Address Table Information 35
 - SNMPv3 Target Parameters Table Information 36
 - SNMPv3 Notify Table Information 36
 - SNMPv3 Dump Information 38
 - BladeCenter Information 39
 - General System Information 40
 - Show Recent Syslog Messages 41

User Status	42
Layer 2 Information	43
FDB Information	45
Show All FDB Information	46
Clearing Entries from the Forwarding Database	46
Link Aggregation Control Protocol Information	46
Link Aggregation Control Protocol	47
802.1p Information	48
Access Control List Information	49
802.1x Information	50
Spanning Tree Information	52
RSTP/MSTP Information	55
Common Internal Spanning Tree Information	58
Trunk Group Information	60
VLAN Information	61
Failover Information	62
Layer 3 Information	63
IP Routing Information	63
Show All IP Route Information	65
ARP Information	66
Show All ARP Entry Information	67
ARP Address List Information	68
BGP Information	69
BGP Peer information	69
BGP Summary information	70
Dump BGP Information	70
OSPF Information	71
OSPF General Information	72
OSPF Interface Information	73
OSPF Database Information	73
OSPF Information Route Codes	75
Routing Information Protocol	76
RIP Routes Information	76
RIP User Configuration	77
IP Information	77
IGMP Multicast Group Information	78
IGMP Group Information	80
IGMP Multicast Router Information	81
VRRP Information	81
Link Status Information	83
Port Information	84

Logical Port to GEA Port Mapping 85
Fiber Port SFP Status 86
Information Dump 86

Statistics Commands 87

Port Statistics 88

802.1x Authenticator Statistics 89
802.1x Authenticator Diagnostics 90
Bridging Statistics 93
Ethernet Statistics 94
Interface Statistics 96
Interface Protocol Statistics 98
Link Statistics 98

Layer 2 Statistics 99

FDB Statistics 99
LACP Statistics 100

Layer 3 Statistics 102

IP Statistics 104
Route Statistics 106
ARP statistics 107
ICMP Statistics 107
TCP Statistics 109
UDP Statistics 111
OSPF Statistics 111
 OSPF Global Statistics 112
IGMP Statistics 116
VRRP Statistics 117
Routing Information Protocol Statistics 118

Management Processor Statistics 119

MP Packet Statistics 119
TCP Statistics 120
UDP Statistics 121
CPU Statistics 121

Access Control List Statistics 122

ACL Statistics 122

SNMP Statistics 123

NTP Statistics 126
Statistics Dump 127

Configuration Commands 129

Viewing and Saving Changes 129

 Saving the Configuration 130

System Configuration 130

 System Host Log Configuration 131

 SSH Server Configuration 133

 RADIUS Server Configuration 134

 TACACS+ Server Configuration 135

 LDAP Server Configuration 138

 NTP Server Configuration 139

 System SNMP Configuration 140

 SNMPv3 Configuration 143

 User Security Model Configuration 145

 SNMPv3 View Configuration 146

 View-based Access Control Model Configuration 147

 SNMPv3 Group Configuration 148

 SNMPv3 Community Table Configuration 148

 SNMPv3 Target Address Table Configuration 149

 SNMPv3 Target Parameters Table Configuration 150

 SNMPv3 Notify Table Configuration 151

System Access Configuration 153

 Management Network Configuration 154

 User Access Control Configuration 155

 System User ID Configuration 156

 Strong Password Configuration 157

 HTTPS Access Configuration 157

Port Configuration 159

 Port Link Configuration 160

 Temporarily Disabling a Port 161

 ACL Port Configuration 161

 Management Port Configuration 162

Layer 2 Configuration 163

 802.1x Configuration 164

 802.1x Global Configuration 164

 802.1x Port Configuration 166

 Rapid Spanning Tree Protocol/Multiple Spanning Tree Protocol Configuration 168

 Common Internal Spanning Tree Configuration 169

 CIST Bridge Configuration 169

 CIST Port Configuration 170

Spanning Tree Configuration	172
Bridge Spanning Tree Configuration	173
Spanning Tree Port Configuration	174
Trunk Configuration	176
IP Trunk Hash Configuration	177
Layer 2 IP Trunk Hash Configuration	177
Link Aggregation Control Protocol Configuration	178
LACP Port Configuration	179
Failover Configuration	180
Failover Trigger Configuration	181
Auto Monitor Configuration	181
VLAN Configuration	182
Protocol-based VLAN Configuration	183
Layer 3 Configuration	185
IP Interface Configuration	186
Default Gateway Configuration	187
IP Static Route Configuration	188
IP Multicast Route Configuration	189
ARP Configuration	190
ARP Static Configuration	190
IP Forwarding Configuration	191
Network Filter Configuration	192
Routing Map Configuration	193
IP Access List Configuration	194
Autonomous System Filter Path Configuration	195
Routing Information Protocol Configuration	196
Routing Information Protocol Interface Configuration	197
Open Shortest Path First Configuration	199
Area Index Configuration	200
OSPF Summary Range Configuration	201
OSPF Interface Configuration	202
OSPF Virtual Link Configuration	204
OSPF Host Entry Configuration	205
OSPF Route Redistribution Configuration	206
OSPF MD5 Key Configuration	206
Border Gateway Protocol Configuration	207
BGP Peer Configuration	208
BGP Redistribution Configuration	210
BGP Aggregation Configuration	211
IGMP Configuration	212
IGMP Snooping Configuration	212

IGMP Relay Configuration	214
IGMP Relay Multicast Router Configuration	215
IGMP Static Multicast Router Configuration	216
IGMP Filtering Configuration	216
IGMP Filter Definition	217
IGMP Filtering Port Configuration	218
IGMP Advanced Configuration	218
Domain Name System Configuration	219
Bootstrap Protocol Relay Configuration	220
VRRP Configuration	220
Virtual Router Configuration	222
Virtual Router Priority Tracking Configuration	224
Virtual Router Group Configuration	225
Virtual Router Group Priority Tracking Configuration	227
VRRP Interface Configuration	228
VRRP Tracking Configuration	229
Quality of Service Configuration	230
802.1p Configuration	230
DSCP Configuration	231
Access Control Configuration	232
Access Control List Configuration	232
Ethernet Filtering Configuration	233
IP version 4 Filtering Configuration	234
TCP/UDP Filtering Configuration	236
Packet Format Filtering Configuration	237
ACL Group Configuration	237
ACL Metering Configuration	238
ACL Re-Mark Configuration	239
Re-Marking In-Profile Configuration	239
Update User Priority Configuration	239
Re-Marking Out-of-Profile Configuration	240
Port Mirroring Configuration	240
Port-Mirroring Configuration	241
Configuration Dump	241
Saving the Active Switch Configuration	242
Restoring the Active Switch Configuration	242

Operations Commands 243

- Operations-Level Port Options 244
- Operations-Level Port 802.1x Options 245
- Operations-Level VRRP Options 245
- Operations-Level BGP Options 246

Boot Options 247

- Scheduled Reboot of the Switch 248
 - Scheduled Reboot Commands 248
- Updating the Switch Software Image 249
 - Loading New Software to Your Switch 249
 - Selecting a Software Image to Run 250
 - Uploading a Software Image from Your Switch 251
- Selecting a Configuration Block 252
- Resetting the Switch 253
 - Accessing the Alteon OS CLI 253

Maintenance Commands 255

- System Maintenance 256
- Forwarding Database Maintenance 256
- Debugging Commands 258
- ARP Cache Maintenance 259
- IP Route Manipulation 260
- IGMP Group Information 261
- Uuencode Flash Dump 261
- TFTP or FTP System Dump Put 262
- Clearing Dump Information 263
- Panic Command 263
- Unscheduled System Dumps 264

Index 265

Preface

The Alteon OS *ISCLI Reference* describes how to configure and use the software with your GbE Switch Module (GbESM). 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.

Who Should Use This Book

This *ISCLI Reference* 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 < >	Indicate a variable to enter based on the description inside the brackets. Do not type the brackets when entering the command. Example: If the command syntax is <code>ping <IP address></code> you enter ping 192.32.10.12
bold body text	Indicates objects such as window names, dialog box names, and icons, as well as user interface objects such as buttons, and tabs.
bold Courier text	Indicates command names, options, and text that you must enter. Example: Use the show ip arp command.
braces { }	Indicate required elements in syntax descriptions where there is more than one option. You must choose only one of the options. Do not type the braces when entering the command. Example: If the command syntax is show portchannel {<1-13> hash information} you enter: show portchannel <1-13> or show portchannel hash or show portchannel information
brackets []	Indicate optional elements in syntax descriptions. Do not type the brackets when entering the command. Example: If the command syntax is show ip ospf interface [<1-248>] you enter show ip ospf interface or show ip ospf interface <1-248>
italic text	Indicates variables in command syntax descriptions. Also indicates new terms and book titles. Example: If the command syntax is show spanning-tree stp <1-128> <1-128> represents a number between 1-128.

Table 1 Typographic Conventions

Typeface or Symbol	Meaning
plain Courier text	Indicates command syntax and system output, for example, prompts and system messages. Example: <code>configure terminal</code>
vertical line	Separates choices for command keywords and arguments. Enter only one of the choices. Do not type the vertical line when entering the command. Example: If the command syntax is <code>show portchannel {<1-13> hash information}</code> you must enter: <code>show portchannel <1-13></code> or <code>show portchannel hash</code> or <code>show portchannel information</code>

How to Get Help

If you need help, service, or technical assistance, see the “Getting help and technical assistance” appendix in the Nortel 10Gb Ethernet Switch Module for IBM BladeCenter *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 Alteon OS CLI. To access the ISCLI, enter the following command and reset the GbESM:

```
Main# boot/mode ISCLI
```

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

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

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.

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. A password is required to enter Privileged EXEC mode. The default password is **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 1-1 on page 19](#).

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

Table 1-1 lists the ISCLI command modes.

Table 1-1 ISCLI Command Modes

Command Mode/Prompt	Command used to enter or exit
User EXEC Router>	Default mode, entered automatically on console Exit: exit or logout
Privileged EXEC Router#	Enter Privileged EXEC mode, from User EXEC mode: enable Exit to User EXEC mode: disable Quit ISCLI: exit or logout
Global Configuration Router(config)#	Enter Global Configuration mode, from Privileged EXEC mode: configure terminal Exit to Privileged EXEC: end or exit
Interface IP Configuration Router(config-ip-if)#	Enter Interface IP Configuration mode, from Global Configuration mode: interface ip <1-250> Exit to Global Configuration mode: exit Exit to Privileged EXEC mode: end
Port Configuration Router(config-if)#	Enter Port Configuration mode, from Global Configuration mode: interface port <port alias or number> Exit to Privileged EXEC mode: exit Exit to Global Configuration mode: end
VLAN Configuration Router(config-vlan)#	Enter VLAN Configuration mode, from Global Configuration mode: vlan <1-4093> Exit to Global Configuration mode: exit Exit to Privileged EXEC mode: end
OSPF Configuration Router(config-router-ospf)#	Enter OSPF Configuration mode, from Global Configuration mode: router ospf Exit to Global Configuration mode: exit Exit to Privileged EXEC mode: end
BGP Configuration Router(config-router-bgp)#	Enter BGP Configuration mode, from Global Configuration mode: router bgp Exit to Global Configuration mode: exit Exit to Privileged EXEC mode: end
RIP Configuration Router(config-router-rip)#	Enter RIP Configuration mode, from Global Configuration mode: router rip Exit to Global Configuration mode: exit Exit to Privileged EXEC mode: end

Table 1-1 ISCLI Command Modes

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

Global Commands

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

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

Table 1-2 Description of Global Commands

Command	Action
<code>?</code>	Provides more information about a specific command or lists commands available at the current level.
<code>exit</code>	Go up one level in the command mode structure.
<code>copy running-config startup-config</code>	Write configuration changes to non-volatile flash memory.
<code>exit</code> or <code>quit</code>	Exit from the command line interface and log out.
<code>ping</code>	<p>Use this command to verify station-to-station connectivity across the network. The format is as follows:</p> <pre>ping <host name> <IP address> [tries (1-32)> [msec delay]] [-m -mgt -e -ext7 -d -data]</pre> <p>Where <i>IP address</i> is the hostname or IP address of the device, <i>tries</i> (optional) is the number of attempts (1-32), <i>msec delay</i> (optional) is the number of milliseconds between attempts. By default, the <code>-m</code> or <code>-mgt</code> option for internal management ports is used. To use the external management port, specify the <code>-e</code> or <code>-ext7</code> option; to use data ports, specify the <code>-d</code> or <code>-data</code> option.</p>
<code>tracert</code>	<p>Use this command to identify the route used for station-to-station connectivity across the network. The format is as follows:</p> <pre>tracert <host name> <IP address> [<max-hops (1-32)> [msec delay]]</pre> <p>Where <i>IP address</i> is the hostname or IP address of the target station, <i>max-hops</i> (optional) is the maximum distance to trace (1-16 devices), and <i>delay</i> (optional) is the number of milliseconds for wait for the response. As with <code>ping</code>, the DNS parameters must be configured if specifying hostnames.</p>

Table 1-2 Description of Global Commands

Command	Action
telnet	<p>This command is used to telnet out of the switch. The format is as follows:</p> <pre>telnet <hostname> <IP address> [port] [-m -mgt -e -ext7 -d -data]</pre> <p>Where <i>IP address</i> is the hostname or IP address of the device. By default, the -m or -mgt option for internal management ports is used. To use the external management port, specify the -e or -ext7 option; to use data ports, specify the -d or -data option.</p>
show history	This command brings up the history of the last 10 commands.
console-log	Enables or disables console logging for the current session.

Command Line Interface Shortcuts

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 GbE Switch Module. 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 GbE Switch Module. Users may display information that has no security or privacy implications, such as switch statistics and current operational state information.
- **oper:** Interaction with the switch is completely passive—nothing can be changed on the GbE Switch Module. Users may display information that has no security or privacy implications, such as switch statistics and current operational state information.
- **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 GbE Switch Module. 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 1-3 User Access Levels

User Account	Description and Tasks Performed	Password
User	The User has no direct responsibility for switch management. He or she can view all switch status information and statistics, but cannot make any configuration changes to the switch.	user
Operator	The Operator 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.	

Table 1-3 User Access Levels

User Account	Description and Tasks Performed	Password
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 2-1 Information Commands

Command Syntax and Usage

show interface link

Displays configuration information about each port, including:

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

Command mode: All

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

show interface information

Displays port status information, including:

- Port alias
- Whether the port uses VLAN Tagging or not
- Port VLAN ID (PVID)
- Port name
- VLAN membership

Command mode: All

For details, see [page 84](#).

show geaport

Displays the GbESM port mapping between the two Gigabit Ethernet Aggregators (GEA).

Command mode: All

For details, see [page 85](#).

Table 2-1 Information Commands

Command Syntax and Usage

show sfp

Displays the status of the 10Gb Small Form Pluggable (XFP) module on each Fiber External Port.

Command mode: All

For details, see [page 86](#).

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 2-2 on page 28](#), with pointers to where detailed information can be found.

Table 2-2 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 the 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 40](#).

show logging messages

Displays most recent syslog messages.

Command mode: All

For details, see [page 41](#).

Table 2-2 System Information Commands

Command Syntax and Usage
show access user Displays configured user names and their status. 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 2-3 SNMPv3 commands

Command Syntax and Usage
show snmp-server v3 user Displays User Security Model (USM) table information. Command mode: All To view the table, see page 30 .
show snmp-server v3 view Displays information about view, subtrees, mask and type of view. Command mode: All To view a sample, see page 32 .
show snmp-server v3 access Displays View-based Access Control information. Command mode: All To view a sample, see page 32 .
show snmp-server v3 group Displays information about the group that includes, the security model, user name, and group name. Command mode: All To view a sample, see page 34 .

Table 2-3 SNMPv3 commands

Command Syntax and Usage

show snmp-server v3 community

Displays information about the community table information.

Command mode: AllTo view a sample, see [page 34](#).

show snmp-server v3 target-address

Displays the Target Address table information.

Command mode: AllTo view a sample, see [page 35](#).

show snmp-server v3 target-parameters

Displays the Target parameters table information.

Command mode: AllTo view a sample, see [page 36](#).

show snmp-server v3 notify

Displays the Notify table information.

Command mode: AllTo view a sample, see [page 36](#).

show snmp-server v3

Displays all the SNMPv3 information.

Command mode: AllTo view a sample, see [page 38](#).

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 2-4 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. Alteon OS supports DES algorithm for privacy. The software also supports two authentication algorithms: MD5 and HMAC-SHA.

SNMPv3 View Table Information

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

The following command displays the SNMPv3 View Table:

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

Command mode: All

View Name	Subtree	Mask	Type
iso	1.3		included
vlv2only	1.3		included
vlv2only	1.3.6.1.6.3.15		excluded
vlv2only	1.3.6.1.6.3.16		excluded
vlv2only	1.3.6.1.6.3.18		excluded

Table 2-5 SNMPv3 View Table Information Parameters

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

SNMPv3 Access Table Information

The access control sub system provides authorization services.

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

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

The following command displays SNMPv3 access information:

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

Command mode: All

Group Name	Prefix	Model	Level	Match	ReadV	WriteV	NotifyV
-----	-----	-----	-----	-----	-----	-----	-----
vlv2grp		snmpv1	noAuthNoPriv	exact	iso	iso	vlv2only
admingrp		usm	authPriv	exact	iso	iso	iso

Table 2-6 SNMPv3 Access Table Information

Field	Description
Group Name	Displays the name of group.
Prefix	Displays the prefix that is configured to match the values.
Model	Displays the security model used, for example, SNMPv1, or SNMPv2 or USM.
Level	Displays the minimum level of security required to gain rights of access. For example, noAuthNoPriv, authNoPriv, or auth-Priv.
Match	Displays the match for the contextName. The options are: exact and prefix.
ReadV	Displays the MIB view to which this entry authorizes the read access.
WriteV	Displays the MIB view to which this entry authorizes the write access.
NotifyV	Displays the Notify view to which this entry authorizes the notify access.

SNMPv3 Group Table Information

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

The following command displays SNMPv3 group information:

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

Command mode: All

Sec Model	User Name	Group Name
-----	-----	-----
snmpv1	vlv2only	vlv2grp
usm	adminmd5	admingrp
usm	adminsha	admingrp

Table 2-7 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	vlv2only	vlv2trap

Table 2-8 SNMPv3 Community Table 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 2-9 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 2-10 SNMPv3 Target Parameters Table Information

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

SNMPv3 Notify Table Information

The following command displays the SNMPv3 Notify Table:

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

Command mode: All

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

Table 2-11 SNMPv3 Notify Table Information

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

SNMPv3 Dump Information

The following command displays SNMPv3 information:

show snmp-server v3

Command mode: All

```

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

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

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

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

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

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

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

```

BladeCenter Information

The following command displays information about the BladeCenter chassis:

show system chassis

Command mode: All

```
IBM BladeCenter Chassis Related Information:

Switch Module Bay = 9
Chassis Type      = Enterprise
POST Results      = 0xff

Management Module Control -

    Default Configuration      = FALSE
    Skip Extended Memory Test  = TRUE
    Disable External Ports     = FALSE
    POST Diagnostics Control   = Normal Diagnostics

    Control Register           = 0x39
    Extended Control Register   = 0x00

Management Module Status Reporting -

    Device PowerUp Complete    = TRUE
    Over Current Fault         = FALSE
    Fault LED                   = OFF
    Primary Temperature Warning = OK
    Secondary Temperature Warning = OK
    Fuse Condition              = OK

    Status Register            = 0x40
    Extended Status Register    = 0x01
```

Chassis information includes details about the chassis and the management module settings.

General System Information

The following command displays system information:

show sys-info

Command mode: All

```
System Information at 0:16:42 Wed Jan 3, 2007
Time zone: No timezone configured

Nortel 10Gb Ethernet Switch Module

Switch is up 5 days, 2 hours, 16 minutes and 42 seconds.
Last boot: 0:00:47 Wed Jan 3, 2007 (power cycle)

MAC address: 00:17:ef:4a:9f:00      IP (If 1) address: 172.20.100.30
Internal Management Port MAC Address: 00:17:ef:4a:9f:02
Internal Management Port IP Address (if 250):
External Management Port MAC Address: 00:17:ef:4a:9f:01
External Management Port IP Address (if 249): 198.208.70.103
Software Version 1.0.0 (FLASH image1), active configuration.

PCBA Part Number:      320486-A
FAB Number:            EL4512027
Serial Number:         ZK12E15E004J
Manufacturing Date:    0608
Hardware Revision:     4
Board Revision:        2
PLD Firmware Version:  5.0

Temperature Sensor 1 (Warning): 46.0 C (Warn at 85.0 C/Recover at
79.0 C)
Temperature Sensor 2 (Shutdown): 46.5 C (Warn at 93.0 C/Recover at
86.0 C)
Temperature Sensor 3 (Exhaust): 34.0 C
Temperature Sensor 4 (Inlet):   42.5 C

Switch is in I/O Module Bay 7
```

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
- IP address of IP interface #1
- Hardware version and part number
- Software image file and version number
- Configuration name
- 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

```

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

This command displays the status of the configured usernames.

Layer 2 Information

Table 2-12 Layer 2 Information Commands

Command Syntax and Usage
<div>show qos transmit-queue information Displays 802.1p Information. Command mode: All For details, see page 48.</div>
<div>show dot1x information Displays 802.1x Information. Command mode: All For details, see page 50.</div>
<div>show spanning-tree In addition to seeing if STG is enabled or disabled, you can view the following STG bridge information:<ul style="list-style-type: none">■ Priority■ Hello interval■ Maximum age value■ Forwarding delay■ Aging timeYou can also see the following port-specific STG information:<ul style="list-style-type: none">■ Port alias and priority■ Cost■ StateCommand mode: All</div>
<div>show spanning-tree stp <1-128> information Displays information about a specific Spanning Tree Group. Command mode: All For details, see page 52.</div>

Table 2-12 Layer 2 Information Commands

Command Syntax and Usage

show spanning-tree mstp cist information

Displays Common internal Spanning Tree (CIST) bridge information, including the following:

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

You can also view port-specific CIST information, including the following:

- Port number and priority
- Cost
- State

Command mode: All

For details, see [page 58](#).

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 60](#).

show vlan

Displays VLAN configuration information for all configured VLANs, including:

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

Command mode: All

For details, see [page 61](#).

show failover

Displays Layer 2 Failover information.

Command mode: All

For details, see [page 62](#).

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 2-13 FDB Information Commands

Command Syntax and Usage

show mac-address-table address <i><MAC address></i>
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, <i>xx:xx:xx:xx:xx:xx</i> . For example, 08:00:20:12:34:56. You can also enter the MAC address using the format, <i>xxxxxxxxxxxx</i> . For example, 080020123456.
Command mode: All
show mac-address-table port <i><port alias or number></i>
Displays all FDB entries for a particular port.
Command mode: All
show mac-address-table vlan <i><1-4095></i>
Displays all FDB entries on a single VLAN.
Command mode: All
show mac-address-table
Displays all entries in the Forwarding Database.
Command mode: All
For more information, see page 46 .
show mac-address-table state { <i>flood forward ifmac ignore trunk unknown</i> }
Displays all FDB entries for a particular state.
Command mode: All

Show All FDB Information

The following command displays Forwarding Database information:

show mac-address-table

Command mode: All

MAC address	VLAN	Port	Trnk	State
-----	----	----	----	-----
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

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.”

If the state for the port is listed as an interface (IF), the MAC address is for a standard VRRP virtual router.

Clearing Entries from the Forwarding Database

To delete a MAC address from the forwarding database (FDB) or to clear the entire FDB, refer to [“Forwarding Database Maintenance” on page 256](#).

Link Aggregation Control Protocol Information

Use these commands to display LACP status information about each port on a GbE Switch Module.

Table 2-14 LACP Information Commands

Command Syntax and Usage
show lacp aggregator Displays information about the LACP aggregator. Command mode: All
show interface port <port alias or number> lacp information Displays LACP information for the port. Command mode: All

Table 2-14 LACP Information Commands

Command Syntax and Usage

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	lacp	adminkey	operkey	selected	prio	attached aggr	trunk
-----	-----	-----	-----	-----	-----	-----	-----
INT1	active	30	30	y	32768	17	19
INT2	active	30	30	y	32768	17	19
INT3	off	3	3	n	32768	--	--
INT4	off	4	4	n	32768	--	--
...							

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

- lacp
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.
- attached aggr
Displays the aggregator associated with each port.
- trunk
This value represents the LACP trunk group number.

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

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
...			
MGT	0	0	1
EXT1	0	0	1
EXT2	0	0	1
EXT3	0	0	1
EXT4	0	0	1

Port	Priority	COSq	Weight
INT1	0	0	1
INT2	0	0	1
...			
MGT	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 2-15 802.1p 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 2-16 802.1p 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

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

show access-control

Command mode: All

```
Current ACL information:
-----
Filter 2 profile:
  Ethernet
    - VID          : 2/0xffff
  Meter
    - Set to disabled
    - Set committed rate : 64
    - Set max burst size : 32
  Re-Mark
    - Set use of TOS precedence to disabled
  Actions          : Permit
No ACL groups configured.
```

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

Table 2-17 ACL Parameter Descriptions

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

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	authorized	initialize	initialize
EXT2	force-auth	authorized	initialize	initialize
*EXT3	force-auth	authorized	initialize	initialize
EXT4	force-auth	authorized	initialize	initialize
*EXT5	force-auth	authorized	initialize	initialize
*EXT6	force-auth	authorized	initialize	initialize
*EXT7	force-auth	authorized	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 2-18 802.1x Parameter Descriptions

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

Spanning Tree Information

The following command displays Spanning Tree information:

show spanning-tree stp <1-128> information

Command mode: All

```

-----
upfast disabled, update 40
-----

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

Current Root:          Path-Cost  Port Hello MaxAge FwdDel
8000 00:16:60:f9:1e:00      0    EXT2   2    20    15

Parameters:  Priority  Hello  MaxAge  FwdDel  Aging
              32768    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  8000-00:16:60:f9:1e:00  8013
EXT4     128    4!      n  FORWARDING  8000-00:16:60:f9:1e:00  8014
EXT5     128     2      n  DISABLED
EXT6     128     2      n  DISABLED
* = 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). 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:

- Slot number
- Port alias and priority
- Cost
- State

The following table describes the STG parameters.

Table 2-19 Spanning Tree Parameter Descriptions

Parameter	Description
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 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.
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.

Table 2-19 Spanning Tree Parameter Descriptions (Continued)

Parameter	Description
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 BLOCKING, LISTENING, LEARNING, FORWARDING, or DISABLED.

RSTP/MSTP Information

The following command displays RSTP/MSTP information:

show spanning-tree stp <1-128> information

Command mode: All

Spanning Tree Group 1: On (RSTP)									
VLANs: 1									
Current Root:									
8000 00:11:58:ae:39:00		Path-Cost 0		Port Hello EXT4 2		MaxAge 20		FwdDel 15	
Parameters:									
Priority 32768		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
EXT5	128	2000	FWD						
EXT6	128	2000	FWD						
* = 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) or the IEEE 802.1s Multiple Spanning Tree Protocol (MSTP).

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

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

You can view port-specific RSTP information, including the following:

- Port number and priority
- Cost
- State

The following table describes the STP parameters in RSTP or MSTP mode.

Table 2-20 RSTP/MSTP Parameter Descriptions

Parameter	Description
Current Root	The Current Root shows information about the root bridge for the Spanning Tree. Information includes the priority (hex) and 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 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.

Table 2-20 RSTP/MSTP Parameter Descriptions (Continued)

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

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
              32768      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
EXT6   128  20000  FWD
EXT3   128  20000  FWD
* = 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 CIST bridge information, including the following:

- Priority
- Maximum age value
- Forwarding delay

You can view port-specific CIST information, including the following:

- Port number and priority
- Cost
- Link type and Port type

The following table describes the CIST parameters.

Table 2-21 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.
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.

Table 2-21 CIST Parameter Descriptions

Parameter	Description
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).
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 (hex) 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, 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

The following command displays VLAN information:

show vlan information

Command mode: All

VLAN	Name	Status	Ports
1	Default VLAN	ena	INT1-INT14 EXT1-EXT6
4094	EXT-Mgmt VLAN	ena	EXT7
4095	Mgmt VLAN	ena	MGT1 MGT2

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
- Port membership of the VLAN
- Protocol-based VLAN information

Failover Information

The following command displays Layer 2 Failover information.

show failover

Command mode: All

```
Current global Failover setting: OFF
Current global VLAN Monitor settings: OFF

Current Trigger 1 setting: disabled
limit 0
Auto Monitor settings:

Current Trigger 2 setting: disabled
limit 0
Auto Monitor settings:

Current Trigger 3 setting: disabled
limit 0
Auto Monitor settings:
...
```

Layer 3 Information

Table 2-22 Layer 3 Information Commands

Command Syntax and Usage

show ip information

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

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 information: Enable status, lnet and lmask
- Port status

Command mode: All except User EXEC

show ip vrrp information

Displays VRRP information.

Command mode: All except User EXEC

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

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 except User EXEC

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 2-23 Route Information Commands

Command Syntax and Usage

show ip route address <IP address>

Displays a single route by destination IP address.

Command mode: All except User EXEC

show ip route gateway <IP address>

Displays routes to a single gateway.

Command mode: All except User EXEC

Table 2-23 Route Information Commands

Command Syntax and Usage

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

Displays routes of a single type.

Command mode: All except User EXEC

For a description of IP routing types, see [Table 2-24 on page 65](#).

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

Displays routes of a single tag.

Command mode: All except User EXEC

For a description of IP routing types, see [Table 2-25 on page 66](#).

```
show ip route interface <1-250>
```

Displays routes on a single interface.

Command mode: All except User EXEC

```
show ip route
```

Displays all routes configured in the switch.

Command mode: All except User EXEC

For more information, see [page 65](#).

Show All IP Route Information

The following command displays IP route information:

show ip route

Command mode: All except User EXEC

Status code: * - best						
Destination	Mask	Gateway	Type	Tag	Metr	If
* 11.0.0.0	255.0.0.0	11.0.0.1	direct	fixed		211
* 11.0.0.1	255.255.255.255	11.0.0.1	local	addr		211
* 11.255.255.255	255.255.255.255	11.255.255.255	broadcast	broadcast		211
* 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
* 12.255.255.255	255.255.255.255	12.255.255.255	broadcast	broadcast		12
* 13.0.0.0	255.0.0.0	11.0.0.2	indirect	ospf	2	211
* 47.0.0.0	255.0.0.0	47.133.88.1	indirect	static		24
* 47.133.88.0	255.255.255.0	47.133.88.46	direct	fixed		24
* 172.30.52.223	255.255.255.255	172.30.52.223	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 2-24 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 2-25 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 2-27 on page 67](#)), VLAN and port for the address, and port referencing information.

Table 2-26 ARP Information Commands

Command Syntax and Usage
show ip arp find <i><IP address></i> Displays a single ARP entry by IP address. Command mode: All except User EXEC
show ip arp interface <i><port alias or number></i> Displays the ARP entries on a single port. Command mode: All except User EXEC
show ip arp vlan <i><1-4093></i> Displays the ARP entries on a single VLAN. Command mode: All except User EXEC

Table 2-26 ARP Information Commands

Command Syntax and Usage

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 except User EXEC

For more information, see [page 67](#).

show ip arp reply

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

Command mode: All except User EXEC

Show All ARP Entry Information

The following command displays ARP information:

show ip arp

Command mode: All except User EXEC

IP address	Flags	MAC address	VLAN	Port
47.80.22.1		00:e0:16:7c:28:86	1	INT6
47.80.23.243	P	00:03:42:fa:3b:30	1	
47.80.23.245		00:c0:4f:60:3e:c1	1	INT6
190.10.10.1	P	00:03:42:fa:3b:30	10	

Referenced ports are the ports that request the ARP entry. So the traffic coming into the referenced ports has the destination IP address. From the ARP entry (the referenced ports), this traffic needs to be forwarded to the egress port (port INT6 in the above example).

The Flag field is interpreted as follows:

Table 2-27 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 ARP address list information:

show ip arp reply

Command mode: All except User EXEC

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 2-28 BGP Peer Information Commands

Command Syntax and Usage

show ip bgp neighbor information

Displays BGP peer information.

Command mode: All except User EXEC

See [page 69](#) 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 except User EXEC

See [page 70](#) for a sample output.

show ip bgp information

Displays the BGP routing table.

Command mode: All except User EXEC

See [page 70](#) 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 except User EXEC

```
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 except User EXEC

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 except User EXEC

Status codes: * valid, > best, i - internal						
Origin codes: i - IGP, e - EGP, ? - incomplete						
Network	Next Hop	Metr	LcPrf	Wght	Path	
*> 10.0.0.0	205.178.21.147	1		256	147	148 i
*>i205.178.15.0	0.0.0.0				0	i
*	205.178.21.147	1		128	147	i
*> 205.178.17.0	205.178.21.147	1		128	147	i
13.0.0.0	205.178.21.147	1		256	147	{35} ?
The 13.0.0.0 is filtered out by rmap; or, a loop detected.						

OSPF Information

Table 2-29 OSPF Information Commands

Command Syntax and Usage

show ip ospf general-information

Displays general OSPF information.

Command mode: All except User EXEC

See [page 72](#) for a sample output.

show ip ospf area information

Displays area information for a particular area index. If no parameter is supplied, it displays area information for all the areas.

Command mode: All except User EXEC

show interface ip {<1-248>} ospf

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

Command mode: All except User EXEC

See [page 73](#) for a sample output.

show ip ospf area-virtual-link information

Displays information about all the configured virtual links.

Command mode: All except User EXEC

show ip ospf neighbor

Displays the status of all the current neighbors.

Command mode: All except User EXEC

show ip ospf summary-range <0-2>

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

Command mode: All except User EXEC

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

Displays the list of summary ranges belonging to NSSA areas.

Command mode: All except User EXEC

show ip ospf routes

Displays OSPF routing table.

Command mode: All except User EXEC

See [page 75](#) for a sample output.

show ip ospf information

Displays the OSPF information.

Command mode: All except User EXEC

OSPF General Information

The following command displays general OSPF information:

show ip ospf general-information

Command mode: All except User EXEC

```
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 ASExtern : 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 [*<1-248>*]

Command mode: All except User EXEC

```
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 2-30 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 except User EXEC

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 except User EXEC

Table 2-30 OSPF Database Information Commands**Command Syntax and Usage****show ip ospf database database-summary**

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

- a) the number of LSAs of each type in each area.
- b) the total number of LSAs for each area.
- c) the total number of LSAs for each LSA type for all areas combined.
- d) the total number of LSAs for all LSA types for all areas combined.

No parameters are required.

Command mode: All except User EXEC

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 except User EXEC

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 except User EXEC

show ip ospf database nssa

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

Command mode: All except User EXEC

show ip ospf database router

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

Command mode: All except User EXEC

show ip ospf database self

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

Command mode: All except User EXEC

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 except User EXEC

show ip ospf database

Displays all the LSAs.

Command mode: All except User EXEC

OSPF Information Route Codes

The following command displays RIP route information:

show ip ospf routes

Command mode: All except User EXEC

```
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 2-31 Routing Information Protocol Commands

Command Syntax and Usage
show ip rip routes Displays RIP routes. Command mode: All except User EXEC For more information, see page 76 .
show interface ip {<1-250>} rip Displays RIP user's configuration. Command mode: All For more information, see page 77 .

RIP Routes Information

The following command displays RIP route information:

show ip rip routes
Command mode: All except User EXEC

```
>> IP Routing#  
  
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 under-going garbage collection with metric = 16. This table does not contain directly connected routes and locally configured static routes.

RIP User Configuration

The following command displays RIP user information:

show interface ip {<1-250>} rip

Command mode: All

```
RIP USER CONFIGURATION :
  RIP on updat 30
  RIP Interface 2 : 102.1.1.1,          enabled
    version 2, listen enabled, supply enabled, default none
    poison disabled, trigg enabled, mcast enabled, metric 1
    auth none, key none
  RIP Interface 3 : 103.1.1.1,          enabled
    version 2, listen enabled, supply enabled, default none
    poison disabled, trigg enabled, mcast enabled, metric 1
```

IP Information

The following command displays Layer 3 information:

show layer3 information

Command mode: All

```
IP information:
  AS number 0

Interface information:
  1: 10.200.30.3      255.255.0.0      10.200.255.255,  vlan 1, up
249: 10.90.90.97     255.255.255.0    10.20.30.255,   vlan 4094, up
250 10.90.90.80      255.255.255.0    10.90.90.255,   vlan 4095, up

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

Current BOOTP relay settings: OFF
  0.0.0.0, 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 2-32 IGMP Multicast Group Information Commands

Command Syntax and Usage
show ip igmp snoop Displays IGMP Snooping information. Command mode: All except User EXEC
show ip igmp relay Displays IGMP Relay information. Command mode: All except User EXEC
show ip igmp mrouter information Displays IGMP Multicast Router information. Command mode: All except User EXEC
show ip igmp filtering Displays current IGMP Filtering parameters. Command mode: All except User EXEC
show ip igmp profile <1-16> Displays information about the current IGMP filter. Command mode: All except User EXEC
show ip igmp groups address <IP address> Displays a single IGMP multicast group by its IP address. Command mode: All except User EXEC

Table 2-32 IGMP Multicast Group Information Commands

Command Syntax and Usage	
show ip igmp groups vlan <i><1-4093></i>	Displays all IGMP multicast groups on a single VLAN. Command mode: All except User EXEC
show ip igmp groups interface <i><port alias or number></i>	Displays all IGMP multicast groups on a single port. Command mode: All except User EXEC
show ip igmp groups portchannel <i><1-13></i>	Displays all IGMP multicast groups on a single trunk group. Command mode: All except User EXEC
show ip igmp groups detail <i><IP address></i>	Displays details about an IGMP multicast group, including source and timer information. Command mode: All except User EXEC
show ip igmp groups	Displays information for all multicast groups. Command mode: All except User EXEC

IGMP Group Information

The following command displays IGMP Group information:

show ip igmp groups

Command mode: All except User EXEC

Note: Local groups (224.0.0.x) are not snooped/relayed and will not appear.				
Group	VLAN	Port	Version	Expires
-----	-----	-----	-----	-----
232.1.1.1	2	EXT4	V2	4:16
236.0.0.1	9	EXT1	V2	

IGMP Group information includes:

- IGMP Group address
- VLAN and port
- IGMP version
- Expiration timer value

IGMP Multicast Router Information

The following command displays Mrouter information:

show ip igmp mrouter information

Command mode: All except User EXEC

VLAN	Port	Version	Expires	Max Query Resp. Time
-----	-----	-----	-----	-----
1	EXT1	V2	4:09	128
2	EXT3	V2	4:09	125
3	EXT4	V2	static	unknown

IGMP Mrouter information includes:

- VLAN and port where the Mrouter is connected
- IGMP version
- Mrouter expiration
- Maximum query response time

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 except User EXEC

VRRP information:				
1:	vrid 2,	205.178.18.210,	if 1,	reter, prio 100, master, server
2:	vrid 1,	205.178.18.202,	if 1,	reter, prio 100, backup
3:	vrid 3,	205.178.18.204,	if 1,	reter, prio 100, master, proxy

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

- Virtual router number
- Virtual router ID and IP address
- Interface number
- Ownership status
 - `owner` identifies the preferred master virtual router. A virtual router is the owner when the IP address of the virtual router and its IP interface are the same.
 - `rener` identifies virtual routers which are not owned by this device.
- Priority value. During the election process, the virtual router with the highest priority becomes master.
- Activity status
 - `master` identifies the elected master virtual router.
 - `backup` identifies that the virtual router is in backup mode.
 - `init` identifies that the virtual router is waiting for a startup event.
For example, once it receives a startup event, it transitions to master if its priority is 255, (the IP address owner), or transitions to backup if it is not the IP address owner.
- Server status. The `server` state identifies virtual routers.
- Proxy status. The proxy state identifies virtual proxy routers, where the virtual router shares the same IP address as a proxy IP address. The use of virtual proxy routers enables redundant switches to share the same IP address, minimizing the number of unique IP addresses that must be configured.

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	10000	full	yes	yes	up
INT2	2	10000	full	yes	yes	up
INT3	3	10000	full	yes	yes	up
INT4	4	10000	full	yes	yes	up
INT5	5	10000	full	yes	yes	down
INT6	6	10000	full	yes	yes	up
INT7	7	10000	full	yes	yes	up
INT8	8	10000	full	yes	yes	up
INT9	9	10000	full	yes	yes	up
INT10	10	10000	full	yes	yes	up
INT11	11	10000	full	yes	yes	up
INT12	12	10000	full	yes	yes	up
INT13	13	10000	full	yes	yes	up
INT14	14	10000	full	yes	yes	up
MGT1	15	100	full	yes	yes	up
MGT2	16	100	full	yes	yes	up
EXT1	17	10000	full	yes	yes	up
EXT2	18	10000	full	yes	yes	up
EXT3	19	10000	full	yes	yes	up
EXT4	20	10000	full	yes	yes	up
EXT5	21	10000	full	yes	yes	down
EXT6	22	10000	full	yes	yes	down
EXT7	23	any	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 an GbE Switch Module slot, including:

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

Port Information

The following command displays port information:

show interface information

Command mode: All except User EXEC

Alias	Port	Tag	Fast	PVID	NAME	VLAN(s)
INT1	1	y	n	1	INT1	1 10
INT2	2	y	n	1	INT2	1
INT3	3	y	n	1	INT3	1
INT4	4	y	n	1	INT4	1
INT5	5	y	n	1	INT5	1
INT6	6	y	n	1	INT6	1
INT7	7	y	n	1	INT7	1
INT8	8	y	n	1	INT8	1
INT9	9	y	n	1	INT9	1
INT10	10	y	n	1	INT10	1
INT11	11	y	n	1	INT11	1
INT12	12	y	n	1	INT12	1
INT13	13	y	n	1	INT13	1
INT14	14	y	n	1	INT14	1
MGT1	15	n	n	4095	MGT1	4095
MGT2	16	n	n	4095	MGT2	4095
EXT1	17	n	n	1	EXT1	1
EXT2	18	n	n	1	EXT2	1
EXT3	19	n	n	1	EXT3	1
EXT4	20	n	n	1	EXT4	1
EXT5	21	n	n	1	EXT5	1
EXT6	22	n	n	1	EXT6	1
EXT7	23	n	n	4094	EXT7	4094

* = 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
- Whether the port uses VLAN tagging or not (y or n)
- Port VLAN ID (PVID)
- Port name

- VLAN membership
- Whether the port is configured for Port Fast Forwarding (**Fast**)
- Whether the port is enabled for FBD Learning (**Lrn**)

Logical Port to GEA Port Mapping

The following command displays information about GEA ports:

show geaport

Command mode: All

Alias	Logical Port	GEA Port(0-based)	GEA Unit
INT1	1	3	0
INT2	2	4	0
INT3	3	5	0
INT4	4	6	0
INT5	5	7	0
INT6	6	8	0
INT7	7	9	0
INT8	8	10	0
INT9	9	11	0
INT10	10	12	0
INT11	11	13	0
INT12	12	14	0
INT13	13	15	0
INT14	14	16	0
MGT1	15	255	0
MGT2	16	255	0
EXT1	17	18	0
EXT2	18	19	0
EXT3	19	0	0
EXT4	20	1	0
EXT5	21	17	0
EXT6	22	2	0
EXT7	23	255	0

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 display correlates the port alias to logical port number, and shows the GEA unit on which each port resides.

Fiber Port SFP Status

The following command displays XFP information:

show sfp

Command mode: All

Port	Device	TX-Enable	RX-Signal	TX-Fault
EXT1	FI-XFP	****	NOT Installed	****
EXT2	SR-XFP	enabled	ok	N/A
EXT3	FI-XFP	****	NOT Installed	****
EXT4	FI-XFP	****	NOT Installed	****
EXT5	FI-XFP	****	NOT Installed	****
EXT6	FI-XFP	****	NOT Installed	****

<= XFP NOT APPROVED

This command displays the status of the 10Gb Small Form Pluggable (XFP) module on each Fiber External Port.

Information Dump

The following command dumps switch information:

show information-dump

Command mode: All

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

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

CHAPTER 3

Statistics Commands

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

Table 3-1 Statistics Commands

Command Syntax and Usage

show layer2 counters

Command mode: All

Displays Layer 2 statistics.

show layer3 counters

Command mode: All

Displays Layer 3 statistics.

show snmp-server counters

Command mode: All

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

show ntp counters

Displays Network Time Protocol (NTP) Statistics.

Command mode: All

See [page 126](#) 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 127](#).

Port Statistics

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

Table 3-2 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 89](#) for sample output.

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

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

Command mode: All

See [page 93](#) for sample output.

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

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

Command mode: All

See [page 94](#) for sample output.

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

Displays interface statistics for the port.

Command mode: All

See [page 96](#) for sample output.

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

Displays IP statistics for the port.

Command mode: All

See [page 98](#) for sample output.

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

Displays link statistics for the port.

Command mode: All

See [page 98](#) for sample output.

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

Clears LACP statistics for the port.

Command mode: All

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 3-3 802.1x 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
eapolLogoff-FramesRx	Total number of EAPOL Logoff frames received
eapolRespId-FramesRx	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
invalidEapol-FramesRx	Total number of invalid EAPOL frames received
eapLengthError-FramesRx	Total number of EAP length error frames received

Table 3-3 802.1x Authenticator Statistics of a Port

Statistics	Description
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**

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 3-4 802.1x Authenticator Diagnostics of a Port

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

Table 3-4 802.1x Authenticator Diagnostics of a Port

Statistics	Description
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.
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 3-5 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 3-6 Ethernet Statistics for Port

Statistics	Description
dot3StatsAlignmentErrors	<p>A count of frames received on a particular interface that are not an integral number of octets in length and do not pass the Frame Check Sequence (FCS) check.</p> <p>The count represented by an instance of this object is incremented when the <code>alignmentError</code> status is returned by the MAC service to the Logical Link Control (LLC) (or other MAC user). Received frames for which multiple error conditions obtained are, according to the conventions of IEEE 802.3 Layer Management, counted exclusively according to the error status presented to the LLC.</p>
dot3StatsFCSErrors	<p>A count of frames received on a particular interface that are an integral number of octets in length but do not pass the Frame Check Sequence (FCS) check.</p> <p>The count represented by an instance of this object is incremented when the <code>frameCheckError</code> status is returned by the MAC service to the LLC (or other MAC user). Received frames for which multiple error conditions obtained are, according to the conventions of IEEE 802.3 Layer Management, counted exclusively according to the error status presented to the LLC.</p>

Table 3-6 Ethernet Statistics for Port

Statistics	Description
dot3StatsSingle-CollisionFrames	<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>
dot3StatsMultiple-CollisionFrames	<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>
dot3StatsLate-Collisions	<p>The number of times that a collision is detected on a particular interface later than 512 bit-times into the transmission of a packet.</p> <p>Five hundred and twelve bit-times corresponds to 51.2 microseconds on a 10 Mbit/s system. A (late) collision included in a count represented by an instance of this object is also considered as a (generic) collision for purposes of other collision-related statistics.</p>
dot3StatsExcessive Collisions	<p>A count of frames for which transmission on a particular interface fails due to excessive collisions.</p>
dot3StatsInternal-MacTransmitErrors	<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>
dot3StatsFrameToo-Longs	<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>

Table 3-6 Ethernet Statistics for Port

Statistics	Description
dot3StatsInternal-MacReceiveErrors	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 dot3StatsFrameTooLongs object, the dot3Stats-AlignmentErrors object, or the dot3StatsFCSErrors object. 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.

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
Discards:                       0                     0
Errors:                         0                    21187

```

Table 3-7 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.

Table 3-7 Interface Statistics for Port

Statistics	Description
<code>ifInDiscards</code>	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.
<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>ifInUnknownProtos</code>	For packet-oriented interfaces, the number of packets received via the interface which were discarded because of an unknown or unsupported protocol. For character-oriented or fixed-length interfaces which support protocol multiplexing, the number of transmission units received via the interface which were discarded because of an unknown or unsupported protocol. For any interface which does not support protocol multiplexing, this counter will always be 0.
<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>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 3-8 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 3-9 Link Statistics

Statistics	Description
linkStateChange	The total number of link state changes.

Layer 2 Statistics

Table 3-10 Layer 2 Statistics Commands

Command Syntax and Usage

show mac-address-table counters

Displays FDB statistics.

Command mode: All

See [page 99](#) for sample output.

clear mac-address-table counters

Clears FDB statistics.

Command mode: All

show interface port <port alias or number> lacp counters

Displays Link Aggregation Control Protocol (LACP) statistics.

Command mode: All

See [page 100](#) for sample output.

clear interface port <port alias or number> lacp counters

Clears Link Aggregation Control Protocol (LACP) statistics.

Command mode: All

show layer2 counters

Dumps all Layer 2 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 except User EXEC

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 3-11 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 3-12 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 repose 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.

Table 3-12 LACP Statistics

Statistic	Description
LACPDUs transmitted	Total number of LACP data units transmitted.
Marker PDUs trans- mitted	Total number of LACP marker data units transmitted.
Marker Rsp PDUs transmitted	Total number of LACP marker response data units transmitted.

Layer 3 Statistics

Table 3-13 Layer 3 Statistics Commands

Command Syntax and Usage

show ip counters

Displays IP statistics.

Command mode: All except User EXEC

See [page 104](#) for sample output.

show ip route counters

Displays route statistics.

Command mode: All except User EXEC

See [page 106](#) for sample output.

show ip arp counters

Displays Address Resolution Protocol (ARP) statistics.

Command mode: All except User EXEC

See [page 107](#) for sample output.

show ip dns counters

Displays Domain Name System (DNS) statistics.

Command mode: All except User EXEC

show ip icmp counters

Displays ICMP statistics.

Command mode: All except User EXEC

See [page 107](#) for sample output.

show ip tcp counters

Displays TCP statistics.

Command mode: All except User EXEC

See [page 109](#) for sample output.

show ip udp counters

Displays UDP statistics.

Command mode: All except User EXEC

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

show ip ospf counters

Displays OSPF statistics.

Command mode: All except User EXEC

See [page 112](#) for sample output.

Table 3-13 Layer 3 Statistics Commands

Command Syntax and Usage
show ip igmp counters Displays IGMP statistics. Command mode: All except User EXEC See page 116 for sample output.
show ip vrrp counters When virtual routers are configured, you can display the following protocol statistics for VRRP: <ul style="list-style-type: none">■ Advertisements received (vrrpInAdvers)■ Advertisements transmitted (vrrpOutAdvers)■ Advertisements received, but ignored (vrrpBadAdvers) Command mode: All except User EXEC See page 117 for sample output.
show ip rip counters Displays Routing Information Protocol (RIP) statistics. Command mode: All except User EXEC See page 118 for sample output.
clear ip igmp [<1-4093>] counters Clears IGMP statistics. Command mode: All above Privileged EXEC
clear ip vrrp counters Clears VRRP statistics. Command mode: All above Privileged EXEC
clear ip counters Clears IP statistics. Use this command with caution as it will delete all the IP statistics. Command mode: All above Privileged EXEC
show layer3 counters Dumps all Layer 3 statistics. Use this command to gather data for tuning and debugging switch performance. If you want to capture dump data to a file, set your communication software on your workstation to capture session data prior to issuing the dump command. Command mode: All except User EXEC

IP Statistics

The following command displays IP statistics:

show ip counters

Command mode: All except User EXEC

Use the following command to clear IP 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 3-14 IP Statistics

Statistics	Description
ipInReceives	The total number of input datagrams received from interfaces, including those received in error.
ipInHdrErrors	The number of input datagrams discarded due to errors in their IP headers, including bad checksums, version number mismatch, other format errors, time-to-live exceeded, errors discovered in processing their IP options, and so forth.
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 3-14 IP Statistics

Statistics	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.
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.

Table 3-14 IP Statistics

Statistics	Description
ipFragOKs	The number of IP datagrams that have been successfully fragmented at this entity (the switch).
ipFragFails	The number of IP datagrams that have been discarded because they needed to be fragmented at this entity (the switch) but could not be, for example, because their Don't Fragment flag was set.
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 Time-To-Live (TTL) field of the IP header of datagrams originated at this entity (the switch), whenever a TTL value is not supplied by the transport layer protocol.
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 except User EXEC

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

Table 3-15 Route Statistics

Statistics	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 except User EXEC

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

Table 3-16 ARP Statistics

Statistics	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.

ICMP Statistics

The following command displays ICMP statistics:

show ip icmp counters

Command mode: All except User EXEC

ICMP statistics:			
icmpInMsgs:	245802	icmpInErrors:	1393
icmpInDestUnreaches:	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	icmpOutDestUnreaches:	15
icmpOutTimeExcds:	0	icmpOutParmProbs:	0
icmpOutSrcQuenchs:	0	icmpOutRedirects:	0
icmpOutEchos:	253777	icmpOutEchoReps:	18
icmpOutTimestamps:	0	icmpOutTimestampReps:	0
icmpOutAddrMasks:	0	icmpOutAddrMaskReps:	0

Table 3-17 ICMP Statistics

Statistics	Description
<code>icmpInMsgs</code>	The total number of ICMP messages which the entity (the switch) received. Note that this counter includes all those counted by <code>icmpInErrors</code> .
<code>icmpInErrors</code>	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).
<code>icmpInDestUnreachs</code>	The number of ICMP Destination Unreachable messages received.
<code>icmpInTimeExcds</code>	The number of ICMP Time Exceeded messages received.
<code>icmpInParmProbs</code>	The number of ICMP Parameter Problem messages received.
<code>icmpInSrcQuenchs</code>	The number of ICMP Source Quench (buffer almost full, stop sending data) messages received.
<code>icmpInRedirects</code>	The number of ICMP Redirect messages received.
<code>icmpInEchos</code>	The number of ICMP Echo (request) messages received.
<code>icmpInEchoReps</code>	The number of ICMP Echo Reply messages received.
<code>icmpInTimestamps</code>	The number of ICMP Timestamp (request) messages received.
<code>icmpInTimestampReps</code>	The number of ICMP Timestamp Reply messages received.
<code>icmpInAddrMasks</code>	The number of ICMP Address Mask Request messages received.
<code>icmpInAddrMaskReps</code>	The number of ICMP Address Mask Reply messages received.
<code>icmpOutMsgs</code>	The total number of ICMP messages which this entity (the switch) attempted to send. Note that this counter includes all those counted by <code>icmpOutErrors</code> .
<code>icmpOutErrors</code>	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.
<code>icmpOutDestUnreachs</code>	The number of ICMP Destination Unreachable messages sent.
<code>icmpOutTimeExcds</code>	The number of ICMP Time Exceeded messages sent.
<code>icmpOutParmProbs</code>	The number of ICMP Parameter Problem messages sent.
<code>icmpOutSrcQuenchs</code>	The number of ICMP Source Quench (buffer almost full, stop sending data) messages sent.

Table 3-17 ICMP Statistics

Statistics	Description
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 except User EXEC

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 3-18 TCP Statistics

Statistics	Description
tcpRtoAlgorithm	The algorithm used to determine the timeout value used for retransmitting unacknowledged octets.
tcpRtoMin	The minimum value permitted by a TCP implementation for the retransmission timeout, measured in milliseconds. More refined semantics for objects of this type depend upon the algorithm used to determine the retransmission timeout. In particular, when the timeout algorithm is rsre(3), an object of this type has the semantics of the LBOUND quantity described in RFC 793.

Table 3-18 TCP Statistics

Statistics	Description
<code>tcpRtoMax</code>	The maximum value permitted by a TCP implementation for the retransmission timeout, measured in milliseconds. More refined semantics for objects of this type depend upon the algorithm used to determine the retransmission timeout. In particular, when the timeout algorithm is <code>rsre(3)</code> , an object of this type has the semantics of the <code>UBOUND</code> quantity described in RFC 793.
<code>tcpMaxConn</code>	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.
<code>tcpActiveOpens</code>	The number of times TCP connections have made a direct transition to the SYN-SENT state from the CLOSED state.
<code>tcpPassiveOpens</code>	The number of times TCP connections have made a direct transition to the SYN-RCVD state from the LISTEN state.
<code>tcpAttemptFails</code>	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.
<code>tcpEstabResets</code>	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.
<code>tcpInSegs</code>	The total number of segments received, including those received in error. This count includes segments received on currently established connections.
<code>tcpOutSegs</code>	The total number of segments sent, including those on current connections but excluding those containing only retransmitted octets.
<code>tcpRetransSegs</code>	The total number of segments retransmitted - that is, the number of TCP segments transmitted containing one or more previously transmitted octets.
<code>tcpInErrs</code>	The total number of segments received in error (for example, bad TCP checksums).
<code>tcpCurBuff</code>	The total number of outstanding memory allocations from heap by TCP protocol stack.
<code>tcpCurConn</code>	The total number of outstanding TCP sessions that are currently opened.
<code>tcpOutRsts</code>	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 except User EXEC

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

Table 3-19 UDP Statistics

Statistics	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.

OSPF Statistics

Table 3-20 OSPF Statistics Commands

Command Syntax and Usage
show ip ospf counters Displays OSPF statistics. Command mode: All except User EXEC See page 112 for sample output.
show ip ospf area counters Displays OSPF area statistics. Command mode: All except User EXEC
show ip ospf interface counters [<1-248>] 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:
hello                   2
start                   0
n2way                   2
adjoint ok              2
negotiation done        2
exchange done           2
bad requests            0
bad sequence            0
loading done            2
nlway                   0
rst_ad                  0
down                    1

Intf change Stats:
hello                   4
down                    2
loop                    0
unloop                  0
wait timer              2
backup                  0
nbr change              5

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

```


Table 3-21 OSPF General Statistics

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

Table 3-21 OSPF General Statistics

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

Table 3-21 OSPF General Statistics

Statistics	Description
Intf Change Stats:	
hello	The sum total number of Hello packets sent on all interfaces and areas.
down	The sum total number of interfaces down in all OSPF areas.
loop	The sum total of interfaces no longer connected to the attached network across all OSPF areas and interfaces.
unloop	The sum total number of interfaces, connected to the attached network in all OSPF areas.
wait timer	The sum total number of times the Wait Timer has been fired, indicating the end of the waiting period that is required before electing a (Backup) Designated Router across all OSPF areas and interfaces.
backup	The sum total number of Backup Designated Routers on the attached network for all OSPF areas and interfaces.
nbr change	The sum total number of changes in the set of bidirectional neighbors associated with any interface across all OSPF areas.
Timers Kickoff:	
hello	The sum total number of times the Hello timer has been fired (which triggers the send of a Hello packet) across all OPSF areas and interfaces.
retransmit	The sum total number of times the Retransmit timer has been fired across all OPSF areas and interfaces.
lsa lock	The sum total number of times the Link State Advertisement (LSA) lock timer has been fired across all OSPF areas and interfaces.
lsa ack	The sum total number of times the LSA Ack timer has been fired across all OSPF areas and interfaces.
dbage	The total number of times the data base age (Dbage) has been fired.
summary	The total number of times the Summary timer has been fired.
ase export	The total number of times the Autonomous System Export (ASE) timer has been fired.

IGMP Statistics

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

show ip igmp counters

Command mode: All except User EXEC

```
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 3-22 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.

VRRP Statistics

Virtual Router Redundancy Protocol (VRRP) support on the 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.

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

- Advertisements received (vrrpInAdvers)
- Advertisements transmitted (vrrpOutAdvers)
- Advertisements received, but ignored (vrrpBadAdvers)

The statistics for the VRRP LAN are displayed:

show ip vrrp counters

Command mode: All except User EXEC

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

Table 3-23 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.

Table 3-23 VRRP Statistics

Statistics	Description
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 except User EXEC

```
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 3-24 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 119](#).

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 120](#).

show mp udp-block

Displays all UDP control blocks that are in use.

Command mode: All

To view a sample output, see [page 121](#).

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 121](#).

MP Packet Statistics

The following command displays MP packet statistics:

show mp packet

Command mode: All except User EXEC

Packet counts:			
allocs:	1722684	frees:	1722684
mediums:	0	mediums hi-watermark:	4
jumbos:	0	jumbos hi-watermark:	0
smalls:	0	smalls hi-watermark:	8
failures:	0		

Table 3-25 Packet Statistics

Statistics	Description
allocs	Total number of packet allocations from the packet buffer pool by the TCP/IP protocol stack.
frees	Total number of times the packet buffers are freed (released) to the packet buffer pool by the TCP/IP protocol stack.
mediums	Total number of packet allocations with size between 128 to 1536 bytes from the packet buffer pool by the TCP/IP protocol stack.
mediums hi-water-mark	The highest number of packet allocation with size between 128 to 1536 bytes from the packet buffer pool by the TCP/IP protocol stack.
jumbos	Total number of packet allocations with more than 1536 bytes from the packet buffer pool by the TCP/IP protocol stack.
jumbos hi-watermark	The highest number of packet allocation with more than 1536 bytes from the packet buffer pool by the TCP/IP protocol stack.
smalls	Total number of packet allocations with size less than 128 bytes from the packet buffer pool by the TCP/IP protocol stack.
smalls 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.
failures	Total number of packet allocation failures 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 3-26 MP Specified TCP Statistics

Statistics	Description
10ad41e8/10ad5790	Memory
0.0.0.0/47.81.27.5	Destination IP address

Table 3-26 MP Specified TCP Statistics

Statistics	Description
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 3-27 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 3-28 ACL Statistics Commands

Command Syntax and Usage

show access-control list <1-384> counters
Displays the Access Control List Statistics for a specific ACL.
Command mode: All
For details, see [page 122](#).

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

ACL Statistics

This option displays statistics for the selected ACL.

show access-control list <1-384> counters
Command mode: All

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

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 3-29 SNMP Statistics

Statistics	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 3-29 SNMP Statistics

Statistics	Description
<code>snmpInASNParseErrs</code>	The total number of ASN.1 or BER errors encountered by the SNMP protocol entity when decoding SNMP Messages received. Note: OSI's method of specifying abstract objects is called ASN.1 (Abstract Syntax Notation One, defined in X.208), and one set of rules for representing such objects as strings of ones and zeros is called the BER (Basic Encoding Rules, defined in X.209). ASN.1 is a flexible notation that allows one to define a variety of data types, from simple types such as integers and bit strings to structured types such as sets and sequences. BER describes how to represent or encode values of each ASN.1 type as a string of eight-bit octets.
<code>snmpEnableAuthTraps</code>	An object to enable or disable the authentication traps generated by this entity (the switch).
<code>snmpOutPkts</code>	The total number of SNMP Messages which were passed from the SNMP protocol entity to the transport service.
<code>snmpInBadTypes</code>	The total number of SNMP Messages which failed ASN parsing.
<code>snmpInTooBigs</code>	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> .
<code>snmpInNoSuchNames</code>	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> .
<code>snmpInBadValues</code>	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> .
<code>snmpInReadOnlyls</code>	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.
<code>snmpInGenErrs</code>	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> .
<code>snmpInTotalReqVars</code>	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).

Table 3-29 SNMP Statistics

Statistics	Description
<code>snmpInTotalSetVars</code>	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).
<code>snmpInGetRequests</code>	The total number of SNMP Get-Request Protocol Data Units (PDUs), which have been accepted and processed by the SNMP protocol entity.
<code>snmpInGetNexts</code>	The total number of SNMP Get-Next Protocol Data Units (PDUs), which have been accepted and processed by the SNMP protocol entity.
<code>snmpInSetRequests</code>	The total number of SNMP Set-Request Protocol Data Units (PDUs), which have been accepted and processed by the SNMP protocol entity.
<code>snmpInGetResponses</code>	The total number of SNMP Get-Response Protocol Data Units (PDUs), which have been accepted and processed by the SNMP protocol entity.
<code>snmpInTraps</code>	The total number of SNMP Trap Protocol Data Units (PDUs), which have been accepted and processed by the SNMP protocol entity.
<code>snmpOutTooBigs</code>	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> .
<code>snmpOutNoSuchNames</code>	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> .
<code>snmpOutBadValues</code>	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> .
<code>snmpOutReadOnlys</code>	Not in use.
<code>snmpOutGenErrs</code>	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> .
<code>snmpOutGetRequests</code>	The total number of SNMP Get-Request Protocol Data Units (PDUs), which have been generated by the SNMP protocol entity.
<code>snmpOutGetNexts</code>	The total number of SNMP Get-Next Protocol Data Units (PDUs), which have been generated by the SNMP protocol entity.
<code>snmpOutSetRequests</code>	The total number of SNMP Set-Request Protocol Data Units (PDUs), which have been generated by the SNMP protocol entity.
<code>snmpOutGetResponses</code>	The total number of SNMP Get-Response Protocol Data Units (PDUs), which have been generated by the SNMP protocol entity.

Table 3-29 SNMP Statistics

Statistics	Description
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

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

The following command displays NTP statistics:

show ntp counters

Command mode: All

```
NTP statistics:
  Primary Server:
    Requests Sent:           17
    Responses Received:      17
    Updates:                 1
  Secondary Server:
    Requests Sent:           0
    Responses Received:      0
    Updates:                 0
  Last update based on response from primary server.
  Last update time: 18:04:16 Tue Jul 13, 2004
  Current system time: 18:55:49 Tue Jul 13, 2004
```

Table 3-30 NTP Statistics

Field	Description
Primary Server	<p>Requests Sent: The total number of NTP requests the switch sent to the primary NTP server to synchronize time.</p> <p>Responses Received: The total number of NTP responses received from the primary NTP server.</p> <p>Updates: The total number of times the switch updated its time based on the NTP responses received from the primary NTP server.</p>
Secondary Server	<p>Requests Sent: The total number of NTP requests the switch sent to the secondary NTP server to synchronize time.</p> <p>Responses Received: The total number of NTP responses received from the secondary NTP server.</p> <p>Updates: The total number of times the switch updated its time based on the NTP responses received from the secondary NTP server.</p>
Last update based on response from primary server	Last update of time on the switch based on either primary or secondary NTP response received.
Last update time	The time stamp showing the time when the switch was last updated.
Current system time	The switch system time when the following command was issued: show ntp counters

Statistics Dump

The following command dumps switch statistics:

show counters

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

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

CHAPTER 4

Configuration Commands

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

Table 4-1 General Configuration Commands

Command Syntax and Usage
show running-config Dumps current configuration to a script file. Command mode: All For details, see page 241 .
copy running-config {ftp tftp} [data-port ext7-port mgt-port] Backs up current configuration to FTP or TFTP server. Select a management port, or press Enter to use the default (management port). Command mode: All For details, see page 242 .
copy {ftp tftp} running-config [data-port ext7-port mgt-port] Restores current configuration from a FTP or TFTP server. Select a management port, or press Enter to use the default (management port). Command mode: All For details, see page 242 .

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 or the management module. 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 252](#).

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 4-2 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

Table 4-2 System Configuration Commands

Command Syntax and Usage	
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
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 <1-1024 characters multi-line ('-' to end)>	Displays login notice immediately before the “Enter password:” prompt. This notice can contain up to 1024 characters and new lines. Command mode: Global configuration
[no] banner <1-80 characters>	Configures a login banner of up to 80 characters. When a user or administrator logs into the switch, the login banner is displayed. It is also displayed as part of the output from the show sys-info command. Command mode: Global configuration
[no] hostname <character string>	Enables or disables displaying of the host name (system administrator’s name) in the Command Line Interface (CLI). Command mode: Global configuration
show system	Displays the current system parameters. Command mode: All

System Host Log Configuration

Table 4-3 Host Log Configuration Commands

Command Syntax and Usage	
[no] logging host {<1-2>} address {<IP address>} [ext7-port mgt-port]	Sets the IP address of the first or second syslog host. Select a management port, or press Enter to use the default (data port). Command mode: Global configuration
logging host {<1-2>} severity {<1-7>}	This option sets the severity level of the first or second syslog host displayed. The default is 7, which means log all the seven severity levels. Command mode: Global configuration

Table 4-3 Host Log Configuration Commands

Command Syntax and Usage

logging host {<1-2>} **facility** {<1-7>}

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

Command mode: Global configuration

logging console

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

Command mode: Global configuration

no logging console

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

Command mode: Global configuration

[no] logging log {<feature>}

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

Command mode: Global configuration

show logging

Displays the current syslog settings.

Command mode: All

SSH Server Configuration

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

NOTE – Most of the following commands are accessible only through a serial connection.

Table 4-4 SSH Server Configuration Commands

Command Syntax and Usage

ssh interval *<0-24>*
Set the interval 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

no ssh enable
Disables the SSH server.
Command mode: Global configuration

Table 4-4 SSH Server Configuration Commands**Command Syntax and Usage****show ssh**

Displays the current SSH server configuration.

Command mode: All**RADIUS Server Configuration****Table 4-5 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 or secondary 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 4-5 RADIUS Configuration Commands

Command Syntax and Usage	
[no] radius-server telnet-backdoor	Enables or disables the RADIUS 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 RADIUS backdoor password for your GbESM, contact your IBM 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 4-6 TACACS+ Server Commands

Command Syntax and Usage	
[no] tacacs-server host <i><IP address></i>	Defines the primary or secondary TACACS+ server address.
Command mode: Global configuration	
[no] tacacs-server host <i><IP address></i> key <i><1-32 characters></i>	This is the primary or secondary shared secret between the switch and the TACACS+ server(s).
Command mode: Global configuration	
[default] tacacs-server port [<i><TCP port number></i>]	Enter the number of the TCP port to be configured, between 1 - 65000. The default is 49.
Command mode: Global configuration	
tacacs-server retransmit <i><1-3></i>	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 <i><4-15></i>	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 telnet-backdoor	Enables or disables the TACACS+ back door for telnet. The telnet command also applies to SSH/SCP connections, and the Browser-Based Interface (BBI). The default is disabled . To obtain the TACACS+ backdoor password for your GbESM, contact your IBM Service and Support line.
Command mode: Global configuration	
[no] tacacs-server secure-backdoor	Enables or disables TACACS+ secure backdoor access through telnet, SSH, or HTTP.
[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	

Table 4-6 TACACS+ Server Commands**Command Syntax and Usage****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

[no] tacacs-server command-logging

Enables or disables TACACS+ command logging.

Command mode: Global configuration

tacacs-server enable

Enables the TACACS+ server.

Command mode: Global configuration

no tacacs-server enable

Disables the TACACS+ server. This is the default setting.

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 4-7 LDAP Configuration commands**Command Syntax and Usage****[no] ldap-server primary-host <IP address>**

Sets the primary LDAP server address.

Command mode: Global configuration

Table 4-7 LDAP Configuration commands

Command Syntax and Usage	
[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
[no] ldap-server telnet-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 IBM 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 4-8 NTP Configuration Commands

Command Syntax and Usage

[no] ntp primary-server *<IP address>* [**ext7-port** | **mgt-port** | **data-port**]

Prompts for the IP addresses of the primary NTP server to which you want to synchronize the switch clock. Select a management port, or press **Enter** to use the default (data port).

Command mode: Global configuration

[no] ntp secondary-server *<IP address>* [**ext7-port** | **mgt-port** | **data-port**]

Prompts for the IP addresses of the secondary NTP server to which you want to synchronize the switch clock. Select a management port, or press **Enter** to use the default (data port).

Command mode: Global configuration

ntp interval *<1-44640>*

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

Command mode: Global configuration

ntp timezone *<time zone offset, in HH:MM>*

Prompts for the NTP time zone offset, in hours and minutes, of the switch you are synchronizing from Greenwich Mean Time (GMT). The offset format is hh:mm (hours:minutes).

Command mode: Global configuration

[no] ntp daylight savings

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

ntp enable

Enables the NTP synchronization service.

Command mode: Global configuration

no ntp enable

Disables the NTP synchronization service.

Command mode: Global configuration

show ntp

Displays the current NTP service settings.

Command mode: All

System SNMP Configuration

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

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

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

SNMP parameters that can be modified include:

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

Table 4-9 System SNMP Commands

Command Syntax and Usage
snmp-server name <i><1-64 characters></i> Configures the name for the system. The name can have a maximum of 64 characters. Command mode: Global configuration
snmp-server location <i><1-64 characters></i> Configures the name of the system location. The location can have a maximum of 64 characters. Command mode: Global configuration
snmp-server contact <i><1-64 characters></i> Configures the name of the system contact. The contact can have a maximum of 64 characters. Command mode: Global configuration

Table 4-9 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 <1-250>

Configures the source interface for SNMP traps.

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 4-10 SNMPv3 Configuration Commands

Command Syntax and Usage
<p>snmp-server user <1-16></p> <p>This command allows you to create a user security model (USM) entry for an authorized user. You can also configure this entry through SNMP.</p> <p>Command mode: Global configuration</p> <p>To view command options, see page 145.</p>
<p>snmp-server view <1-128></p> <p>This command allows you to create different MIB views.</p> <p>Command mode: Global configuration</p> <p>To view command options, see page 146.</p>
<p>snmp-server access <1-32></p> <p>This command allows you to specify access rights. The View-based Access Control Model defines a set of services that an application can use for checking access rights of the user. You need access control when you have to process retrieval or modification request from an SNMP entity.</p> <p>Command mode: Global configuration</p> <p>To view command options, see page 147.</p>
<p>snmp-server group <1-16></p> <p>A group maps the user name to the access group names and their access rights needed to access SNMP management objects. A group defines the access rights assigned to all names that belong to a particular group.</p> <p>Command mode: Global configuration</p> <p>To view command options, see page 148.</p>

Table 4-10 SNMPv3 Configuration Commands

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 148](#).

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 149](#).

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 150](#).

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 151](#).

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 4-11 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	
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 4-12 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

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 4-13 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> 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> 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 4-14 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:

snmp-server user <1-16> name <1-32 characters> on [page 145](#).

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 145](#).

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 4-15 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:

snmp-server user <1-16> name <1-32 characters> on [page 145](#).

Command string: Global configuration

Table 4-15 SNMPv3 Community Table Configuration Commands

Command Syntax and Usage	
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 4-16 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	

Table 4-16 Target Address Table Configuration Commands**Command Syntax and Usage**

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:

snmp-server target-parameters <1-16> **name** <1-32 characters> on [page 150](#).

Command mode: Global configuration

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 4-17 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 4-17 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 145) 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 4-18 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	

Table 4-18 Notify Table Commands

Command Syntax and Usage

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 4-19 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. You will see this command only if you are connected to the switch through the management module.

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

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 4-20 Management Network Configuration Commands

Command Syntax and Usage	
access management-network <i><IP address></i> <i><IP mask></i>	Adds a defined network through which switch access is allowed through Telnet, SNMP, RIP, or the Alteon OS browser-based interface. A range of IP addresses is produced when used with a network mask address. Specify an IP address and mask address in dotted-decimal notation. 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 <i><IP address></i> <i><IP mask></i>	Removes a defined network, which consists of a management network address and a management network mask address. Command mode: Global configuration
show access management-network	Displays the current configuration. Command mode: All except User EXEC

User Access Control Configuration

The following table describes user-access control commands.

NOTE – Passwords can be a maximum of 15 characters.

Table 4-21 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 <1-15 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 <1-15 characters> Sets the operator (oper) password. The operator password can have a maximum of 15 characters. The operator 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 administrator-password <1-15 characters> Sets the administrator (admin) password. The super user administrator has complete access to all information and configuration commands on the GbE Switch Module, 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 4-22 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. Alteon OS 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 password of up to 15 characters maximum.

Command mode: Global configuration

access user <1-10> **enable**

Enables the user ID.

Command mode: Global configuration

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 4-23 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
access user strong-password faillog <1-255> Configures the number of failed login attempts allowed before a security notification is logged. Command mode: Global configuration
show access user strong-password Displays the current Strong Password configuration. Command mode: All except User EXEC

HTTPS Access Configuration

Table 4-24 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

Table 4-24 HTTPS Access Configuration Commands

Command Syntax and Usage

access https generate-certificate

Allows you to generate a certificate to connect to the SSL to be used during the key exchange. A default certificate is created when HTTPS is enabled for the first time. The user can create a new certificate defining the information that they want to be used in the various fields. For example:

- Country Name (2 letter code) []: CA
- State or Province Name (full name) []: Ontario
- Locality Name (for example, city) []: Ottawa
- Organization Name (for example, company) []: Blade
- Organizational Unit Name (for example, section) []: Alteon
- 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

Port Configuration

Use the Port Configuration commands to configure settings for switch ports INT1-INT14 and EXT1-EXT6. If you are configuring management ports (MGT1, MGT2, or EXT7), see [“Management Port Configuration” on page 162](#).

Table 4-25 Port Configuration Commands

Command Syntax and Usage
interface port <i><port alias or number></i> Enter Interface port mode. Command mode: Global configuration
dot1p <i><0-7></i> Configures the port's 802.1p priority level. Command mode: Interface port
pvid <i><1-4093></i> 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 <i><1-64 characters></i> 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] 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. It is disabled by default. Command mode: Interface port
[no] tag-pvid Disables or enables VLAN tag persistence. When disabled, the VLAN tag is removed from packets whose VLAN tag matches the port PVID. The default value is disabled for INT and EXT ports, and enabled for MGT ports. Command mode: Interface port

Table 4-25 Port Configuration Commands

Command Syntax and Usage	
[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 shutdown	Enables the port. Command mode: Interface port
shutdown	Disables the port. (To temporarily disable a port without changing its configuration attributes, refer to “Temporarily Disabling a Port” on page 161.) Command mode: Interface port
show interface port <i><port alias or number></i>	Displays current port parameters. Command mode: All

Port Link Configuration

Use these commands to set flow control for the port link. The speed and mode parameters are fixed for server ports (INT1-INT14) and data ports (EXT1-EXT6), so these options are not available.

Table 4-26 Port Link Configuration Commands

Command Syntax and Usage	
flowcontrol {receive send both}	
no flowcontrol	Sets the flow control. The choices include: <ul style="list-style-type: none">■ Receive flow control■ Transmit flow control■ Both receive and transmit flow control (default)■ No flow control Command mode: Interface port
show interface port <i><port alias or number></i>	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 243](#) for other operations-level commands.

ACL Port Configuration

Table 4-27 ACL/QoS Configuration Commands

Command Syntax and Usage
access-control list <1-384> 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 <1-384> Deletes the specified ACL list from the port. Command mode: Interface port
access-control group <1-384> 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 <1-384> 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

Management Port Configuration

You can use these commands to set port parameters for management ports (MGT1, MGT2, and EXT7). Use this menu to set port parameters for the port link. For MGT1 and MGT2, the values for speed, duplex, and flow control are fixed, and cannot be configured.

Table 4-28 Management Port Configuration Commands

Command Syntax and Usage
<div><div>speed {10 100 1000 auto}</div><div>Sets the link speed. The choices include:</div><div><div>■ 10 Mbps</div><div>■ 100 Mbps</div><div>■ 1000 Mbps</div><div>■ Auto — for auto negotiation</div></div><div>Command mode: Interface port</div></div>
<div><div>duplex {full half any}</div><div>Sets the operating mode. The choices include:</div><div><div>■ Full-duplex</div><div>■ Half-duplex</div><div>■ Any — for auto negotiation (default)</div></div><div>Command mode: Interface port</div></div>
<div><div>[no] flowcontrol {receive send both}</div><div>Sets the flow control. The choices include:</div><div><div>■ Receive flow control</div><div>■ Transmit flow control</div><div>■ Both receive and transmit flow control (default)</div><div>■ No flow control</div></div><div>Command mode: Interface port</div></div>
<div><div>no shutdown</div><div>Enables the port.</div><div>Command mode: Interface port</div></div>
<div><div>shutdown</div><div>Disables the port.</div><div>Command mode: Interface port</div></div>
<div><div>show interface port <port alias or number></div><div>Displays current port parameters.</div><div>Command mode: All</div></div>

Layer 2 Configuration

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

Table 4-29 Layer 2 Configuration Commands

Command Syntax and Usage
<div>vlan <i><1-4093></i> Enter VLAN configuration mode. Command mode: Global configuration To view command options, see page 182.</div>
<div>[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 and path cost by 3000 for all external STP ports. Command mode: Global configuration</div>
<div>spanning-tree uplinkfast max-update-rate <i><10-200></i> Configures the station update rate. The default value is 40. Command mode: Global configuration</div>
<div>show layer2 Displays current Layer 2 parameters. Command mode: All</div>

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 4-30 802.1x 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 4-31 802.1x Global Configuration Commands

Command Syntax and Usage	
dot1x mode {[force-unauthorized auto force-authorized]}	Sets the type of access control for all ports: <ul style="list-style-type: none">■ force-unauthorized - the port is unauthorized unconditionally.■ auto - the port is unauthorized until it is successfully authorized by the RADIUS server.■ force-authorized - the port is authorized unconditionally, allowing all traffic. The default value is <code>force-authorized</code> . 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

Table 4-31 802.1x Global Configuration Commands

Command Syntax and Usage

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 to 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

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

Table 4-31 802.1x Global Configuration Commands**Command Syntax and Usage****default dot1x**

Resets the global 802.1x parameters to their default values.

Command mode: Global configuration

show dot1x

Displays current global 802.1x parameters.

Command mode: All

802.1x 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 4-32 802.1x 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 to the authentication server. The default value is 30 seconds.

Command mode: Interface port

Table 4-32 802.1x 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 following command:	
radius-server timeout	
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	
dot1x apply-global	
Applies current global 802.1x configuration parameters to the port.	
Command mode: Interface port	
show interface port <port alias or number> dot1x	
Displays current 802.1x port parameters.	
Command mode: All	

Rapid Spanning Tree Protocol/Multiple Spanning Tree Protocol Configuration

Alteon OS supports the IEEE 802.1w Rapid Spanning Tree Protocol (RSTP) and IEEE 802.1s Multiple Spanning Tree Protocol (MSTP). MSTP allows you to map many VLANs to a small number of spanning tree groups, each with its own topology.

Up to 32 Spanning Tree Groups can be configured in **mstp** mode. MRST is turned off by default.

Table 4-33 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 a 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 a 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 to traverse before it is dropped. The range is from 4 to 60 hops. The default is 20. Command mode: Global configuration
spanning-tree mode {pvst rstp mstp}	Selects and enables Per VLAN Spanning Tree mode (pvst), Rapid Spanning Tree mode (rstp) or Multiple Spanning Tree mode (mst). The default mode is pvst. Command mode: Global configuration
show spanning-tree mstp mrst	Displays the current RSTP/MSTP configuration. Command mode: All

Common Internal Spanning Tree Configuration

Table 4-34 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 4-34 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 Except User EXEC

CIST Bridge Configuration

CIST bridge parameters are used only when the switch is in MSTP or RSTP mode. CIST parameters do not affect operation of STP/PVST+.

Table 4-35 CIST Bridge Configuration Commands

Command Syntax and Usage
spanning-tree mstp cist-bridge priority {<0-65535>} Configures the CIST bridge priority. The bridge priority parameter controls which bridge on the network is the MSTP root bridge. To make this switch the root bridge, configure the bridge priority lower than all other switches and bridges on your network. The lower the value, the higher the bridge priority. The range is 0 to 65535, and the default is 65535. Command mode: Global configuration
spanning-tree mstp cist-bridge maximum-age {<6-40>} Configures the CIST bridge maximum age. The maximum age parameter specifies the maximum time the bridge waits without receiving a configuration bridge protocol data unit before it reconfigures the MSTP network. The range is 6 to 40 seconds, and the default is 20 seconds. Command mode: Global configuration

Table 4-35 CIST Bridge Configuration Commands

Command Syntax and Usage
spanning-tree mstp cist-bridge forward-delay {<4-30>}
Configures the CIST bridge forward delay parameter. The forward delay parameter specifies the amount of time that a bridge port has to wait before it changes from the listening state to the learning state and from the learning state to the forwarding state. The range is 4 to 30 seconds, and the default is 15 seconds.
Command mode: Global configuration
show spanning-tree mstp cist
Displays the current CIST bridge configuration.
Command mode: All Except User EXEC

CIST Port Configuration

CIST port parameters are used to modify MRST 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 4-36 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 {<1-200000000>}
Configures the CIST port path cost. The port path cost is used to help determine the designated port for a segment. Generally speaking, the faster the port, the lower the path cost. The default is 2000 for 10 Gigabit ports, 20000 for Gigabit ports.
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 4-36 CIST Port Configuration Commands

Command Syntax and Usage
<div><div>spanning-tree mstp cist link-type {auto p2p shared}</div><div>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</div></div>
<div><div>[no] spanning-tree mst cist edge</div><div>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). This command is disabled by default. Command mode: Interface port</div></div>
<div><div>spanning-tree mst cist enable</div><div>Enables MRST on the port. Command mode: Interface port</div></div>
<div><div>no spanning-tree mst cist enable</div><div>Disables MRST on the port. Command mode: Interface port</div></div>
<div><div>show interface port {<port alias or number>} spanning-tree mstp cist</div><div>Displays the current CIST port configuration. Command mode: All Except User EXEC</div></div>

Spanning Tree Configuration

Alteon OS 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 127 and STG 128 are reserved for management).

NOTE – When VRRP is used for active/active redundancy, STG must be enabled.

Table 4-37 Spanning Tree Configuration Commands

Command Syntax and Usage

spanning-tree stp {<1-128>} **vlan** {<1-4093>}

Associates a VLAN with a spanning tree and requires an external VLAN ID as a parameter.

Command mode: Global configuration

no spanning-tree stp {<1-128>} **vlan** {<1-4093>}

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 {<1-128>} **vlan all**

Removes all VLANs from a spanning tree.

Command mode: Global configuration

spanning-tree stp {<1-128>} **enable**

Globally enables Spanning Tree Protocol. STG is turned on by default.

Command mode: Global configuration

no spanning-tree stp {<1-128>} **enable**

Globally disables Spanning Tree Protocol.

Command mode: Global configuration

default spanning-tree <1-128>

Restores a spanning tree instance to its default configuration.

Command mode: Global configuration

show spanning-tree stp {<1-128>}

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
- Bridge aging time

Table 4-38 Bridge Spanning Tree Configuration Commands

Command Syntax and Usage

spanning-tree stp {<1-128>} 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 range is 0 to 65535, and the default is 65535.

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 {<1-128>} 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 {<1-128>} 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 re configures 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

spanning-tree stp {<1-128>} 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

Table 4-38 Bridge Spanning Tree Configuration Commands

Command Syntax and Usage
spanning-tree stp {<1-128>} bridge aging {<1-65535>} Configures the forwarding database aging time. The aging time specifies the amount of time the bridge waits without receiving a packet from a station before removing the station from the forwarding database. The range is 1 to 65535 seconds, and the default is 300 seconds. To disable aging, set this parameter to 0. Command mode: Global configuration
show spanning-tree stp {<1-128>} 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 4-39 Spanning Tree Port Commands

Command Syntax and Usage	
spanning-tree stp {<1-128>} priority {<0-240>}	<p>Configures the port priority. The port priority helps determine which bridge port becomes the designated port. In a network topology that has multiple bridge ports connected to a single segment, the port with the lowest port priority becomes the designated port for the segment. The range is 0 to 255, and the default is 128.</p> <p>RSTP/MSTP: The range is 0 to 240, in steps of 16 (0, 16, 32...) and the default is 128.</p> <p>Command mode: Interface port</p>
spanning-tree stp {<1-128>} path-cost {<1-65535>}	<p>Configures the port path cost. The port path cost is used to help determine the designated port for a segment. Generally speaking, the faster the port, the lower the path cost. The default is 19 for 100Mbps ports, 20000 for 1Gb ports and 2000 for 10Gb ports. A value of 0 (zero) indicates that the default cost will be computed for an auto negotiated link speed.</p> <p>Command mode: Interface port</p>
spanning-tree stp {<1-128>} link {auto p2p shared}	<p>Defines the type of link connected to the port, as follows:</p> <p>auto: Configures the port to detect the link type, and automatically match its settings.</p> <p>p2p: Configures the port for Point-To-Point protocol.</p> <p>shared: Configures the port to connect to a shared medium (usually a hub).</p> <p>Command mode: Interface port</p>
[no] spanning-tree stp {<1-128>} edge	<p>Enables or disables this port as an edge port. An edge port is not connected to a bridge, and can begin forwarding traffic as soon as the link is up. Configure server ports as edge ports (enabled).</p> <p>Command mode: Interface port</p>
spanning-tree stp {<1-128>} enable	<p>Enables STG on the port.</p> <p>Command mode: Interface port</p>
no spanning-tree stp {<1-128>} enable	<p>Disables STG on the port.</p> <p>Command mode: Interface port</p>
show interface port {<port alias or number>} spanning-tree stp {<1-128>}	<p>Displays the current STG port parameters.</p> <p>Command mode: All</p>

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 GbE Switch Module, with the following restrictions:

- Any physical switch port can belong to no more than one trunk group.
- Up to 20 ports/trunks can belong to the same trunk group.
- Best performance is achieved when all ports in a trunk are configured for the same speed.
- Trunking from non-Alteon devices must comply with Cisco® EtherChannel® technology.

By default, each trunk group is empty and disabled.

Table 4-40 Trunk Configuration Commands

Command Syntax and Usage

portchannel {<1-13>} **member** {<port alias or number>}

Adds a physical port to the current trunk group.

Command mode: Global configuration

no portchannel {<1-13>} **member** {<port alias or number>}

Removes a physical port from the current trunk group.

Command mode: Global configuration

portchannel {<1-13>} **enable**

Enables the current trunk group.

Command mode: Global configuration

no portchannel {<1-13>} **enable**

Disables the current trunk group.

Command mode: Global configuration

no portchannel {<1-13>}

Removes the current trunk group configuration.

Command mode: Global configuration

show portchannel {<1-13>}

Displays current trunk group parameters.

Command mode: All

IP Trunk Hash Configuration

Use the following commands to configure IP trunk hash settings for the GbESM.

Table 4-41 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 GbE Switch Module. 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 4-42 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
portchannel hash source-ip-address Enable trunk hashing on the source IP. Command mode: Global configuration

Table 4-42 Layer 2 IP Trunk Hash commands**Command Syntax and Usage****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 4-43 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 4-44 Link Aggregation Control Protocol Commands

Command Syntax and Usage

lacp mode {*off*|*active*|*passive*}

Set the LACP mode for this port, as follows:

- **off**
Turn LACP off for this port. You can use this port to manually configure a static trunk. The default value is **off**.
- **active**
Turn LACP on and set this port to active. Active ports initiate LACPDUs.
- **passive**
Turn LACP on and set this port to passive. Passive ports do not initiate LACPDUs, but respond to LACPDUs from active ports.

Command mode: Interface port

lacp priority {<*1-65535*>}

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

Command mode: Interface port

lacp key {<*1-65535*>}

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

Command mode: Interface port

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

Displays the current LACP configuration for this port.

Command mode: All

Failover Configuration

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

Table 4-45 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	Displays current Layer 2 Failover parameters. Command mode: All

Failover Trigger Configuration

Table 4-46 Failover Trigger Configuration Commands

Command Syntax and Usage
[no] failover trigger <1-8> enable Enables or disables the Failover trigger. Command mode: Global configuration
failover trigger <1-8> limit <0-5> Configures the minimum number of operational links allowed within each trigger before the trigger initiates a failover event. If you enter a value of zero (0), the switch triggers a failover event only when no links in the trigger are operational. Command mode: Global configuration
show failover trigger <1-8> Displays the current failover trigger settings. Command mode: All except User EXEC

Auto Monitor Configuration

Table 4-47 Auto Monitor Configuration Commands

Command Syntax and Usage
failover trigger <1-8> amon trunk <1-13> Adds a trunk group to the Auto Monitor. Command mode: Global configuration
no failover trigger <1-8> amon trunk <1-13> Removes a trunk group from the Auto Monitor. Command mode: Global configuration
failover trigger <1-8> amon admin-key <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 admin-key <1-65535> Removes a LACP admin key from the Auto Monitor. Command mode: Global configuration

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, the VLAN commands are disabled, except VLAN 1, which is enabled all the time. Internal server ports (INTx) and external ports (EXTx) are in VLAN 1 by default. Up to 1024 VLANs can be configured on the GbESM.

Table 4-48 VLAN Configuration Commands

Command Syntax and Usage	
vlan {<1-4093>}	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 {<1-128>}	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	
enable	Enables this VLAN.
Command mode: VLAN	
no enable	Disables this VLAN without removing it from the configuration.
Command mode: VLAN	

Table 4-48 VLAN Configuration Commands

Command Syntax and Usage
no vlan {<1-4093>} 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 4-49 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>} 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
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>} Deletes the selected protocol configuration from the VLAN. Command mode: VLAN

Table 4-49 Protocol VLAN commands**Command Syntax and Usage****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>} tag-pvlan {<port alias or number>}**

Defines a port that will be tagged by the selected protocol on this VLAN.

Command mode: VLAN**show protocol-vlan {<1-8>}**

Displays current parameters for the selected PVLAN.

Command mode: All

Layer 3 Configuration

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

Table 4-50 Layer 3 Configuration Commands

Command Syntax and Usage
interface ip {<1-250>} Configures the IP Interface. Command mode: Global configuration To view command options, see page 186 .
router rip Configures the Routing Interface Protocol. Command mode: Global configuration To view command options, see page 196 .
router ospf Configures OSPF. Command mode: Global configuration To view command options, see page 199 .
router bgp Configures Border Gateway Protocol. Command mode: Global configuration To view command options, see page 207 .
router vrrp Configures Virtual Router Redundancy. Command mode: Global configuration To view command options, see page 220 .
ip router-id <IP address> Sets the router ID. Command mode: Global configuration
show layer3 Displays the current IP configuration. Command mode: All

IP Interface Configuration

The GbE Switch Module can be configured with up to 250 IP interfaces. Each IP interface represents the GbE Switch Module on an IP subnet on your network. The Interface option is disabled by default.

NOTE – To maintain connectivity between the management module and the GbE Switch Module, use the management module interface to change the IP address of the switch.

Table 4-51 IP Interface Configuration Commands

Command Syntax and Usage

interface ip {<1-250>}

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 {<1-4093>}

Configures the VLAN number for this interface. Each interface can belong to one VLAN, though any VLAN can have multiple IP interfaces in it.

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 4-51 IP Interface Configuration Commands

Command Syntax and Usage
no interface ip {<1-250>} Removes this IP interface. Command mode: Interface IP
show interface ip {<1-250>} Displays the current interface settings. Command mode: All

Default Gateway Configuration

NOTE – The switch can be configured with up to six gateways. Gateways one to four are reserved for default gateways. Gateways 253 is reserved for external switch management and gateway 254 is reserved for internal switch management.

This option is disabled by default.

Table 4-52 Default Gateway Commands

Command Syntax and Usage
ip gateway {<1-4, 253, 254>} address {<IP address>} Configures the IP address of the default IP gateway using dotted decimal notation. Command mode: Global configuration
ip gateway {<1-4, 253, 254>} interval {<0-60>} The switch pings the default gateway to verify that it's up. This command sets the time between health checks. The range is from 0 to 60 seconds. The default is 2 seconds. Command mode: Global configuration
ip gateway {<1-4, 253, 254>} 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 {<1-4, 253, 254>} arp-health-check Enables or disables Address Resolution Protocol (ARP) health checks. The default value is disabled . The arp option does not apply to management gateways 253 and 254. Command mode: Global configuration
ip gateway {<1-4, 253, 254>} enable Enables the gateway for use. Command mode: Global configuration

Table 4-52 Default Gateway Commands**Command Syntax and Usage**

no ip gateway {<1-4, 253, 254>} **enable**

Disables the gateway.

Command mode: Global configuration

no ip gateway {<1-4, 253, 254>}

Deletes the gateway from the configuration.

Command mode: Global configuration

show ip gateway {<1-4, 253, 254>}

Displays the current gateway settings.

Command mode: All except User EXEC

IP Static Route Configuration

Up to 128 static routes can be configured.

Table 4-53 IP Static Route Configuration Commands**Command Syntax and Usage**

ip route <IP subnet> <IP netmask> <IP nexthop> [*<interface number>*]

Adds a static route. You will be prompted to enter a destination IP address, destination subnet mask, and gateway address. Enter all addresses using dotted decimal notation.

Command mode: Global configuration

no ip route <IP subnet> <IP netmask> [*<interface number>*]

Removes a static route. The destination address of the route to remove must be specified using dotted decimal notation.

Command mode: Global configuration

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 Route commands.

Table 4-54 IP Multicast Route Configuration Commands

Command Syntax and Usage	
ip mroute <i><IPMC destination></i> <i><vlan number></i> <i><port alias or number></i> <primary backup host> <i><VR ID></i> none	<p>Adds a static multicast route. You will be prompted to enter a destination IP address (in dotted decimal notation), VLAN, and member port. Indicate whether the route is used for a primary, backup, or host multicast router.</p> <p>Command mode: Global configuration</p>
no ip mroute <i><IPMC destination></i> <i><vlan number></i> <i><port alias or number></i> <primary backup host> <i><VR ID></i> none	<p>Removes a static multicast route. The destination address, VLAN, and member port of the route to remove must be specified.</p> <p>Command mode: Global configuration</p>
ip mroute <i><IP address></i> <i><1-4093></i> portchannel <i><1-26></i> {primary backup host} [<1-255>]	<p>Selects a trunk/VLAN combination on which the static multicast router is connected. Trunks 1-13 are static trunks, and trunks 14-26 are dynamic trunks.</p> <p>Command mode: Global configuration</p>
no ip mroute <i><IP address></i> <i><1-4093></i> portchannel <i><1-26></i> {primary backup host} [<1-255>]	<p>Removes a static multicast router from the selected trunk/VLAN combination.</p> <p>Command mode: Global configuration</p>
show ip mroute	<p>Displays the current IP multicast routes.</p> <p>Command mode: All except User EXEC</p>

ARP Configuration

Address Resolution Protocol (ARP) is the TCP/IP protocol that resides within the Internet layer. ARP resolves a physical address from an IP address. ARP queries machines on the local network for their physical addresses. ARP also maintains IP to physical address pairs in its cache memory. In any IP communication, the ARP cache is consulted to see if the IP address of the computer or the router is present in the ARP cache. Then the corresponding physical address is used to send a packet.

Table 4-55 ARP Configuration Commands

Command Syntax and Usage	
ip arp rearp {<2-120>}	Defines re-ARP period in minutes. You can set this duration between 2 and 120 minutes.
Command mode: Global configuration	
show ip arp	Displays the current ARP configurations.
Command mode: All except User EXEC	

ARP Static Configuration

Static ARP entries are permanent in the ARP cache and do not age out like the ARP entries that are learnt 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 4-56 ARP Static Configuration Commands

Command Syntax and Usage	
ip arp <IP address> <MAC address> <VLAN number> <port alias or number>	Adds a permanent ARP entry.
Command mode: Global configuration	
no ip arp {<IP address>}	Deletes a permanent ARP entry.
Command mode: Global configuration	

Table 4-56 ARP Static Configuration Commands

Command Syntax and Usage
clear ip arp-cache Clears static ARP entries. Command mode: Global configuration
show ip arp static Displays current static ARP configuration. Command mode: All except User EXEC

IP Forwarding Configuration

Table 4-57 IP Forwarding Configuration Commands

Command Syntax and Usage
[no] ip routing directed-broadcasts Enables or disables forwarding directed broadcasts. This command is disabled by default. Command mode: Global configuration
ip routing Enables IP forwarding (routing) on the GbE Switch Module. Command mode: Global configuration
no ip routing Disables IP forwarding (routing) on the GbE Switch Module. Forwarding is turned off by default. Command mode: Global configuration
show ip routing Displays the current IP forwarding settings. Command mode: All except User EXEC

Network Filter Configuration

Table 4-58 IP Network Filter Configuration Commands

Command Syntax and Usage

ip match-address <1-256> <IP address> <IP netmask>

Sets the starting IP address for this filter. The default address is 0.0.0.0

Command mode: Global configuration.

ip match-address <1-256> **mask** <IP netmask>

Sets the IP subnet mask that is used with **ip match-address** <match-id> <IP address> to define the range of IP addresses that will be accepted by the peer when the filter is enabled. The default value is 0.0.0.0.

For Border Gateway Protocol (BGP), assign the network filter to 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 4-59 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 194 .
[no] as-path-list <1-8> Configures the Autonomous System (AS) Filter. Command mode: Route map For more information, see page 195 .
[no] as-path-preference <1-65535> Sets the AS path preference of the matched route. You can configure up to three path preferences. Command mode: Route map
[no] local-preference <0-4294967294> Sets the local preference of the matched route, which affects both inbound and outbound directions. The path with the higher preference is preferred. Command mode: Route map
[no] metric <1-4294967294> Sets the metric of the matched route. Command mode: Route map
[no] metric-type {type1 type2} Assigns the type of OSPF metric. The default is type 1. <ul style="list-style-type: none">■ Type 1—External routes are calculated using both internal and external metrics.■ Type 2—External routes are calculated using only the external metrics. Type 1 routes have more cost than Type 2.■ none—Removes the OSPF metric. Command mode: Route map

Table 4-59 Routing Map Configuration Commands

Command Syntax and Usage	
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 4-60 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 192 for details.	
[no] access-list <1-8> metric <1-4294967294>	Sets the metric value in the AS-External (ASE) LSA.
Command mode: Route map	

Table 4-60 IP Access List Configuration Commands

Command Syntax and Usage	
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 4-61 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

Table 4-61 AS Filter Configuration Commands**Command Syntax and Usage****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 4-62 Routing Information Protocol Commands**Command Syntax and Usage****router rip**

Enter Router RIP configuration mode.

Command mode: Router RIP**timers update** {<1-120>}

Configures the time interval for sending for RIP table updates, in seconds.

The default value is 30 seconds.

Command mode: Router RIP**enable**Globally turns RIP **on**.**Command mode:** Router RIP**no enable**Globally turns RIP **off**.**Command mode:** Router RIP**show ip rip**

Displays the current RIP configuration.

Command mode: All except User EXEC

Routing Information Protocol Interface Configuration

RIP Commands are used for configuring Routing Information Protocol parameters. This option is turned off by default.

NOTE – Do not configure RIP1 parameters if your routing equipment uses RIP version 2.

Table 4-63 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
[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

Table 4-63 RIP Interface Commands**Command Syntax and Usage**

[no] ip rip default-action {none|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 {<1-250>} rip

Displays the current RIP configuration.

Command mode: All except User EXEC

Open Shortest Path First Configuration

Table 4-64 OSPF Configuration Commands

Command Syntax and Usage

router ospf

Enter Router OSPF configuration mode.

Command mode: Global configuration

area-range <0-2>

Configures summary routes for up to 16 IP addresses.

Command mode: Router OSPF

See [page 201](#) to view command options.

ip ospf <1-248>

Configures the OSPF interface.

Command mode: Interface IP

See [page 202](#) 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 204](#) to view command options.

message-digest-key <1-255> **md5-key** <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 205](#) to view command options.

lsdb-limit <0-2000>

Sets the link state database limit.

Command mode: Router OSPF

default-information <1-16777214> <AS value (1-2)>/none

Sets one default route among multiple choices in an area. Use none for no default.

Command mode: Router OSPF

Table 4-64 OSPF Configuration Commands**Command Syntax and Usage****enable**

Enables OSPF on the GbE Switch Module.

Command mode: Router OSPF

no enable

Disables OSPF on the GbE Switch Module.

Command mode: Router OSPF

show ip ospf

Displays the current OSPF configuration settings.

Command mode: All except User EXEC

Area Index Configuration**Table 4-65** 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

Table 4-65 Area Index Configuration Commands

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

OSPF Summary Range Configuration

Table 4-66 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 GbE Switch Module. Command mode: Router OSPF	

Table 4-66 OSPF Summary Range Configuration Commands**Command Syntax and Usage****[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 4-67** OSPF Interface Configuration Commands**Command Syntax and Usage****ip ospf area <0-2>**

Configures the OSPF area index.

Command mode: Interface IP**ip ospf priority <0-255>**

Configures the priority value for the GbE Switch Module's OSPF interfaces.

(A priority value of 255 is the highest and 1 is the lowest. A priority value of 0 specifies that the interface cannot be used as Designated Router (DR) or Backup Designated Router (BDR).)

Command mode: Interface IP**ip ospf cost <1-65535>**

Configures cost set for the selected path—preferred or backup. Usually the cost is inversely proportional to the bandwidth of the interface. Low cost indicates high bandwidth.

Command mode: Interface IP

Table 4-67 OSPF Interface Configuration Commands

Command Syntax and Usage	
ip ospf hello-interval <1-65535>	Configures the interval in seconds between the hello packets for the interfaces.
Command mode: Interface IP	
ip ospf dead-interval <1-65535>	Configures the health parameters of a hello packet, which is set for an interval of seconds before declaring a silent router to be down.
Command mode: Interface IP	
ip ospf transit-delay <1-3600>	Configures the transit delay in seconds.
Command mode: Interface IP	
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	
ip ospf enable	Enables OSPF interface.
Command mode: Interface IP	
no ip ospf enable	Disables OSPF interface.
Command mode: Interface IP	
no ip ospf	Deletes OSPF interface.
Command mode: Interface IP	
show interface ip <1-250> ospf	Displays the current settings for OSPF interface.
Command mode: All except User EXEC	

OSPF Virtual Link Configuration

Table 4-68 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>

Configures the authentication parameters of a hello packet, which is set to be in an interval of seconds.

Command mode: Router OSPF

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

Configures the health parameters of a hello packet, which is set to be in an interval of seconds. Default is 40 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

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

Table 4-68 OSPF Virtual Link Configuration Commands

Command Syntax and Usage
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 4-69 OSPF Host Entry Configuration Commands

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

OSPF Route Redistribution Configuration .

Table 4-70 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** <*/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 4-71 OSPF MD5 Key Configuration Command Options

Command Syntax and Usage

message-digest-key <*/1-255*> **md5-key** <*key string*>

Sets the authentication key for this OSPF packet.

Command mode: Router OSPF

no message-digest-key <*/1-255*>

Deletes the authentication key for this OSPF packet.

Command mode: Router OSPF

show ip ospf message-digest-key <*/1-255*>

Displays the current MD5 key configuration.

Command mode: All except User EXEC

Border Gateway Protocol Configuration

Border Gateway Protocol (BGP) is an Internet protocol that enables routers on a network to share routing information with each other and advertise information about the segments of the IP address space they can access within their network with routers on external networks. BGP allows you to decide what is the “best” route for a packet to take from your network to a destination on another network, rather than simply setting a default route from your border router(s) to your upstream provider(s). You can configure BGP either within an autonomous system or between different autonomous systems. When run within an autonomous system, it's called internal BGP (iBGP). When run between different autonomous systems, it's called external BGP (eBGP). BGP is defined in RFC 1771.

BGP commands enable you to configure the switch to receive routes and to advertise static routes, fixed routes and virtual server IP addresses with other internal and external routers. In the current Alteon OS implementation, the GbE Switch Module does not advertise BGP routes that are learned from other BGP “speakers”.

The BGP command option is turned off by default.

NOTE – Fixed routes are subnet routes. There is one fixed route per IP interface.

Table 4-72 Border Gateway Protocol Commands

Command Syntax and Usage	
router bgp	Enter Router BGP configuration mode. Command mode: Global configuration
neighbor <I-16>	Configures each BGP <i>peer</i> : 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 208 .
as <I-65535>	Set Autonomous System number. Command mode: Router BGP

Table 4-72 Border Gateway Protocol Commands

Command Syntax and Usage	
local-preference <i><0-4294967294></i>	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 4-73 BGP Peer Configuration Commands

Command Syntax and Usage	
neighbor <i><1-16></i> remote-address <i><IP address></i>	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 <i><1-16></i> remote-as <i><1-65535></i>	Sets the remote autonomous system number for the specified peer.
Command mode: Router BGP	
neighbor <i><1-16></i> timers hold-time <i><0, 3-65535></i>	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. It is set at 90 seconds by default.
Command mode: Router BGP	

Table 4-73 BGP Peer Configuration Commands

Command Syntax and Usage	
neighbor <1-16> timers keep-alive <0, 1-21845>	Sets the keep-alive time for the specified peer in seconds. It is set at 0 by default.
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.
Command mode: Router BGP	
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	

Table 4-73 BGP Peer Configuration Commands**Command Syntax and Usage****no neighbor** <I-16> **shutdown**

Enables this peer configuration.

Command mode: Router BGP**neighbor** <I-16> **shutdown**

Disables this peer configuration.

Command mode: Router BGP**no neighbor** <I-16>

Deletes this peer configuration.

Command mode: Router BGP**show ip bgp neighbor** [<I-16>]

Displays the current BGP peer configuration.

Command mode: All except User EXEC**BGP Redistribution Configuration****Table 4-74 BGP Redistribution Configuration Commands****Command Syntax and Usage****[no] neighbor** <I-16> **redistribute default-metric** <I-4294967294>

Sets default metric of advertised routes.

Command mode: Router BGP**[no] neighbor** <I-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

Table 4-74 BGP Redistribution Configuration Commands

Command Syntax and Usage
[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
[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 4-75 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 4-75 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 4-76 describes the commands used to configure basic IGMP parameters.

Table 4-76 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 except User EXEC

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 4-77 describes the commands used to configure IGMP Snooping.

Table 4-77 IGMP Snooping Configuration Commands

Command Syntax and Usage	
ip igmp snoop enable	Enables IGMP Snooping.
Command mode: Global configuration	
no ip igmp snoop enable	Disables IGMP Snooping.
Command mode: Global configuration	
ip igmp snoop mrouter-timeout <1-600>	Configures the timeout value for IGMP Membership Queries (mrouter). Once the timeout value is reached, the switch removes the multicast router from its IGMP table, if the proper conditions are met. The range is from 1 to 600 seconds. The default is 255 seconds.
Command mode: Global configuration	
ip igmp snoop source-ip <IP address>	Configures the source IP address used as a proxy for IGMP Group Specific Queries.
Command mode: Global configuration	
ip igmp snoop vlan <1-4093>	Adds the selected VLAN(s) to IGMP Snooping.
Command mode: Global configuration	
no ip igmp snoop vlan <1-4093> enable	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 except User EXEC	

IGMP Relay Configuration

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

Table 4-80 describes the commands used to configure IGMP Relay.

Table 4-78 IGMP Relay Configuration Commands

Command Syntax and Usage	
<code>ip igmp relay enable</code>	Enables IGMP Relay. Command mode: Global configuration
<code>no ip igmp relay enable</code>	Disables IGMP Relay. Command mode: Global configuration
<code>ip igmp relay vlan <1-4093></code>	Adds the VLAN to the list of IGMP Relay VLANs. Command mode: Global configuration
<code>no ip igmp relay vlan <1-4093></code>	Removes the VLAN from the list of IGMP Relay VLANs. Command mode: Global configuration
<code>ip igmp relay report <0-150></code>	Configures the interval between unsolicited Join reports sent by the switch, in seconds. The default value is 10. Command mode: Global configuration
<code>show ip igmp relay</code>	Displays the current IGMP Relay configuration. Command mode: All except User EXEC

IGMP Relay Multicast Router Configuration

Table 4-80 describes the commands used to configure multicast routers for IGMP Relay.

Table 4-79 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	
ip igmp relay mrouter <1-2> enable	Enables the multicast router.
Command mode: Global configuration	
no ip igmp relay mrouter <1-2> enable	Disables the multicast router.
Command mode: Global configuration	
no ip igmp relay mrouter <1-2>	Deletes the multicast router from IGMP Relay.
Command mode: Global configuration	

IGMP Static Multicast Router Configuration

Table 4-80 describes the commands used to configure a static multicast router.

NOTE – When you configure a static multicast router on a VLAN, the process of learning multicast routers is disabled for that VLAN.

Table 4-80 IGMP Static Multicast Router Configuration Commands

Command Syntax and Usage
ip igmp mrouter <i><port alias or number></i> <i><1-4093></i> <i><version (1-2)></i> 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. Note: Port number must be an external port (EXT1-EXT6). Command mode: Global configuration
no ip igmp mrouter <i><port alias or number></i> <i><1-4093></i> <i><version (1-2)></i> Removes a static multicast router from the selected port/VLAN combination. 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 4-81 describes the commands used to configure an IGMP filter.

Table 4-81 IGMP Filtering Configuration Commands

Command Syntax and Usage
ip igmp profile <i><1-16></i> Configures the IGMP filter. Command mode: Global configuration To view command options, see page 217 .
ip igmp filtering Enables IGMP filtering globally. Command mode: Global configuration

Table 4-81 IGMP Filtering Configuration Commands

Command Syntax and Usage
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 except User EXEC

IGMP Filter Definition

Table 4-82 describes the commands used to define an IGMP filter.

Table 4-82 IGMP Filter Definition Commands

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

IGMP Filtering Port Configuration

[Table 4-83](#) describes the commands used to configure a port for IGMP filtering.

Table 4-83 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 4-80](#) describes the commands used to configure advanced IGMP parameters.

Table 4-84 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
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

Table 4-84 IGMP Advanced Configuration Commands

Command Syntax and Usage
<div><div>[no] ip igmp fastleave <1-4093></div><div>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.</div><div>Command mode: Global configuration</div></div>
<div><div>[no] ip igmp flood</div><div>Configures the switch to flood unregistered IP multicast reports to all ports.</div><div>Command mode: Global configuration</div></div>

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 4-85 Domain Name Service Commands

Command Syntax and Usage
<div><div>[no] ip dns primary-server <IP address></div><div>You will be prompted to set the IP address for your primary DNS server. Use dotted decimal notation.</div><div>Command mode: Global configuration</div></div>
<div><div>[no] ip dns secondary-server <IP address></div><div>You will be prompted to set the IP address for your secondary DNS server. If the primary DNS server fails, the configured secondary will be used instead. Enter the IP address using dotted decimal notation.</div><div>Command mode: Global configuration</div></div>
<div><div>[no] ip dns domain-name <string></div><div>Sets the default domain name used by the switch. For example: mycompany.com</div><div>Command mode: Global configuration</div></div>
<div><div>show ip dns</div><div>Displays the current Domain Name System settings.</div><div>Command mode: All except User EXEC</div></div>

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 GbE Switch Module.

BOOTP relay is turned off by default.

Table 4-86 Bootstrap Protocol Relay Configuration Commands

Command Syntax and Usage	
[no] ip bootp-relay server <IP address>	Sets the IP address of the first or second BOOTP server. Command mode: Global configuration
ip bootp-relay enable	Globally turns on BOOTP relay. Command mode: Global configuration
no ip bootp-relay enable	Globally turns off BOOTP relay. Command mode: Global configuration
show ip bootp-relay	Displays the current BOOTP relay configuration. Command mode: All except User EXEC

VRRP Configuration

Virtual Router Redundancy Protocol (VRRP) support on GbE Switch Modules 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. Alteon OS has extended VRRP to include virtual servers as well, allowing for full active/active redundancy between switches. For more information on VRRP, see the “High Availability” chapter in the Alteon OS *Application Guide*.

Table 4-87 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 except User EXEC

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 4-88 VRRP Virtual Router Configuration Commands

Command Syntax and Usage

virtual-router <1-250> **virtual-router-id** <1-255>

Defines the virtual router ID. This is used in conjunction with the **[no] virtual-router <vr-id> address <IP address>** command below to define a virtual router on this switch. To create a pool of VRRP-enabled routing devices which can provide redundancy to each other, each participating VRRP device must be configured with the same virtual router.

The *vr-id* for standard virtual routers (where the virtual router IP address is not the same as any virtual server) can be any integer between 1 and 255. The default value is 1.

All *vr-id* values must be unique within the VLAN to which the virtual router’s IP interface belongs.

Command mode: Router VRRP

[no] virtual-router <1-250> **address** <IP address>

Defines the IP address for this virtual router using dotted decimal notation. This is used in conjunction with the *vr-id* (above) to configure the same virtual router on each participating VRRP device. The default address is 0.0.0.0.

Command mode: Router VRRP

virtual-router <1-250> **interface** <1-248>

Selects a switch IP interface. If the IP interface has the same IP address as the *addr* option above, this switch is considered the “owner” of the defined virtual router. An owner has a special priority of 255 (highest) and will always assume the role of master router, even if it must pre-empt another virtual router which has assumed master routing authority. This pre-emption occurs even if the *preem* option below is disabled. The default value is 1.

Command mode: Router VRRP

Table 4-88 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. This can be any integer between 1 and 254. The default value is 100.

During the master router election process, the routing device with the highest virtual router priority number wins. If there is a tie, the device with the highest IP interface address wins. If this virtual router's IP address 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 pre-emption. When enabled, if this virtual router 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 `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

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 pre-emption 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 4-89 VRRP Priority Tracking Configuration Commands

Command Syntax and Usage

[no] virtual-router <I-1024> 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 <I-1024> 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 <I-1024> 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 <I-1024> 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 GbE Switch Module 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 GbE Switch Modules in a hot-standby failover configuration, where only one switch is active at any time.

Table 4-90 VRRP Virtual Router Group Configuration Commands

Command Syntax and Usage

group virtual-router-id <1-255>

Defines the virtual router ID.

The `vr-id` for standard virtual routers (where the virtual router IP address is not the same as any virtual server) can be any integer between 1 and 255. All `vr-id` values must be unique within the VLAN to which the virtual router's IP interface (see `if` below) belongs. The default virtual router ID is 1.

Command mode: Router VRRP

group interface <1-248>

Selects a switch IP interface. The default switch IP interface number is 1.

Command mode: Router VRRP

group priority <1-254>

Defines the election priority bias for this virtual router group. This can be any integer between 1 and 254. The default value is 100.

During the master router election process, the routing device with the highest virtual router priority number wins. If there is a tie, the device with the highest IP interface address wins. If this virtual router's IP address (`addr`) is the same as the one used by the IP interface, the priority for this virtual router will automatically be set to 255 (highest).

When priority tracking is used, this base priority value can be modified according to a number of performance and operational criteria.

Command mode: Router VRRP

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

Table 4-90 VRRP Virtual Router Group Configuration Commands

Command Syntax and Usage	
[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 <code>preemption</code> is disabled, this virtual router will always pre-empt any other master if this switch is the owner (the IP interface address and virtual router address are the same). By default, this option is enabled. 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 4-91 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* (1 to 248) 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 4-92 VRRP Interface Commands

Command Syntax and Usage

interface <1-248> authentication { password none }
Defines the type of authentication that will be used: none (no authentication) or password (password authentication).
Command mode: Router VRRP
interface <1-248> 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 <1-248>
Clears the authentication configuration parameters for this IP interface. The IP interface itself is not deleted.
Command mode: Router VRRP
show ip vrrp interface <1-248>
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 224](#)), the priority level for the virtual router is increased by a defined amount.

Table 4-93 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 224) are enabled.

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 4-94 802.1p Configuration Commands

Command Syntax and Usage	
qos transmit-queue mapping <i><priority (0-7)></i> <i><queue (0-1)></i>	
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 (0-7) that handles the matching traffic.	
Command mode: Global configuration	
qos transmit-queue weight-cos <i><queue (0-1)></i> <i><weight (0-15)></i>	
Configures the weight of the selected Class of Service queue (COSq). Enter the queue number (0-1), followed by the scheduling weight (0-15).	
Command mode: Global configuration	
show qos transmit-queue	
Displays the current 802.1p parameters.	
Command mode: All 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 4-95 DSCP Configuration Commands

Command Syntax and Usage	
qos dscp dscp-mapping <i><DSCP value></i> <i><new DSCP value></i>	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 <i><DSCP value></i> <i><priority (0-7)></i>	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 4-96 General ACL Configuration Commands

Command Syntax and Usage
[no] access-control list <1-384> Configures an Access Control List. Command mode: Global configuration To view command options, see page 232 .
[no] access-control group <1-384> Configures an ACL Group. Command mode: Global configuration To view command options, see page 237 .
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 4-97 ACL Configuration Commands

Command Syntax and Usage
[no] access-control list <1-384> egress-port <port alias or number> Configures the ACL to function on egress packets. Command mode: Global configuration
access-control list <1-384> action {permit deny class-of-service <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 Class of Service queue that handles the packets. Command mode: Global configuration
access-control list <1-384> statistics Enables or disables the statistics collection for the Access Control List. Command mode: All except User EXEC

Table 4-97 ACL Configuration Commands

Command Syntax and Usage
default access-control list <1-384> Resets the ACL parameters to their default values. Command mode: Global configuration
show access-control list <1-384> 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 4-98 Ethernet Filtering Configuration Commands

Command Syntax and Usage
[no] access-control list <1-384> ethernet source-mac-address {<MAC address>} {<MAC mask>} Defines the source MAC address for this ACL. Command mode: Global configuration
[no] access-control list <1-384> ethernet destination-mac-address {<MAC address>} {<MAC mask>} Defines the destination MAC address for this ACL. Command mode: Global configuration
[no] access-control list <1-384> ethernet vlan {<VLAN ID>} {<VLAN mask>} Defines a VLAN number and mask for this ACL. Command mode: Global configuration
[no] access-control list <1-384> ethernet ethernet-type {arp ip ipv6 mpls rarp any 0xXXXX} Defines the Ethernet type for this ACL. Command mode: Global configuration
[no] access-control list <1-384> ethernet priority <0-7> Defines the Ethernet priority value for the ACL. Command mode: Global configuration
default access-control list <1-384> ethernet Resets Ethernet parameters for the ACL to their default values. Command mode: Global configuration

Table 4-98 Ethernet Filtering Configuration Commands

Command Syntax and Usage
no access-control list <1-384> ethernet Removes Ethernet parameters for the ACL. Command mode: Global configuration
show access-control list {<1-384>} ethernet Displays the current Ethernet parameters for the ACL. Command mode: All except User EXEC

IP version 4 Filtering Configuration

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

Table 4-99 IP version 4 Filtering Configuration Commands

Command Syntax and Usage

[no] access-control list <1-384> **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 <1-384> **ipv4 destination-ip-address** <IP address> <IP mask>

Defines a destination IP address for the ACL. If defined, traffic with this destination IP address will match this ACL.

Command mode: Global configuration

[no] access-control list <1-384> **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.

<u>Number</u>	<u>Name</u>
1	icmp
2	igmp
6	tcp
17	udp
89	ospf
112	vrrp

Command mode: Global configuration

Table 4-99 IP version 4 Filtering Configuration Commands

Command Syntax and Usage	
[no] access-control list <1-384> 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 <1-384> ipv4	Resets the IPv4 parameters for the ACL to their default values.
Command mode: Global configuration	
show access-control list <1-384> 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 4-100 TCP/UDP Filtering Configuration Commands

Command Syntax and Usage

[no] access-control list <1-384> tcp-udp source-port <1-65535>	
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:	
<u>Number</u>	<u>Name</u>
20	ftp-data
21	ftp
22	ssh
23	telnet
25	smtp
37	time
42	name
43	whois
53	domain
69	tftp
70	gopher
79	finger
80	http
Command mode: Global configuration	

[no] access-control list <1-384> tcp-udp destination-port <1-65535>	
Defines a destination port for the ACL. If defined, traffic with the specified TCP or UDP destination port will match this ACL. Specify the port number, just as with <code>sport</code> above.	
Command mode: Global configuration	

[no] access-control list <1-384> tcp-udp flags <flag (0x0-0x3f)>	
Defines a TCP/UDP flag for the ACL.	
Command mode: Global configuration	

default access-control list <1-384> tcp-udp	
Resets the TCP/UDP parameters for the ACL to their default values.	
Command mode: Global configuration	

show access-control list <1-384> 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 4-101 Packet Format Filtering Configuration Commands

Command Syntax and Usage	
<code>access-control list <1-384> packet-format ethernet {ethertype2 snap llc}</code>	Defines the Ethernet format for the ACL. Command mode: Global configuration
<code>[no] access-control list <1-384> packet-format tagged</code>	Defines the tagging format for the ACL. Command mode: Global configuration
<code>[no] access-control list <1-384> packet-format ip {ipv4 ipv6}</code>	Defines the IP format for the ACL. Command mode: Global configuration
<code>default access-control list <1-384> packet-format</code>	Resets Packet Format parameters for the ACL to their default values. Command mode: Global configuration
<code>show access-control list <1-384> packet-format</code>	Displays the current Packet Format parameters for the ACL. Command mode: All except User EXEC

ACL Group Configuration

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

Table 4-102 ACL Group Configuration Commands

Command Syntax and Usage	
<code>access-control group <1-384> list <1-384></code>	Adds the selected ACL to the ACL Group. Command mode: Global configuration

Table 4-102 ACL Group Configuration Commands**Command Syntax and Usage**

no access-control group <1-384> **list** <1-384>

Removes the selected ACL from the ACL Group.

Command mode: Global configuration

show access-control group <1-384>

Displays the current ACL group parameters.

Command mode: All except User EXEC

ACL Metering Configuration

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

Table 4-103 ACL Metering Configuration Commands**Command Syntax and Usage**

access-control list <1-384> **meter action** {permit|deny}

Configures a filter action for packets that match the ACL definitions. You can choose to permit (pass) or deny (drop) packets.

Command mode: Global configuration

access-control list <1-384> **meter committed-rate** <1000-1000000>

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

Command mode: Global configuration

access-control list <1-384> **meter maximum-burst-size** <32-4096>

Configures the maximum burst size, in Kilobits. Enter one of the following values for mbsize: 32, 64, 128, 256, 512, 1024, 2048, 4096

Command mode: Global configuration

[no] **access-control list** <1-384> **meter enable**

Enables or disables ACL Metering.

Command mode: Global configuration

access-control list <1-384> **meter action** {drop|pass}

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

Command mode: Global configuration

show access-control list <1-384> **meter**

Displays current ACL Metering parameters.

Command mode: All

ACL Re-Mark Configuration

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

Re-Marking In-Profile Configuration

Table 4-104 Re-Mark Configuration Commands

Command Syntax and Usage
access-control list <1-384> re-mark in-profile dscp <0-63> Sets the DiffServ Code Point (DSCP) of In-Profile packets to the selected value. Command mode: Global configuration
show access-control list <1-384> re-mark Displays current Re-Mark In-Profile parameters. Command mode: All

Update User Priority Configuration

Table 4-105 User Priority Configuration Commands

Command Syntax and Usage
access-control list <1-384> re-mark in-profile dot1p <0-7> Defines 802.1p value. The value is the priority bits information in the packet structure. Command mode: Global configuration
[no] access-control list <1-384> re-mark in-profile use-tos-precedence Enable or disable mapping of TOS (Type of Service) priority to 802.1p priority for In-Profile packets. When enabled, the TOS value is used to set the 802.1p value. Command mode: Global configuration
show access-control list <1-384> re-mark Displays current Re-Mark In-Profile User Priority parameters. Command mode: All

Re-Marking Out-of-Profile Configuration

Table 4-106 Out-of-Profile Configuration Commands

Command Syntax and Usage

access-control list <1-384> **re-mark out-profile dscp** <0-63>

Sets the DiffServ Code Point (DSCP) of Out-of-Profile packets to the selected value. The switch sets the DSCP value on Out-of-Profile packets.

Command mode: Global configuration

show access-control list <1-384> **re-mark**

Displays current Re-Mark Out-of-Profile parameters.

Command mode: All

Port Mirroring Configuration

Port mirroring is disabled by default. For more information about port mirroring on the GbE Switch Module, see “Appendix A: Troubleshooting” in the *Alteon OS 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 monitored 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 4-107 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 4-108 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 mirrored 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

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 242](#).

`copy running-config tftp` Saving the Active Switch Configuration

When the `copy running-config 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 TFTP server. To start the switch configuration upload, at the prompt, enter:

```
Router(config)# copy running-config {ftp|tftp} [ext7-port|mgt-  
port|data-port]
```

Select a port, or press **Enter** to use the default (management port). The switch prompts you for the server address and filename.

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 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.

`copy tftp running-config` Restoring the Active Switch Configuration

When the `copy 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|tftp} running-config [ext7-port|mgt-  
port|data-port]
```

Select a port, or press **Enter** to use the default (management port). The switch prompts you for the server address and filename.

CHAPTER 5

Operations Commands

Operations commands generally affect switch performance immediately, but do not alter permanent switch configurations. For example, you can use Operations commands to immediately disable a port (without the need to apply or save the change), with the understanding that when the switch is reset, the port returns to its normally configured operation.

These commands enable you to alter switch operational characteristics without affecting switch configuration.

Table 5-1 General Operations Commands

Command Syntax and Usage

password *<15 characters>*

Allows the user to change the password. You must enter the current password in use for validation.

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 Options

Operations-level port options are used for temporarily disabling or enabling a port, and for re-setting the port.

Table 5-2 Port Operations Commands

Command Syntax and Usage
<div>no interface port <i><port alias or number></i> shutdown Temporarily enables the port. The port will be returned to its configured operation mode when the switch is reset. Command Mode: Privileged EXEC</div>
<div>interface port <i><port alias or number></i> shutdown Temporarily disables the port. The port will be returned to its configured operation mode when the switch is reset. Command Mode: Privileged EXEC</div>
<div>show interface port <i><port alias or number></i> operation Displays the port interface operational state. Command Mode: Privileged EXEC</div>

Operations-Level Port 802.1x Options

Operations-level port 802.1x options are used to temporarily set 802.1x parameters for a port.

Table 5-3 802.1x Operations Commands

Command Syntax and Usage

interface port *<port alias or number>* **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 alias or number>* } **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 Options

Table 5-4 Virtual Router Redundancy Operations Commands

Command Syntax and Usage

router vrrp backup *<1-255>*

Forces the specified master virtual router on this switch into backup mode. This is generally used for passing master control back to a preferred switch once the preferred switch has been returned to service after a failure. When this command is executed, the current master gives up control and initiates a new election by temporarily advertising its own priority level as 0 (lowest). After the new election, the virtual router forced into backup mode by this command will resume master control in the following cases:

- This switch owns the virtual router (the IP addresses of the virtual router and its IP interface are the same)
- This switch's virtual router has a higher priority and preemption is enabled.
- There are no other virtual routers available to take master control.

Command Mode: Privileged EXEC

Operations-Level BGP Options

Table 5-5 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	

CHAPTER 6

Boot Options

To use the Boot Options commands, you must be logged in to the switch as the administrator. The Boot Options commands provide options for:

- Selecting a switch software image to be used when the switch is next reset
- Selecting a configuration block to be used when the switch is next reset
- Downloading or uploading a new software image to the switch via FTP/TFTP

In addition to the Boot commands, you can use a Web browser or SNMP to work with switch image and configuration files. To use SNMP, refer to “Working with Switch Images and Configuration Files” in the *Command Reference*.

The boot options are discussed in the following sections.

Scheduled Reboot of the Switch

This feature allows the switch administrator to schedule a reboot to occur at a particular time in future. This feature is particularly helpful if the user needs to perform switch upgrades during off-peak hours. You can set the reboot time, cancel a previously scheduled reboot, and check the time of the current reboot schedule.

Scheduled Reboot Commands

Table 6-1 Scheduled Reboot commands

Command Syntax and Usage
boot schedule <i><day></i> <i><time (hh:mm)></i> Configures the switch reset time. The following options are valid for the day value: monday tuesday wednesday thursday friday saturday sunday Command Mode: Global configuration
no boot schedule Cancels the switch reset time. Command Mode: Global configuration
show boot Displays the current switch reboot schedule. Command Mode: All except User EXEC

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 GbE Switch Module, go to:

<http://www.ibm.com/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 tftp {<image1|image2|boot-image>} [ext7-port|mgt-port|
data-port]
```

or

```
Router# copy ftp {<image1|image2|boot-image>} [ext7-port|mgt-port|
data-port]
```

Select a port, or press **Enter** to use the default (management port).

2. Enter the hostname or IP address of the FTP or TFTP server.

```
Address or name of remote host: <name or IP address>
```

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>} tftp [ext7-port|mgt-port|  
data-port]
```

or

```
Router# copy {<image1|image2|boot-image>} ftp [ext7-port|mgt-port|  
data-port]
```

Select a port, or press **Enter** to use the default (management port).

2. Enter the name or the IP address of the FTP or TFTP server:

```
Address or name of remote host: <name or IP address>
```

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 1.0.1  
that was downloaded at 0:23:39 Thu Jan 1, 2007.  
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.

Use the following procedure to set which configuration block you want the switch to load the next time it is reset:

1. **In Global Configuration mode, enter:**

```
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.

NOTE – Resetting the switch causes the date and time to revert to default values. Use the following commands and to re-enter the current date and time:

```
>>Router (config)# system date <yyyy><mm><dd>
>>Router (config)# system time <hh><mm><ss>
```

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 Alteon OS CLI

To access the Alteon OS CLI, enter the following command from the ISCLI:

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

The default command-line interface for the GbESM is the Alteon OS 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 command is enabled:

```
boot cli-mode prompt
```

Only an administrator connected through the console port 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 switch administrator forces a switch *panic*. The **debug panic** command causes the switch to dump state information to flash memory, and then causes the switch to reboot.
- 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 7-1 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 261](#).

copy flash-dump tftp

Saves the system dump information via TFTP.

Command mode: All except User EXEC

For details, see [page 262](#).

copy flash-dump ftp

Saves the system dump information via FTP.

Command mode: All except User EXEC

clear flash-dump

Clears dump information from flash memory.

Command mode: All except User EXEC

Table 7-1 General Maintenance Commands

Command Syntax and Usage	
debug panic	Dumps MP information to FLASH and reboots. Command mode: All except User EXEC For details, see page 263 .
show tech-support	Dumps all GbE Switch Module 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

System Maintenance

System maintenance commands are reserved for use by IBM Service Support. The options are used to perform system debugging.

Table 7-2 System Maintenance Commands

Command Syntax and Usage	
debug debug-flags	This command sets the flags that are used for debugging purposes by service support group. 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 7-3 FDB Manipulation 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 xx:xx:xx:xx:xx:xx format (such as 08:00:20:12:34:56) or xxxxxxxxxxxxxx format (such as 080020123456).	
Command mode: All except User EXEC	
show mac-address-table port {<port alias or number>}	
Displays all FDB entries for a particular port.	
Command mode: All except User EXEC	
show mac-address-table vlan {<1-4093>}	
Displays all FDB entries on a single VLAN.	
Command mode: All except User EXEC	
show mac-address-table	
Displays all entries in the Forwarding Database.	
Command mode: All	
no mac-address-table <MAC address> [<1-4093>]	
Removes a single FDB entry.	
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 IBM Service Support.

Table 7-4 Miscellaneous Debug Commands

Command Syntax and Usage	
debug mp-trace	<p>Displays the Management Processor trace buffer. Header information similar to the following is shown:</p> <p>MP trace buffer at 13:28:15 Fri May 25, 2001; mask: 0x2ffdf748</p> <p>The buffer information is displayed after the header.</p> <p>Command mode: All except User EXEC</p>
debug mp-snap	<p>Displays the Management Processor snap (or post-mortem) trace buffer. This buffer contains information traced at the time that a reset occurred.</p> <p>Command mode: All except User EXEC</p>
clear flash-config	<p>Deletes all flash configuration blocks.</p> <p>Command mode: All except User EXEC</p>

ARP Cache Maintenance

Table 7-5 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 alias or number>*

Shows ARP entries on a single port.

Command mode: All except User EXEC

show ip arp vlan *<1-4093>*

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 66](#).

IP Route Manipulation

Table 7-6 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|multi-cast}

Shows routes of a single type.

Command mode: All except User EXEC

For a description of IP routing types, see [Table 2-24 on page 65](#)

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 2-25 on page 66](#)

show ip route interface <1-250>

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 63](#).

IGMP Group Information

Table 7-7 describes the IGMP Snooping maintenance commands.

Table 7-7 IGMP Multicast Group Maintenance Commands

Command Syntax and Usage
<div><code>show ip igmp groups address <IP address></code> Displays a single IGMP multicast group by its IP address. Command mode: All except User EXEC</div>
<div><code>show ip igmp groups vlan <1-4093></code> Displays all IGMP multicast groups on a single VLAN. Command mode: All except User EXEC</div>
<div><code>show ip igmp groups interface <port alias or number></code> Displays all IGMP multicast groups on a single port. Command mode: All except User EXEC</div>
<div><code>show ip igmp groups trunk <trunk number></code> Displays all IGMP multicast groups on a single trunk group. Command mode: All except User EXEC</div>
<div><code>show ip igmp groups</code> Displays information for all multicast groups. Command mode: All except User EXEC</div>
<div><code>clear ip igmp snoop</code> Clears the IGMP group table. Command mode: All except User EXEC</div>

Uencode Flash Dump

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

If you want to capture dump information to a file, set your communication software on your workstation to capture session data prior to issuing the `show flash-dump 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 uuencode** command, dump information can be read multiple times. The command does not cause the information to be updated or cleared from flash memory.

NOTE – Dump information is not cleared automatically. In order for any subsequent dump information to be written to flash memory, you must manually clear the dump region. For more information on clearing the dump region, see [page 263](#).

To access dump information, enter:

```
Router# show flash-dump-uuencode
```

The dump information is displayed on your screen and, if you have configured your communication software to do so, captured to a file. If the dump region is empty, the following appears:

```
No FLASH dump available.
```

TFTP or FTP System Dump Put

Use these commands to put (save) the system dump to a TFTP or FTP server.

NOTE – If the TFTP/FTP server is running SunOS or the Solaris operating system, the specified **copy flash-dump tftp** (or **ftp**) file must exist *prior* to executing the **copy flash-dump tftp** command (or **copy flash-dump ftp**), and must be writable (set with proper permission, and not locked by any application). The contents of the specified file will be replaced with the current dump data.

To save dump information via TFTP, enter:

```
Router# copy flash tftp [ext7|mgt|data]
```

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 [ext7|mgt|data]
```

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.
```

Panic Command

The **debug panic** command causes the switch to immediately dump state information to flash memory and automatically reboot.

To select panic, enter:

```
>> Router# debug panic  
A FLASH dump already exists.  
Replacing existing dump and reboot [y/n]:
```

Enter **y** to confirm the command:

```
Confirm dump and reboot [y/n]: y
```

The following messages are displayed:

```
Starting system dump...done.  
  
Rebooted because of PANIC command.  
Bootimg complete 0:01:01 Thu Jan 1, 2007:  
Version 1.0.0 from FLASH image1, active config block.  
  
No POST errors (0xff).  
  
Production Mode.
```

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, 2007. 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

A

abbreviating commands (CLI)	23
access control	
user	155
ACL Port commands	161
ACL statistics	122
active configuration block	130, 252
active IP interface	227
active port	
VLAN	227
active switch configuration	
gtcfg	242
ptcfg	242
restoring	242
active switch, saving and loading configuration...	242
addr	
IP route tag	66
administrator account	25
aging	
STP bridge option	174
STP information	53, 56
autonomous system filter action	195
autonomous system filter path	
action	195
as	195
aspath	195

B

backup configuration block	252
----------------------------------	-----

BGP

configuration	207
eBGP	207
filters, aggregation configuration	211
iBGP	207
in route	209
IP address, border router	208
IP route tag	66
keep-alive time	209
peer	207
peer configuration	208
redistribution configuration	210
remote autonomous system	208
router hops	209
BLOCKING (port state)	54
boot options menu	247
bootstrap protocol	220
Border Gateway Protocol	66
configuration	207
Border Gateway Protocol (BGP)	
operations-level options	246
BPDU. <i>See</i> Bridge Protocol Data Unit.	
bridge priority	53, 59
Bridge Protocol Data Unit (BPDU)	53, 59
STP transmission frequency	173
Bridge Spanning-Tree parameters	173
broadcast	
IP route tag	66
IP route type	65

C

capture dump information to a file	261
Cisco Ether Channel	176
CIST information	58
clear	
dump information	263
command (help)	21

commands	
abbreviations.....	23
conventions used in this manual	14
shortcuts	23
tab completion.....	23
commands, NNCLI	
modes	18
configuration	
802.1x	164
CIST	169
default gateway interval, for health checks	187
default gateway IP address	187
dump command.....	241
failover.....	180
flow control	160, 162
IGMP	212
IP static route	188
port mirroring.....	240
port trunking	176
RIP	196
save changes	130
SNMP	140
switch IP address	186
TACACS+.....	135
VLAN default (PVID).....	159
VLAN IP interface.....	186
VLAN tagging	159
VRRP	220
configuration block	
active	252
backup	252
factory.....	252
selection	252
configuration menu	129
configuring routing information protocol.....	197
COS queue information	48
cost	
STP information	54, 57, 60
STP port option	175
CPU statistics	121
CPU utilization	121

D

daylight savings time	139
debugging	255
default gateway	
information	63
interval, for health checks	187

default password.....	25
delete	
FDB entry	257
direct (IP route type)	65
directed broadcasts	191
DISABLED (port state).....	54
disconnect idle timeout	25
downloading software	249
dump	
configuration command	241
maintenance	255
state information	263
duplex mode	
link status.....	27, 83
dynamic routes	260

E

EtherChannel	
as used with port trunking	176

F

factory configuration block.....	252
failover	
configuration	180
FDB statistics.....	99
fixed	
IP route tag.....	66
flag field	67
flow control	27, 83
configuring	160, 162
forwarding configuration	
IP forwarding configuration	191
forwarding database (FDB)	255
delete entry	257
Forwarding Database Information	45
Forwarding Database Menu	256
forwarding state (FWD)	46, 53, 59, 60
fwd (STP bridge option).....	173
FwdDel (forward delay), bridge port	53, 56, 59

G

GEA Port mapping	85
Greenwich	139
Greenwich Mean Time (GMT)	139
gtcfg (TFTP load command).....	242

H

health checks	
default gateway interval, retries	187
retry, number of failed health checks	187
hello	
STP information	53, 56, 59
help 21	
hot-standby failover	225
hprompt	
system option	131
HTTPS	157

I

ICMP statistics	107
idle timeout	
overview	25
IEEE 802.1s	56
IEEE 802.1w	56
IEEE standards	
802.1d	53, 172
802.1s	168
802.1w	168
802.1x	50
IGMP Relay	214
IGMP Snooping	212
IGMP statistics	116
image	
downloading	249
software, selecting	250
indirect (IP route type)	65
Information	
IGMP Information	78, 81
IGMP Multicast Router Information	261
Trunk Group Information	60
information	
802.1p	48
Information commands	27
Interface change stats	115
IP address	
ARP information	67
configuring default gateway	187
IP forwarding	
directed broadcasts	191
IP forwarding information	63
IP Information	63, 77

IP interface	
active	227
configuring address	186
configuring VLANs	186
IP interfaces	65
information	63
IP route tag	66
priority increment value (ifs) for VRRP	229
IP network filter configuration	192
IP Route Manipulation	260
IP routing	
tag parameters	66
IP Static Route commands	188
IP statistics	104

L

LACP	178
Layer 2 commands	43
Layer 3 commands	63
LDAP	138
LEARNING (port state)	53, 54, 59
Link Aggregation Control Protocol	178
link status	27
command	83
duplex mode	27, 83
port speed	27, 83
Link Status Information	83
linkt (SNMP option)	141
LISTENING (port state)	54
lmask (routing option)	63
lnet (routing option)	63
local (IP route type)	65
log	
syslog messages	132

M

MAC (media access control) address .	28, 41, 45, 67, 256
Maintenance Menu	255
Management Processor (MP)	258
display MAC address	28, 41
manual style conventions	14
martian	
IP route tag (filtered)	66
IP route type (filtered out)	65
MaxAge (STP information)	53, 56, 59
MD5 cryptographic authentication	201

MD5 key	203
media access control. <i>See</i> MAC address.	
meter	
ACL	238
Miscellaneous Debug commands	258
monitor port.....	240
mp	
packet	119
MP. <i>See</i> Management Processor.	
multicast	
IP route type	65
Multiple Spanning Tree	
configuration.....	168
mxage (STP bridge option)	173

N

nbr change statistics.....	114
NNCLI commands	
modes	18
notice	131
NTP synchronization	140
NTP time zone	139

O

online help.....	21
Operations commands	243
operations-level BGP options	246
Operations-Level Port Options	244, 245
operations-level VRRP options.....	245

ospf	
area index	200
authentication key	203
cost of the selected path	202
cost value of the host	205
dead, declaring a silent router to be down.....	203
dead, health parameter of a hello packet.....	204
export.....	206
fixed routes	207
hello	204
host entry configuration	205
host routes.....	199
interface.....	199
interface configuration.....	202
link state database	199
Not-So-Stubby Area.....	200
priority value of the switch interface.....	202
range number	199
route redistribution configuration	206
spf, shortest path first.....	201
stub area	200
summary range configuration	201
transit area	200
transit delay.....	203
type.....	200
virtual link	199
virtual link configuration.....	204
virtual neighbor, router ID.....	204
OSPF Database Information	73
OSPF General Information	72
OSPF Information	71
OSPF Information Route Codes	75

P

panic	
command	263
switch (and Maintenance Menu option)	255
parameters	
tag.....	66
type.....	65
Password	
user access control	155
password	
administrator account	25
default	25
user account	24
passwords	24
ping.....	21

poisoned reverse, as used with split horizon	197
Port configuration.....	159
port configuration	159
Port Menu	
configuration options	159
port mirroring	
configuration.....	240
Port number	83
port speed	27, 83
port states	
UNK (unknown).....	46
port trunking	
description	176
port trunking configuration.....	176
ports	
disabling (temporarily)	161
information	84
IP status	63
membership of the VLAN.....	44, 61
priority	53, 59
VLAN ID	27, 84
preemption	
assuming VRRP master routing authority.....	224
prisrv	
primary radius server.....	134, 138
Protocol-based VLAN	183
ptcfg (TFTP save command)	242
PVID (port VLAN ID).....	27, 84

R

read community string (SNMP option)	141
reboot.....	255, 263
receive flow control	160, 162
reference ports	46
re-mark.....	239
retries	
radius server.....	134
retry	
health checks for default gateway.....	187
rip	
IP route tag	66
RIP Information	77
RIP information	76
RIP. <i>See</i> Routing Information Protocol.	
route statistics	106
router hops.....	209
routing information protocol	
configuration.....	197
Routing Information Protocol (RIP).....	66
options.....	197
poisoned reverse	197
split horizon	197
version 1 parameters.....	196, 197
RSTP information.....	55
Rx/Tx statistics.....	113

S

save (global command)	130
secret	
radius server	134
Secure Shell	133
shortcuts (CLI)	23
snap traces	
buffer	258
SNMP options	141
SNMP statistics	123
SNMPv3.....	143
software	
image	249
image file and version.....	28, 41
spanning tree	
configuration	172
Spanning-Tree Protocol.....	60
bridge aging option.....	174
bridge parameters.....	173
bridge priority.....	53, 59
port cost option	175
root bridge.....	53, 59, 173
switch reset effect.....	253
split horizon	197
state (STP information)	54, 57, 60
static	
IP route tag.....	66
static route	
rem.....	188
statics route	
add	188
statistics	
management processor.....	119
Statistics Menu	87
subnets	
IP interface.....	186
switch	
name and location	28, 41
resetting	253

system	
contact (SNMP option).....	141
date and time.....	28, 41
information.....	41
location (SNMP option).....	141
System Information	28
system options	
hprompt.....	131
tport	153
wport	153

T

tab completion (CLI)	23
TCP statistics	109, 120
Telnet	
configuring switches using.....	241
telnet	
radius server.....	135, 138
text conventions	14
TFTP	249
PUT and GET commands	242
TFTP server.....	242
timeout	
radius server.....	134
timeouts	
idle connection	25
timers kickoff	115
tport	
system option	153
trace buffer	258
traceroute	21
transmit flow control	160, 162
Trunk Group Information.....	60
trunk hash algorithm.....	177
type of area	
ospf	200
type parameters.....	65
typographic conventions, manual	14
tzone	139

U

UCB statistics	121
UDP statistics	111
unknown (UNK) port state	46
Unscheduled System Dump.....	264
upgrade, switch software.....	249
user access control configuration	155

user account.....	24
Uuencode Flash Dump	261

V

virtual router	
description	222
tracking criteria.....	224
virtual router group configuration.....	225
virtual router group priority tracking	227
Virtual Router Redundancy Protocol (VRRP)	
authentication parameters for IP interfaces	228
operations-level options	245
priority tracking options.....	208, 211, 224
Virtual Router Redundancy Protocol configuration.....	220
virtual routers	
increasing priority level of.....	224
priority increment values (vrs) for VRRP	229
VLAN	
active port	227
configuration	182
VLAN tagging	
port configuration	159
port restrictions	183
VLANs	
ARP entry information	67
information	61
name	44, 61
port membership	44, 61
setting default number (PVID).....	159
tagging	27, 84, 183
VLAN Number.....	61
VRRP	
interface configuration.....	228
master advertisements.....	223
tracking configuration.....	229
VRRP Information.....	81
VRRP master advertisements	
time interval	225
VRRP statistics	117

W

watchdog timer.....	255
weights	
setting virtual router priority values	229
wport.....	153