Alteon OS™

NNCLI Reference

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

Part Number: 41Y8579, June 2006

Solutions by

NORTEL

BLADE
NETWORK
TECHNOLOGIES

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

Contents

Preface

The Alteon OS *NNCLI Reference* describes how to configure and use the software with your GbE Switch Module. This guide lists each command, together with the complete syntax and a functional description, from the Nortel Networks Command Line Interface (NNCLI).

For documentation on installing the switches physically, see the *Installation Guide* for your GbE Switch Module.

Who Should Use This Book

This *NNCLI 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 "NNCLI 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 `ping <ip-address>` 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 mlt {<1-11>|hash|information}`** you must enter: **`show mlt <1-11>`** or **`show mlt hash`** or **`show mlt 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 [<interface-instance>]`** you can enter **`show ip ospf interface`** or **`show ip ospf interface <1-128>`**
italic text	Indicates variables in command syntax descriptions. Also indicates new terms and book titles. Where a variable is two or more words, the words are connected by an underscore. Example: If the command syntax is **`show spanning-tree stp <stg-identifier>`** *`stg-identifier`* represents a number between 1-32.

Table 1 Typographic Conventions

Typeface or Symbol	Meaning
`plain Courier text`	Indicates command syntax and system output, for example, prompts and system messages. Example: `configure terminal`
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 Example: If the command syntax is **`show mlt {<`*`1-11`*`>|hash|information}`** you must enter: **`show mlt <`*`1-11`*`>`** or **`show mlt hash`** or **`show mlt information`**

How to Get Help

If you need help, service, or technical assistance, see the “Getting help and technical assistance” appendix in the Nortel Networks’ 10Gb Uplink Ethernet Switch Module for IBM BladeCenter *Installation Guide*.

CHAPTER 1

NNCLI 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 NNCLI commands available for the GbESM.

The NNCLI provides a direct method for collecting switch information and performing switch configuration. Using a basic terminal, the NNCLI allows you to view information and statistics about the switch, and to perform any necessary configuration.

This chapter explains how to access the Nortel Networks Command Line Interface (NNCLI) for the switch.

Accessing the NNCLI

The first time you start the GbESM, it boots into Alteon OS CLI. To access the NNCLI, enter the following command and reset the GbESM:

```
Main# boot/mode nncli
```

To access the Alteon OS CLI, enter the following command from the NNCLI 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.

If you downgrade the switch software to version 1.1 or an earlier release, it will boot into Alteon OS CLI. However, the switch retains the CLI boot mode, and will restore your CLI choice.

NNCLI command modes

The NNCLI 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. That is, all lower-privilege mode commands are accessible when using a higher-privilege mode.

Table 1-1 lists the NNCLI command modes.

Table 1-1 NNCLI 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 NNCLI: **`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 <`***`if-number`***`>`** 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-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 <`***`1-4095`***`>`** 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 NNCLI 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 NNCLI 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
`?`	Provides more information about a specific command or lists commands available at the current level.
`exit`	Go up one level in the command mode structure.
`copy running-config startup-config`	Write configuration changes to non-volatile flash memory.
`exit` or **`quit`**	Exit from the command line interface and log out.
`ping`	Use this command to verify station-to-station connectivity across the network. The format is as follows: **`ping`** <*host name*> | <*IP address*> [*tries (1-32)*> [*msec delay*]] Where *IP address* is the hostname or IP address of the device, *tries* (optional) is the number of attempts (1-32), *msec delay* (optional) is the number of milliseconds between attempts. The DNS parameters must be configured if specifying hostnames.
`traceroute`	Use this command to identify the route used for station-to-station connectivity across the network. The format is as follows: **`traceroute`** <*host name*>| <*IP address*> [<*max-hops (1-32)*> [*msec delay*]] Where *IP address* is the hostname or IP address of the target station, *max-hops* (optional) is the maximum distance to trace (1-16 devices), and *delay* (optional) is the number of milliseconds for wait for the response. The DNS parameters must be configured if specifying hostnames.
`telnet`	This command is used to telnet out of the switch. The format is as follows: **`telnet`** <*hostname*> | <*IP address*> [port] Where *IP address* is the hostname or IP address of the device.
`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 hitting <Tab>, the NNCLI will display all available commands or options that begin with that letter. Entering additional letters will further refine the list of commands or options displayed. If only one command fits the input text when <Tab> is pressed, that command will be 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 five minutes of inactivity. This function is controlled by the idle timeout parameter, which can be set from 1 to 60 minutes.

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 (10, 100, 1000, or 10000) ■ Duplex mode (half, full, or auto) ■ Flow control for transmit and receive (no, yes, or auto) ■ Link status (up or down) **Command mode:** Any For details, see page 78.
`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:** Any For details, see page 79.
`show geaport` Displays the GbESM port mapping between the two Gigabit Ethernet Aggregators (GEA). **Command mode:** Any For details, see page 80.

Table 2-1 Information Commands

Command Syntax and Usage

`show sfp`

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

Command mode: Any

For details, see page 81.

`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: Any

System Information

The information provided by each command option is briefly described in Table 2-2 on page 26, 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 IP interface #1
- Hardware version and part number
- Software image file and version number
- Configuration name
- Log-in banner, if one is configured

Command mode: Any

For details, see page 37.

`show logging messages`

Displays most recent syslog messages.

Command mode: Any

For details, see page 38.

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 user information` Displays User Security Model (USM) table information. **Command mode:** Any To view the table, see page 28.
`show snmp-server view information` Displays information about view, subtrees, mask and type of view. **Command mode:** Any To view a sample, see page 29.
`show snmp-server access information` Displays View-based Access Control information. **Command mode:** Any To view a sample, see page 30.
`show snmp-server group information` Displays information about the group that includes, the security model, user name, and group name. **Command mode:** Any To view a sample, see page 31.

Table 2-3 SNMPv3 commands

Command Syntax and Usage
`show snmp-server community information` Displays information about the community table information. **Command mode:** Any To view a sample, see page 32.
`show snmp-server target-address information` Displays the Target Address table information. **Command mode:** Any To view a sample, see page 33.
`show snmp-server target-parameters information` Displays the Target parameters table information. **Command mode:** Any To view a sample, see page 34.
`show snmp-server notify information` Displays the Notify table information. **Command mode:** Any To view a sample, see page 34.
`show snmp-server information` Displays all the SNMPv3 information. **Command mode:** Any To view a sample, see page 36.

SNMPv3 USM User Table Information

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

```
show snmp-server user information
```

Command mode: Any

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 view information

Command mode: Any

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

Table 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 access information`

Command mode: Any

```
Group Name Prefix Model   Level       Match  ReadV   WriteV   NotifyV
---------- ------ ------- ------      ------  ------  ------   -----
v1v2grp          snmpv1  noAuthNoPriv exact  iso      iso    v1v2only
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 group information`

Command mode: Any

```
Sec Model    User Name                        Group Name
----------   -------------------------------  --------------------
snmpv1       v1v2only                         v1v2grp
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 community information`

Command mode: Any

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

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 target-address information`

Command mode: Any

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 target-parameters information`

Command mode: Any

```
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 `snmpTargeParamsEntry`.
`MP Model`	Displays the Message Processing Model used when generating SNMP messages using this entry.
`User Name`	Displays the `securityName`, which identifies the entry on whose behalf SNMP messages will be generated using this entry.
`Sec Model`	Displays the security model used when generating SNMP messages using this entry. The system may choose to return an `inconsistentValue` error if an attempt is made to set this variable to a value for a security model which the system does not support.
`Sec Level`	Displays the level of security used when generating SNMP messages using this entry.

SNMPv3 Notify Table Information

The following command displays the SNMPv3 Notify Table:

`show snmp-server notify information`

Command mode: Any

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

Table 2-11 SNMPv3 Notify Table Information

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

SNMPv3 Dump Information

The following command displays SNMPv3 information:

`show snmp-server information`

Command mode: Any

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

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

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

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

snmpCommunity Table:
Index      Name       User Name            Tag
---------- ---------- -------------------- ----------
snmpNotify Table:
Name                 Tag
-------------------- --------------------
snmpTargetAddr Table:
Name       Transport Addr  Port Taglist    Params
---------- --------------- ---- ---------- ---------------
snmpTargetParams Table:
Name                 MP Model User Name          Sec Model Sec Level
-------------------- -------- ------------------  --------- -------
```

General System Information

The following command displays system information:

`show sys-info`

Command mode: Any

```
System Information at  0:16:42 Thu May  1, 2006

Nortel Networks 10Gb Uplink Ethernet Switch Module

Switch is up 5 days, 2 hours, 16 minutes and 42 seconds.
Last boot:  0:00:47 Thu May  1, 2006 (power cycle)

MAC address: 00:11:58:ad:a3:00    Management IP Address (if 128): 
10.90.90.97
Software Version 1.0.1 (FLASH image1), factory default configura-
tion.

PCBA Part Number:      317857-A
FAB Number:            EL4512011
Serial Number:         YJ1WDW47N277
Manufacturing Date:
Hardware Revision:     0
Board Revision:        0
PLD Firmware Version:  1.0

Temperature Sensor 1 (Warning): 30.0 C (Warn at 75.0 C/Recover at 
70.0 C)
Temperature Sensor 2 (Shutdown):  30.5 C (Warn at 90.0 C/Recover at 
80.0 C)
```

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: Any

```
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 debut-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 - onlin 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

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

Displays 802.1p Information.

Command mode: Any

For details, see page 45.

```
show dot1x information
```

Displays 802.1x Information.

Command mode: Any

For details, see page 47.

```
show spanning-tree
```

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

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

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

- Port alias and priority
- Cost
- State

Command mode: Any

```
show spanning-tree stp <stg-identifier> information
```

Displays information about a specific Spanning Tree Group.

For details, see page 49.

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: Any

For details, see page 55.

`show mlt information`

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

Command mode: Any

For details, see page 57.

`show vlan information`

Displays VLAN configuration information for all configured VLANs, including:

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

Command mode: Any

For details, see page 58.

`show failover`

Displays Layer 2 Failover information.

Command mode: Any

For details, see page 59.

`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: Any

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` *`<mac-address>`* Displays a single database entry by its MAC address. You are prompted to enter the MAC address of the device. Enter the MAC address using the format, `xx:xx:xx:xx:xx:xx`. For example, `08:00:20:12:34:56`. You can also enter the MAC address using the format, `xxxxxxxxxxxx`. For example, `080020123456`. **Command mode:** Any
`show mac-address-table port` *`<port-identifier>`* Displays all FDB entries for a particular port. **Command mode:** Any
`show mac-address-table vlan` *`<vlan-identifier>`* Displays all FDB entries on a single VLAN. **Command mode:** Any
`show mac-address-table` Displays all entries in the Forwarding Database. **Command mode:** Any For more information, see page 43.
`show mac-address-table state {flood|forward|ifmac|ignore|trunk|unknown}` Displays all FDB entries for a particular state. **Command mode:** Any

Show All FDB Information

The following command displays Forwarding Database information:

`show mac-address-table`

Command mode: Any

```
   MAC address     VLAN  Port Trunk State
----------------- ----  ---- ----- -----
00:02:01:00:00:00  300  EXT1        FWD
00:02:01:00:00:01  300  INT1        FWD
00:02:01:00:00:02  300  INT1        FWD
00:02:01:00:00:03  300  INT7        FWD
00:02:01:00:00:04  300  INT3        FWD
00:02:01:00:00:05  300  INT4        FWD
00:02:01:00:00:06  300  INT6        FWD
00:02:01:00:00:07  300  INT2        FWD
00:02:01:00:00:08  300  INT5        FWD
00:02:01:00:00:09  300  INT4        FWD
00:02:01:00:00:0a  300  INT3        FWD
00:02:01:00:00:0b  300  INT2        FWD
00:02:01:00:00:0c  4095 MGT         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 244.

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 interface port <port-identifier> lacp aggregator` Displays detailed information about the LACP aggregator used by the selected port. **Command mode:** Any
`show lacp` Displays the configured global LACP settings. **Command mode:** Any
`show lacp information` Displays a summary of LACP information. **Command mode:** Any For details, see page 44.

Link Aggregation Control Protocol

The following command displays LACP information:

`show lacp information`

Command mode: Any

```
port  lacp   adminkey  operkey  selected  prio  attached  trunk
                                                   aggr
---------------------------------------------------------------
EXT1  active     30        30         y     128       17     19
EXT2  active     30        30         y     128       17     19
EXT3  off        19        19         n     128       --     --
EXT4  off        20        20         n     128       --     --
```

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: Any

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

Current port priority information:
Port   Priority  COSq  Weight
-----  --------  ----  ------
INT1        0       0      1
INT2        0       0      1
...

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.

802.1x Information

The following command displays 802.1x information:

`show dot1x information`

Command mode: Any

```
System capability : Authenticator
System status     : disabled
Protocol version  : 1
                                   Authenticator    Backend
Port    Auth Mode    Auth Status     PAE State     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
 MGT   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
------------------------------------------------------------------
* - 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 2-17 802.1x Parameter Descriptions

Parameter	Description
Port	Displays each port's alias.
`Auth Mode`	Displays the Access Control authorization mode for the port. The Authorization mode can be one of the following: ■ 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: ■ 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: ■ request ■ response ■ success ■ fail ■ timeout ■ idle

Spanning Tree Information

The following command displays Spanning Tree information:

`show spanning-tree stp` *`<stg-identifier>`* **`information`**

Command mode: Any

```
Spanning Tree Group 1: On (STP/PVST+)
VLANs:  1 2

Current Root:            Path-Cost  Port Hello MaxAge FwdDel Aging
 8000 00:16:60:f9:3e:00        0  (null)    2     20     15    300

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

Port  Priority   Cost   FastFwd     State      Designated Bridge     Des Port
----  --------   ----   --------   -------     --------------------- --------
INT1         0      0       n     DISABLED   *
INT2         0      0       n     DISABLED   *
INT3         0      0       n     DISABLED   *
INT4         0      0       n     DISABLED   *
INT5         0      0       n     DISABLED   *
INT6         0      0       n     DISABLED   *
INT7         0      0       n     DISABLED   *
INT8         0      0       n     DISABLED   *
INT9         0      0       n     DISABLED   *
INT10        0      0       n     DISABLED   *
INT11        0      0       n     DISABLED   *
INT12        0      0       n     DISABLED   *
INT13        0      0       n    FORWARDING  *
INT14        0      0       n    FORWARDING  *
EXT1       128      2       n     DISABLED
EXT2       128      2       n     DISABLED
EXT3       128      2       n     DISABLED
EXT4       128      0!      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 2-18 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 2-18 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 *<stg-identifier>* **information**

Command mode: Any

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

Current Root:            Path-Cost   Port Hello MaxAge FwdDel Aging
 8000 00:11:58:ae:39:00        0     EXT4     2    20      15   300

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

Port  Prio  Cost     State  Role Designated Bridge      Des Port   Type
----- ---- --------- -----  ---- ---------------------- --------  -----
INT1     0         0  DSB *
INT2     0         0  DSB *
INT3     0         0  FWD *
INT4     0         0  DSB *
INT5     0         0  DSB *
INT6     0         0  DSB *
INT7     0         0  DSB *
INT8     0         0  DSB *
INT9     0         0  DSB *
INT10    0         0  DSB *
INT11    0         0  DSB *
INT12    0         0  DSB *
INT13    0         0  DSB *
INT14    0         0  DSB *
EXT1   128      2000  FWD   DESG 8000-00:11:58:ae:39:00    8011     P2P
EXT2   128      2000  DISC  BKUP 8000-00:11:58:ae:39:00    8011     P2P
EXT3   128      2000  FWD   DESG 8000-00:11:58:ae:39:00    8013     P2P
EXT4   128     20000  DISC  BKUP 8000-00:11:58:ae:39:00    8013   Shared
* = STP turned off for this port.
```

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

You can configure the switch software to use the IEEE 802.1w Rapid Spanning Tree Protocol (RSTP) 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 2-19 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 2-19 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: Any

```
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 *
MGT      0         0  FWD *
EXT1   128     20000 FWD    DESG 8000-00:11:58:ae:39:00    8011   2    P2P
EXT2   128     20000 DISC   BKUP 8000-00:11:58:ae:39:00    8011   2    P2P
EXT3   128     20000 FWD    DESG 8000-00:11:58:ae:39:00    8013   2    P2P
EXT4   128     20000 DISC   BKUP 8000-00:11:58:ae:39:00    8013   2   Shared
* = STP turned off for this port.
```

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

In addition to seeing if Common Internal Spanning Tree (CIST) is enabled or disabled, you can view 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 2-20 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 2-20 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 mlt information`

Command mode: Any

```
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: Any

```
VLAN            Name            Status            Ports
----  ------------------------  ------  -------------------------
1     Default VLAN              ena      INT1-INT14 EXT1-EXT4
4095  Mgmt VLAN                 ena      INT1-MGT

PVLAN  Protocol  FrameType  EtherType  Priority  Status       Ports
-----  --------  --------------------  --------  ------  -----------
none   none      none       none       none      none    none

PVLAN      PVLAN-Tagged Ports
-----   ---------------------------
none   none
```

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

Failover Information

The following command displays Layer 2 Failover information.

`show failover`

Command mode: Any

```
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 2-21 Layer 3 Information Commands

Command Syntax and Usage

`show ip information`

Displays IP Information. For details, see page 60.

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 76.

`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 2-22 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 2-22 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 2-23 on page 62.
show ip route tag {fixed|static|addr|rip|ospf|bgp|broadcast|multicast|martian} Displays routes of a single tag. **Command mode:** All except User EXEC For a description of IP routing types, see Table 2-24 on page 63.
show ip route interface *<interface-instance>* 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 62.

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 2-23 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 2-24 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.

ARP Information

The ARP information includes IP address and MAC address of each entry, address status flags (see Table 2-26 on page 64), VLAN and port for the address, and port referencing information.

Table 2-25 ARP Information Commands

Command Syntax and Usage
`show ip arp find` `<`*`ip-address`*`>` Displays a single ARP entry by IP address. **Command mode:** All except User EXEC
`show ip arp interface` `<`*`port-instance`*`>` Displays the ARP entries on a single port. **Command mode:** All except User EXEC
`show ip arp vlan` `<`*`vlan-instance`*`>` Displays the ARP entries on a single VLAN. **Command mode:** All except User EXEC

Table 2-25 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 64.
`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 2-26 ARP Dump Flag Parameters

Flag	Description
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 2-27 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 66 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 67 for a sample output.
`show ip bgp information` Displays the BGP routing table. **Command mode:** All except User EXEC See page 67 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 rrmap; or, a loop detected.
```

OSPF Information

Table 2-28 OSPF Information Commands

Command Syntax and Usage
`show ip ospf general-information` Displays general OSPF information. **Command mode:** All except User EXEC See page 69 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 ip ospf interface [`*`<interface-instance>`***`]`** 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 70 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` *`<area-id>`* Displays the list of summary ranges belonging to non-NSSA areas. **Command mode:** All except User EXEC
`show ip ospf summary-range-nssa` *`<area-id>`* 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 72 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 [*<interface-instance>***]**

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 2-29 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 2-29 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` Displays the AS-external (type 5) LSAs with detailed information of each field of the LSAs. The usage of this command is the same as the usage of the command `asbrsum`. **Command mode:** All except User EXEC
`show ip ospf database network` Displays the network (type 2) LSAs with detailed information of each field of the LSA.network LS database. The usage of this command is the same as the usage of the command `asbrsum`. **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. The usage of this command is the same as the usage of the command `asbrsum`. **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. The usage of this command is the same as the usage of the command `asbrsum`. **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. The usage of this command is the same as the usage of the command `asbrsum`. **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 2-30 Routing Information Protocol Commands

Command Syntax and Usage
`show ip rip route` Displays RIP routes. **Command mode:** All except User EXEC For more information, see page 73.
`show interface ip rip` Displays RIP user's configuration. **Command mode:** Any For more information, see page 74.

RIP Routes Information

The following command displays RIP route information:

`show ip rip route`

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 learnt through RIP, including the routes that are undergoing 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 rip`

Command mode: Any

```
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: Any

```
Interface information:
  1: 172.200.30.3    255.255.0.0     172.200.255.255, vlan 1, up
128: 10.90.90.97     255.255.255.0   10.90.90.255,    vlan 4095, up

Default gateway information: metric strict
  1: 172.200.1.1,     vlan any,  up

Current BOOTP relay settings: OFF
  0.0.0.0, 0.0.0.0

Current IP forwarding settings: ON, dirbr disabled

Current network filter settings:
  none

Current route map settings:
```

IGMP Multicast Group Information

Table 2-31 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 <*filter number*> 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
show ip igmp groups vlan <*vlan-instance*> Displays all IGMP multicast groups on a single VLAN. **Command mode:** All except User EXEC
show ip igmp groups interface <*port-instance*> Displays all IGMP multicast groups on a single port. **Command mode:** All except User EXEC
show ip igmp groups trunk <*trunk-id*> Displays all IGMP multicast groups on a single trunk group. **Command mode:** All except User EXEC
show ip igmp groups Displays information for all multicast groups. **Command mode:** All except User EXEC

IGMP Multicast Router Port Information

The following command displays switch information:

`show ip igmp mrouter information`

Command mode: All except User EXEC

Table 2-32 IGMP Multicast Router Port Information Command Options

Command Syntax and Usage
`show ip igmp mrouter vlan` *`<1-4094>`* Displays the multicast router ports configured or learned on the selected VLAN. **Command mode:** All except User EXEC

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, renter, prio 100, master, server
  2: vrid 1, 205.178.18.202, if  1, renter, prio 100, backup
  3: vrid 3, 205.178.18.204, if  1, renter, prio 100, master, 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.
  - `renter` identifies virtual routers which are not owned by this device.
- Priority value. During the election process, the virtual router with the highest priority becomes master.
- Activity status
  - `master` identifies the elected master virtual router.
  - `backup` identifies that the virtual router is in backup mode.
  - `init` identifies that the virtual router is waiting for a startup event. 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      1000     full     yes    yes       up
 INT2    2      1000     full     yes    yes       up
 INT3    3      1000     full     yes    yes       up
 INT4    4      1000     full     yes    yes       up
 INT5    5      1000     full     yes    yes      down
 INT6    6      1000     full     yes    yes       up
 INT7    7      1000     full     yes    yes       up
 INT8    8      1000     full     yes    yes       up
 INT9    9      1000     full     yes    yes       up
 INT10  10      1000     full     yes    yes       up
 INT11  11      1000     full     yes    yes       up
 INT12  12      1000     full     yes    yes       up
 INT13  13      1000     full     yes    yes       up
 INT14  14      1000     full     yes    yes       up
 MGT    15       100     full     yes    yes       up
 EXT1   17      10000     any     yes    yes       up
 EXT2   18      10000     any     yes    yes       up
 EXT3   19      10000     any     yes    yes       up
 EXT4   20       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 (10, 100, 1000, 10000)
- Duplex mode (half, full, any, or auto)
- Flow control for transmit and receive (no, yes, or auto)
- 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 4095
INT2     2    y    n       1  INT2                1 4095
INT3     3    y    n       1  INT3                1 4095
INT4     4    y    n       1  INT4                1 4095
INT5     5    y    n       1  INT5                1 4095
INT6     6    y    n       1  INT6                1 4095
INT7     7    y    n       1  INT7                1 4095
INT8     8    y    n       1  INT8                1 4095
INT9     9    y    n       1  INT9                1 4095
INT10   10    y    n       1  INT10               1 4095
INT11   11    y    n       1  INT11               1 4095
INT12   12    y    n       1  INT12               1 4095
INT13   13    y    n       1  INT13               1 4095
INT14   14    y    n       1  INT14               1 4095
MGT     15    y    n    4095* MGT                 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
```

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 Fast Port Fowarding

Logical Port to GEA Port Mapping

The following command displays information about GEA ports:

`show geaport`

Command mode: Any

```
Alias  Logical Port  GEA Port(0-based)  GEA Unit
-----  ------------  -----------------  ---------
INT1        1               15              0
INT2        2               19              0
INT3        3               18              0
INT4        4               17              0
INT5        5               13              0
INT6        6               11              0
INT7        7               10              0
INT8        8                8              0
INT9        9                2              0
INT10      10                1              0
INT11      11                5              0
INT12      12                4              0
INT13      13               20              0
INT14      14                6              0
MGT        15               22              0
EXT1       17               25              0
EXT2       18               26              0
EXT3       19               27              0
EXT4       20                0              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 SFP information:

`show sfp`

Command mode: Any

```
Port Device TX-Enable RX-Signal TX-Fault
---- ------ --------- --------- --------
EXT3 SR-XFP  enabled     LOST      N/A
EXT4 CU-SFP  enabled     N/A      none
```

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

Information Dump

The following command dumps switch information:

`show information-dump`

Command mode: Any

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 snmp-server counters` **Command mode:** Any Displays SNMP statistics. See page 113 for sample output.
`show ntp counters` Displays Network Time Protocol (NTP) Statistics. **Command mode:** Any See page 116 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:** Any For details, see page 117.

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-identifier>`* **`dot1x counters`** Displays IEEE 802.1x statistics for the port. **Command mode:** Any See page 85 for sample output.
`show interface port` *`<port-identifier>`* **`bridging-counters`** Displays bridging (“dot1”) statistics for the port. **Command mode:** Any See page 88 for sample output.
`show interface port` *`<port-identifier>`* **`ethernet-counters`** Displays Ethernet (“dot3”) statistics for the port. **Command mode:** Any See page 89 for sample output.
`show interface port` *`<port-identifier>`* **`interface-counters`** Displays interface statistics for the port. **Command mode:** Any See page 92 for sample output.
`show interface port` *`<port-identifier>`* **`ip-counters`** Displays IP statistics for the port. **Command mode:** Any See page 94 for sample output.
`show interface port` *`<port-identifier>`* **`link-counters`** Displays link statistics for the port. **Command mode:** Any See page 94 for sample output.

802.1x Authenticator Statistics

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

show interface port *<port-identifier>* **dot1x counters**

Command mode: Any

```
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
`eapolLogoffFramesRx`	Total number of EAPOL Logoff frames received
`eapolRespIdFramesRx`	Total number of EAPOL Response Identity frames received
`eapolRespFramesRx`	Total number of Response frames received
`eapolReqIdFramesTx`	Total number of Request Identity frames transmitted
`eapolReqFramesTx`	Total number of Request frames transmitted
`invalidEapolFramesRx`	Total number of invalid EAPOL frames received
`eapLengthErrorFramesRx`	Total number of EAP length error frames received

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-identifier>`* **`dot1x`**

Command mode: Any

```
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.

Table 3-4 802.1x Authenticator Diagnostics of a Port

Statistics	Description
`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.
`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.

Table 3-4 802.1x Authenticator Diagnostics of a Port

Statistics	Description
`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-identifier>`* **`bridging-counters`**

Command mode: Any

```
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.

Table 3-5 Bridging Statistics of a Port

Statistics	Description
`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.
`dot1TpLearnedEntryDiscards`	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.
`dot1StpPortForwardTransitions`	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-identifier>`* **`ethernet-counters`**

Command mode: Any

```
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`	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. The count represented by an instance of this object is incremented when the `alignmentError` 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.
`dot3StatsFCSErrors`	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. The count represented by an instance of this object is incremented when the `frameCheckError` 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.
`dot3StatsSingleCollisionFrames`	A count of successfully transmitted frames on a particular interface for which transmission is inhibited by exactly one collision. A frame that is counted by an instance of this object is also counted by the corresponding instance of either the `ifOutUcastPkts`, `ifOutMulticastPkts`, or `ifOutBroadcastPkts`, and is not counted by the corresponding instance of the `dot3StatsMultipleCollisionFrame` object.
`dot3StatsMultipleCollisionFrames`	A count of successfully transmitted frames on a particular interface for which transmission is inhibited by more than one collision. A frame that is counted by an instance of this object is also counted by the corresponding instance of either the `ifOutUcastPkts`, `ifOutMulticastPkts`, or `ifOutBroadcastPkts`, and is not counted by the corresponding instance of the `dot3StatsSingleCollisionFrames` object.
`dot3StatsLateCollisions`	The number of times that a collision is detected on a particular interface later than 512 bit-times into the transmission of a packet. 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.
`dot3StatsExcessiveCollisions`	A count of frames for which transmission on a particular interface fails due to excessive collisions.

Table 3-6 Ethernet Statistics for Port

Statistics	Description
dot3StatsInternalMacTransmitErrors	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 dot3StatsLateCollisions object, the dot3StatsExcessiveCollisions object, or the dot3StatsCarrierSenseErrors 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 transmission errors on a particular interface that are not otherwise counted.
dot3StatsFrameTooLongs	A count of frames received on a particular interface that exceed the maximum permitted frame size. The count represented by an instance of this object is incremented when the frameTooLong 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.
dot3StatsInternalMacReceiveErrors	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 dot3StatsAlignmentErrors 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-identifier>`* **`interface-counters`**

Command mode: Any

```
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.
`ifInDiscards`	The number of inbound packets which were chosen to be discarded even though no errors had been detected to prevent their being delivered to a higher-layer protocol. One possible reason for discarding such a packet could be to free up buffer space.
`ifInErrors`	For packet-oriented interfaces, the number of inbound packets that contained errors preventing them from being delivered to a higher-layer protocol. For character-oriented or fixed-length interfaces, the number of inbound transmission units that contained errors preventing them from being deliverable to a higher-layer protocol.

Table 3-7 Interface Statistics for Port

Statistics	Description
`ifInUnknownProtos`	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.
`ifOutOctets`	The total number of octets transmitted out of the interface, including framing characters.
`ifOutUcastPkts`	The total number of packets that higher-level protocols requested to be transmitted, and which were not addressed to a multicast or broadcast address at this sub-layer, including those that were discarded or not sent.
`ifOutBroadcastPkts`	The total number of packets that higher-level protocols requested to be transmitted, and which were addressed to a broadcast address at this sub-layer, including those that were discarded or not sent. This object is a 64-bit version of `ifOutBroadcastPkts`.
`ifOutMulticastPkts`	The total number of packets that higher-level protocols requested to be transmitted, and which were addressed to a multicast address at this sub-layer, including those that were discarded or not sent. For a MAC layer protocol, this includes both Group and Functional addresses. This object is a 64-bit version of `ifOutMulticastPkts`.
`ifOutDiscards`	The number of outbound packets which were chosen to be discarded even though no errors had been detected to prevent their being transmitted. One possible reason for discarding such a packet could be to free up buffer space.
`ifOutErrors`	For packet-oriented interfaces, the number of outbound packets that could not be transmitted because of errors. For character-oriented or fixed-length interfaces, the number of outbound transmission units that could not be transmitted because of errors.

Interface Protocol Statistics

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

show interface port *<port-identifier>* **ip-counters**

Command mode: Any

```
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-identifier>* **link-counters**

Command mode: Any

```
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:** Any See page 95 for sample output.
`clear mac-address-table counters` Clears FDB statistics. **Command mode:** Any
`show interface port` *`<port-identifier>`* **`lacp counters`** Displays Link Aggregation Control Protocol (LACP) statistics. **Command mode:** Any See page 96 for sample output.

FDB Statistics

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

`show mac-address-table counters`

Command mode: Any

```
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-identifier*> lacp counters

Command mode: Any

```
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
```

Layer 3 Statistics

Table 3-12 Layer 3 Statistics Commands

Command Syntax and Usage
`show ip counters` Displays IP statistics. **Command mode:** All except User EXEC See page 99 for sample output.
`show ip route counters` Displays route statistics. **Command mode:** All except User EXEC See page 101 for sample output.
`show ip arp counters` Displays Address Resolution Protocol (ARP) statistics. **Command mode:** All except User EXEC See page 101 for sample output.
`show ip icmp counters` Displays ICMP statistics. **Command mode:** All except User EXEC See page 102 for sample output.
`show ip tcp counters` Displays TCP statistics. **Command mode:** All except User EXEC See page 104 for sample output.
`show ip udp counters` Displays UDP statistics. **Command mode:** All except User EXEC See page 105 for sample output.
`show ip igmp counters` Displays IGMP statistics. **Command mode:** All except User EXEC See page 106 for sample output.

Table 3-12 Layer 3 Statistics Commands

Command Syntax and Usage

`show ip vrrp counters`

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`)

Command mode: All except User EXEC

See page 107 for sample output.

`show ip rip counters`

Displays Routing Information Protocol (RIP) statistics.

Command mode: All except User EXEC

See page 108 for sample output.

`clear ip igmp [`*`<vlan-instance>`*`] counters`

Clears IGMP statistics.

Command mode: All above Priv EXEC

`clear ip counters`

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

Command mode: All above Priv 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

```
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 3-13 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.
`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.

Table 3-13 IP Statistics

Statistics	Description
`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 *no-route* 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.
`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).

Table 3-13 IP Statistics

Statistics	Description
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 3-14 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 3-15 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
icmpInDestUnreachs:         41   icmpInTimeExcds:              0
icmpInParmProbs:             0   icmpInSrcQuenchs:             0
icmpInRedirects:             0   icmpInEchos:                 18
icmpInEchoReps:         244350   icmpInTimestamps:             0
icmpInTimestampReps:         0   icmpInAddrMasks:              0
icmpInAddrMaskReps:          0   icmpOutMsgs:             253810
icmpOutErrors:               0   icmpOutDestUnreachs:         15
icmpOutTimeExcds:            0   icmpOutParmProbs:             0
icmpOutSrcQuenchs:           0   icmpOutRedirects:             0
icmpOutEchos:           253777   icmpOutEchoReps:             18
icmpOutTimestamps:           0   icmpOutTimestampReps:         0
icmpOutAddrMasks:            0   icmpOutAddrMaskReps:          0
```

Table 3-16 ICMP Statistics

Statistics	Description
`icmpInMsgs`	The total number of ICMP messages which the entity (the switch) received. Note that this counter includes all those counted by `icmpInErrors`.
`icmpInErrors`	The number of ICMP messages which the entity (the switch) received but determined as having ICMP-specific errors (bad ICMP `checksums`, bad length, and so forth).
`icmpInDestUnreachs`	The number of ICMP Destination Unreachable messages received.
`icmpInTimeExcds`	The number of ICMP Time Exceeded messages received.
`icmpInParmProbs`	The number of ICMP Parameter Problem messages received.

Table 3-16 ICMP Statistics

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

Table 3-16 ICMP Statistics

Statistics	Description
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 3-17 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.
tcpRtoMax	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 rsre(3), an object of this type has the semantics of the UBOUND quantity described in RFC 793.
tcpMaxConn	The limit on the total number of TCP connections the entity (the switch) can support. In entities where the maximum number of connections is dynamic, this object should contain the value -1.

Table 3-17 TCP Statistics

Statistics	Description
`tcpActiveOpens`	The number of times TCP connections have made a direct transition to the SYN-SENT state from the CLOSED state.
`tcpPassiveOpens`	The number of times TCP connections have made a direct transition to the SYN-RCVD state from the LISTEN state.
`tcpAttemptFails`	The number of times TCP connections have made a direct transition to the CLOSED state from either the SYN-SENT state or the SYN-RCVD state, plus the number of times TCP connections have made a direct transition to the LISTEN state from the SYN-RCVD state.
`tcpEstabResets`	The number of times TCP connections have made a direct transition to the CLOSED state from either the ESTABLISHED state or the CLOSE-WAIT state.
`tcpInSegs`	The total number of segments received, including those received in error. This count includes segments received on currently established connections.
`tcpOutSegs`	The total number of segments sent, including those on current connections but excluding those containing only retransmitted octets.
`tcpRetransSegs`	The total number of segments retransmitted - that is, the number of TCP segments transmitted containing one or more previously transmitted octets.
`tcpInErrs`	The total number of segments received in error (for example, bad TCP `checksums`).
`tcpCurBuff`	The total number of outstanding memory allocations from heap by TCP protocol stack.
`tcpCurConn`	The total number of outstanding TCP sessions that are currently opened.
`tcpOutRsts`	The number of TCP segments sent containing the RST flag.

UDP Statistics

The following command displays UDP statistics:

`show ip udp counters`

Command mode: All except User EXEC

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

Table 3-18 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.

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 1 statistics:
------------------------------------------------------------------
rxIgmpValidPkts:            0   rxIgmpInvalidPkts:            0
rxIgmpGenQueries:           0   rxIgmpGrpSpecificQueries:     0
rxIgmpLeaves:               0   rxIgmpReports:                0
txIgmpReports:              0   txIgmpGrpSpecificQueries:     0
txIgmpLeaves:               0
Current Groups:             0   Current M-cast Routers:       1
```

Table 3-19 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
`rxIgmpLeaves`	Total number of Leave requests received
`rxIgmpReports`	Total number of Membership Reports received
`txIgmpReports`	Total number of Membership reports transmitted

Table 3-19 IGMP Statistics

Statistic	Description
`txIgmpGrpSpecificQueries`	Total number of Membership Query packets transmitted to specific groups
`txIgmpLeaves`	Total number of Leave messages transmitted
`Current Groups`	Total number of active IGMP groups learned through IGMP Snooping
`Current M-Cast Routers`	Total number of static Multicast Routers configured on the switch

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 3-20 VRRP Statistics

Statistics	Description
`vrrpInAdvers`	The total number of 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 that had a bad version number.
`vrrpBadVrid`	The total number of VRRP advertisements that had a bad virtual router ID.
`vrrpBadAddress`	The total number of VRRP advertisements that had a bad address.
`vrrpBadData`	The total number of VRRP advertisements that had bad data.
`vrrpBadPassword`	The total number of VRRP advertisements that had a bad password.
`vrrpBadInterval`	The total number of VRRP advertisements 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 recevied = 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 3-21 Management Processor Statistics Commands

Command Syntax and Usage
`show mp packet` Displays packet statistics, to check for leads and load. **Command mode:** Any To view a sample output and a description of the stats, see page 109.
`show mp tcp-block` Displays all TCP control blocks that are in use. **Command mode:** Any To view a sample output and a description of the stats, see page 110.
`show mp udp-block` Displays all UDP control blocks that are in use. **Command mode:** Any To view a sample output, see page 111.
`show mp cpu` Displays CPU utilization for periods of up to 1, 4, and 64 seconds. **Command mode:** Any To view a sample output and a description of the stats, see page 111.

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 3-22 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 3-23 MP Specified TCP Statistics

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

Table 3-23 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 3-24 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 3-25 ACL Statistics Commands

Command Syntax and Usage
`show access-control list <list-number> counters` Displays the Access Control List Statistics for a specific ACL. **Command mode:** Any For details, see page 112.
`show access-control counters` Displays all ACL statistics. **Command mode:** All except User EXEC
`clear access-control list <list-number> counters` Clears ACL statistics. **Command mode:** All except User EXEC

ACL Statistics

This option displays statistics for the selected ACL.

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

Command mode: Any

```
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 3-26 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 3-26 SNMP Statistics

Statistics	Description
`snmpInASNParseErrs`	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.
`snmpEnableAuth Traps`	An object to enable or disable the authentication traps generated by this entity (the switch).
`snmpOutPkts`	The total number of SNMP Messages which were passed from the SNMP protocol entity to the transport service.
`snmpInBadTypes`	The total number of SNMP Messages which failed ASN parsing.
`snmpInTooBigs`	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 *too big.*
`snmpInNoSuchNames`	The total number of SNMP Protocol Data Units (PDUs) which were delivered to the SNMP protocol entity and for which the value of the error-status field is `noSuchName`.
`snmpInBadValues`	The total number of SNMP Protocol Data Units (PDUs) which were delivered to the SNMP protocol entity and for which the value of the error-status field is `badValue.`
`snmpInReadOnlys`	The total number of valid SNMP Protocol Data Units (PDUs), which were delivered to the SNMP protocol entity and for which the value of the error-status field is `read-Only'. It should be noted that it is a protocol error to generate an SNMP PDU, which contains the value `read-Only' in the error-status field. As such, this object is provided as a means of detecting incorrect implementations of the SNMP.
`snmpInGenErrs`	The total number of SNMP Protocol Data Units (PDUs), which were delivered to the SNMP protocol entity and for which the value of the error-status field is `genErr.`
`snmpInTotalReqVars`	The total number of MIB objects which have been retrieved successfully by the SNMP protocol entity as a result of receiving valid SNMP Get-Request and Get-Next Protocol Data Units (PDUs).

Table 3-26 SNMP Statistics

Statistics	Description
`snmpInTotalSetVars`	The total number of MIB objects, which have been altered successfully by the SNMP protocol entity as a result of receiving valid SNMP Set-Request Protocol Data Units (PDUs).
`snmpInGetRequests`	The total number of SNMP Get-Request Protocol Data Units (PDUs), which have been accepted and processed by the SNMP protocol entity.
`snmpInGetNexts`	The total number of SNMP Get-Next Protocol Data Units (PDUs), which have been accepted and processed by the SNMP protocol entity.
`snmpInSetRequests`	The total number of SNMP Set-Request Protocol Data Units (PDUs), which have been accepted and processed by the SNMP protocol entity.
`snmpInGetResponses`	The total number of SNMP Get-Response Protocol Data Units (PDUs), which have been accepted and processed by the SNMP protocol entity.
`snmpInTraps`	The total number of SNMP Trap Protocol Data Units (PDUs), which have been accepted and processed by the SNMP protocol entity.
`snmpOutTooBigs`	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 *too big*.
`snmpOutNoSuchNames`	The total number of SNMP Protocol Data Units (PDUs), which were generated by the SNMP protocol entity and for which the value of the error-status is `noSuchName`.
`snmpOutBadValues`	The total number of SNMP Protocol Data Units (PDUs), which were generated by the SNMP protocol entity and for which the value of the error-status field is `badValue.`
`snmpOutReadOnlys`	Not in use.
`snmpOutGenErrs`	The total number of SNMP Protocol Data Units (PDUs), which were generated by the SNMP protocol entity and for which the value of the error-status field is `genErr`.
`snmpOutGetRequests`	The total number of SNMP Get-Request Protocol Data Units (PDUs), which have been generated by the SNMP protocol entity.
`snmpOutGetNexts`	The total number of SNMP Get-Next Protocol Data Units (PDUs), which have been generated by the SNMP protocol entity.
`snmpOutSetRequests`	The total number of SNMP Set-Request Protocol Data Units (PDUs), which have been generated by the SNMP protocol entity.
`snmpOutGet Responses`	The total number of SNMP Get-Response Protocol Data Units (PDUs), which have been generated by the SNMP protocol entity.

Table 3-26 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: Any

```
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 3-27 NTP Statistics

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

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 except User EXEC For details, see page 228.
`copy running-config {ftp|tftp}` Backs up current configuration to FTP or TFTP server. **Command mode:** Priv EXEC For details, see page 229.
`copy {ftp|tftp} running-config` Restores current configuration from a FTP or TFTP server. **Command mode:** Priv EXEC For details, see page 229.

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 240.

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 reverts to its default value when the switch is reset. **Command mode:** config
system time *<hh>:<mm>:<ss>* Configures the system time using a 24-hour clock format. The time reverts to its default value when the switch is reset. **Command mode:** config

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:** config
`system idle` *`<idle-value>`* Sets the idle timeout for CLI sessions, from 1 to 60 minutes. The default is 5 minutes. **Command mode:** config
`system notice` *`<string>`* Displays login notice immediately before the "Enter password:" prompt. This notice can contain up to 1024 characters and new lines. **Command mode:** config
`[no] banner` *`<string>`* 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:** config
`[no] hostname` *`<string>`* Enables or disables displaying of the host name (system administrator's name) in the Command Line Interface (CLI). **Command mode:** config
`show system` Displays the current system parameters. **Command mode:** Any

System Host Log Configuration

Table 4-3 Host Log Configuration Commands

Command Syntax and Usage
`[no] logging host {`*`<host-instance>`***`} address {`***`<ip-address>`***`}`** Sets the IP address of the first or second syslog host. **Command mode:** config
`logging host {`*`<host-instance>`***`} severity {`***`<severity-level>`***`}`** 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:** config

Table 4-3 Host Log Configuration Commands

Command Syntax and Usage
`logging host {<host-instance>} facility {<facility-level>}` This option sets the facility level of the first or second syslog host displayed. The default is 0. **Command mode:** config
`logging console` Enables delivering syslog messages to the console. It is enabled by default. **Command mode:** config
`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:** config
`[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:** config
`show logging` Displays the current syslog settings. **Command mode:** Any

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 the management module interface.

Table 4-4 SSH Server Configuration Commands

Command Syntax and Usage
`ssh interval` *`<interval-value>`* Set the interval for auto-generation of the RSA server key. **Command mode:** config
`ssh scp-password` Set the administration password for SCP access. **Command mode:** config
`ssh generate-host-key` Generate the RSA host key. **Command mode:** config
`ssh generate-server-key` Generate the RSA server key. **Command mode:** config
`ssh port` *`<port-number>`* Sets the SSH server port number. **Command mode:** config
`ssh scp-enable` Enables the SCP apply and save. **Command mode:** config
`no ssh scp-enable` Disables the SCP apply and save. **Command mode:** config
`ssh enable` Enables the SSH server. **Command mode:** config
`no ssh enable` Disables the SSH server. **Command mode:** config

Table 4-4 SSH Server Configuration Commands

Command Syntax and Usage
`show ssh` Displays the current SSH server configuration. **Command mode:** Any

RADIUS Server Configuration

Table 4-5 RADIUS Configuration Commands

Command Syntax and Usage
`[no] radius-server host` *`<ip-address>`* Sets the primary or secondary RADIUS server address. **Command mode:** config
`radius-server host` *`<ip-address>`* **`key`** *`<key-value>`* This is the primary or secondary shared secret between the switch and the RADIUS server(s). **Command mode:** config
`radius-server port` *`<port-number>`* Enter the number of the UDP port to be configured, between 1500 - 3000. The default is 1645. **Command mode:** config
`radius-server retransmit` *`<retry-count>`* Sets the number of failed authentication requests before switching to a different RADIUS server. The default is 3 requests. **Command mode:** config
`radius-server timeout` *`<timeout-value>`* 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:** config
`[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:** config
`radius-server enable` Enables the RADIUS server. **Command mode:** config

Table 4-5 RADIUS Configuration Commands

Command Syntax and Usage
`no radius-server enable` Disables the RADIUS server. **Command mode:** config
`show radius-server` Displays the current RADIUS server parameters. **Command mode:** Any

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` *`<ip-address>`* Defines the primary or secondary TACACS+ server address. **Command mode:** config
`[no] tacacs-server host` *`<ip-address>`* **`key`** *`<key-value>`* This is the primary or secondary shared secret between the switch and the TACACS+ server(s). **Command mode:** config

Table 4-6 TACACS+ Server Commands

Command Syntax and Usage
`tacacs-server port` *`<port-number>`* Enter the number of the TCP port to be configured, between 1 - 65000. The default is 49. **Command mode:** config
`tacacs-server retransmit` *`<retry-count>`* Sets the number of failed authentication requests before switching to a different TACACS+ server. The default is 3 requests. **Command mode:** config
`tacacs-server timeout` *`<timeout-value>`* 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:** config
`[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:** config
`[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:** config
`[no] tacacs-server password-change` Enables or disables TACACS+ password change. The default value is `disabled`. **Command mode:** config
`tacacs-server primary-password` Configures the password for the primary TACACS+ server. The CLI will prompt you for input. **Command mode:** config
`tacacs-server secondary-password` Configures the password for the secondary TACACS+ server. The CLI will prompt you for input. **Command mode:** config

Table 4-6 TACACS+ Server Commands

Command Syntax and Usage
`[no] tacacs-server command-authorization` Enables or disables TACACS+ command authorization. **Command mode:** config
`[no] tacacs-server command-logging` Enables or disables TACACS+ command logging. **Command mode:** config
`tacacs-server enable` Enables the TACACS+ server. **Command mode:** config
`no tacacs-server enable` Disables the TACACS+ server. This is the default setting. **Command mode:** config
`show tacacs-server` Displays current TACACS+ configuration parameters. **Command mode:** Any

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 host` *`<ip-address>`* Sets the primary or secondary LDAP server address. **Command mode:** config
`ldap-server port` *`<port-number>`* Enter the number of the UDP port to be configured, between 1500 - 65000. The default is 389. **Command mode:** config
`ldap-server retransmit` *`<retry-count>`* Sets the number of failed authentication requests before switching to a different LDAP server. The default is 3 requests. **Command mode:** config

Table 4-7 LDAP Configuration commands

Command Syntax and Usage
`ldap-server timeout` *`<timeout-value>`* 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:** config

`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: config

`[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:** config
`ldap-server enable` Enables the LDAP server. **Command mode:** config
`no ldap-server enable` Disables the LDAP server. **Command mode:** config
`show ldap-server` Displays the current LDAP server parameters. **Command mode:** Any

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 server` *`<ip-address>`* Prompts for the IP addresses of the primary or secondary NTP server to which you want to synchronize the switch clock. **Command mode:** config
`ntp interval` *`<interval-value>`* Specifies the interval, that is, how often, in minutes (1-2880), to re-synchronize the switch clock with the NTP server. **Command mode:** config
`ntp timezone` *`<zone-value>`* Prompts for the NTP time zone offset, in hours and minutes, of the switch you are synchronizing from Greenwich Mean Time (GMT).
`[no] ntp daylightsavings` 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:** config
`ntp enable` Enables the NTP synchronization service. **Command mode:** config
`no ntp enable` Disables the NTP synchronization service. **Command mode:** config
`show ntp` Displays the current NTP service settings. **Command mode:** Any

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` *<string>* Configures the name for the system. The name can have a maximum of 64 characters. **Command mode:** config
`snmp-server location` *<string>* Configures the name of the system location. The location can have a maximum of 64 characters. **Command mode:** config
`snmp-server contact` *<string>* Configures the name of the system contact. The contact can have a maximum of 64 characters. **Command mode:** config

Table 4-9 System SNMP Commands

Command Syntax and Usage

`snmp-server read-community` *`<string>`*

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: config

`snmp-server write-community` *`<string>`*

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: config

`snmp-server timeout` *`<timeout-value>`*

Sets the timeout value for the SNMP state machine.

Command mode: config

`[no] snmp-server authentication-trap`

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

Command mode: config

`[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: config

`snmp-server trap-src-if` *`<1-128>`*

Configures the source interface for SNMP traps.

Command mode: config

`show snmp-server`

Displays the current SNMP configuration.

Command mode: Any

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
`snmp-server user` *`<user-instance>`* This command allows you to create a user security model (USM) entry for an authorized user. You can also configure this entry through SNMP. **Command mode:** config To view command options, see page 133.
`snmp-server view` *`<view-instance>`* This command allows you to create different MIB views. **Command mode:** config To view command options, see page 135.
`snmp-server access` *`<access-instance>`* This command allows you to specify access rights. The View-based Access Control Model defines a set of services that an application can use for checking access rights of the user. You need access control when you have to process retrieval or modification request from an SNMP entity. **Command mode:** config To view command options, see page 136.
`snmp-server group` *`<group-instance>`* A group maps the user name to the access group names and their access rights needed to access SNMP management objects. A group defines the access rights assigned to all names that belong to a particular group. **Command mode:** config To view command options, see page 137.

Table 4-10 SNMPv3 Configuration Commands

`snmp-server community` *`<community-instance>`*

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

Command mode: config

To view command options, see page 138.

`snmp-server target-address` *`<taddr-instance>`*

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: config

To view command options, see page 139.

`snmp-server target-parameters` *`<tparam-instance>`*

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: config

To view command options, see page 140.

`snmp-server notify` *`<notify-instance>`*

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: config

To view command options, see page 141.

`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: config

`show snmp-server v3`

Displays the current SNMPv3 configuration.

Command mode: Any

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 *<user-instance>* **name** *<user-name>* This command allows you to configure a string up to 32 characters that represents the name of the user. This is the login name that you need in order to access the switch. **Command mode:** config
snmp-server user *<user-instance>* **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:** config
snmp-server user *<user-instance>* **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:** config
no snmp-server user *<user-instance>* Deletes the USM user entries. **Command mode:** config
show snmp-server user *<user-instance>* Displays the USM user entries. **Command mode:** Any

SNMPv3 View Configuration

Table 4-12 SNMPv3 View Configuration Commands

Command Syntax and Usage
snmp-server view *<view-instance>* **name** *<view-name>* This command defines the name for a family of view subtrees up to a maximum of 32 characters. **Command mode:** config
snmp-server view *<view-instance>* **tree** *<tree-value>* This command defines MIB tree, a string of maximum 32 characters, which when combined with the corresponding mask defines a family of view subtrees. **Command mode:** config
snmp-server view *<view-instance>* **mask** *<mask-value>* This command defines the bit mask, which in combination with the corresponding tree defines a family of view subtrees. **Command mode:** config
snmp-server view *<view-instance>* **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:** config
no snmp-server view *<view-instance>* Deletes the `vacmViewTreeFamily` group entry. **Command mode:** config
show snmp-server view *<view-instance>* Displays the current `vacmViewTreeFamily` configuration. **Command mode:** Any

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 *<access-instance>* **name** *<name-value>* Defines the name of the group. **Command mode:** config
snmp-server access *<access-instance>* **prefix** *<prefix-value>* Defines the name of the context. An SNMP context is a collection of management information that an SNMP entity can access. An SNMP entity has access to many contexts. For more information on naming the management information, see RFC2571, the SNMP Architecture document. The view-based Access Control Model defines a table that lists the locally available contexts by contextName. **Command mode:** config
snmp-server access *<access-instance>* **security {usm|snmpv1|snmpv2}** Allows you to select the security model to be used. **Command mode:** config
snmp-server access *<access-instance>* **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:** config
snmp-server access *<access-instance>* **match {exact|prefix}** If the value is set to `exact`, then all the rows whose contextName exactly matches the prefix are selected. If the value is set to `prefix` then the all the rows where the starting octets of the contextName exactly match the prefix are selected. **Command mode:** config
snmp-server access *<access-instance>* **read-view** *<view-name>* This is a 32 character 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:** config

Table 4-13 View-based Access Control Model Commands

Command Syntax and Usage
`snmp-server access` *`<access-instance>`* **`write-view`** *`<view-name>`* This is a 32 character 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:** config
`snmp-server access` *`<access-instance>`* **`notify-view`** *`<view-name>`* This is a 32 character notify view name that allows you notify access to the MIB view. **Command mode:** config
`no snmp-server access` *`<access-instance>`* Deletes the View-based Access Control entry. **Command mode:** config
`show snmp-server access` *`<access-instance>`* Displays the View-based Access Control configuration. **Command mode:** Any

SNMPv3 Group Configuration

Table 4-14 SNMPv3 Group Configuration Commands

Command Syntax and Usage
`snmp-server group` *`<group-instance>`* **`security {usm|snmpv1|snmpv2}`** Defines the security model. **Command mode:** config
`snmp-server group` *`<group-instance>`* **`user-name`** *`<name>`* Sets the user name as defined in `snmp-server user` *`<user-instance>`* `name` *`<user-name>`* on page 133. **Command mode:** config
`snmp-server group` *`<group-instance>`* **`group-name`** *`<name>`* The name for the access group as defined in `snmp-server access` *`<access-instance>`* `name` *`<name-value>`* on page 133. **Command mode:** config

Table 4-14 SNMPv3 Group Configuration Commands

Command Syntax and Usage
`no snmp-server group` *`<group-instance>`* Deletes the `vacmSecurityToGroup` entry. **Command mode:** config
`show snmp-server group` *`<group-instance>`* Displays the current `vacmSecurityToGroup` configuration. **Command mode:** Any

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` *`<community-instance>`* **`index`** *`<string>`* Allows you to configure the unique index value of a row in this table consisting of 32 characters maximum. **Command string:** config
`snmp-server community` *`<community-instance>`* **`name`** *`<string>`* Defines the user name as defined in `snmp-server user` *`<user-instance>`* `name` *`<user-name>`* on page 133. **Command string:** config
`snmp-server community` *`<community-instance>`* **`user-name`** *`<string>`* Defines a readable 32 character long string that represents the corresponding value of an SNMP community name in a security model. **Command mode:** config
`snmp-server community` *`<community-instance>`* **`tag`** *`<string>`* Allows you to configure a tag of up to 255 characters maximum. This tag specifies a set of transport endpoints to which a command responder application sends an SNMP trap. **Command mode:** config

Table 4-15 SNMPv3 Community Table Configuration Commands

Command Syntax and Usage
no snmp-server community *<community-instance>* Deletes the community table entry. **Command mode:** config
show snmp-server community *<community-instance>* Displays the community table configuration. **Command mode:** Any

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 *<taddr-instance>* **address** *<ip-address>* **name** *<string>* Allows you to configure the locally arbitrary, but unique identifier, target address name associated with this entry. **Command mode:** config
snmp-server target-address *<taddr-instance>* **name** *<string>* **address** *<ip-address>* Allows you to configure a transport address IP that can be used in the generation of SNMP traps. **Command mode:** config
snmp-server target-address *<taddr-instance>* **port** *<port-number>* Allows you to configure a transport address port that can be used in the generation of SNMP traps. **Command mode:** config
snmp-server target-address *<taddr-instance>* **taglist** *<string>* Allows you to configure a list of tags that are used to select target addresses for a particular operation. **Command mode:** config
snmp-server target-address *<taddr-instance>* **parameters-name** *<string>* Defines the name as defined in `snmp-server target-parameters` *<tparam-instance>* `name` *<string>* on page 140. **Command mode:** config

Table 4-16 Target Address Table Configuration Commands

Command Syntax and Usage
`no snmp-server target-address` *`<taddr-instance>`* Deletes the Target Address Table entry. **Command mode:** config
`show snmp-server target-address` *`<taddr-instance>`* Displays the current Target Address Table configuration. **Command mode:** Any

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` *`<tparam-instance>`* **`name`** *`<string>`* Allows you to configure the locally arbitrary, but unique, identifier that is associated with this entry. **Command mode:** config
`snmp-server target-parameters` *`<tparam-instance>`* **`message {snmpv1|snmpv2c|snmpv3}`** Allows you to configure the message processing model that is used to generate SNMP messages. **Command mode:** config
`snmp-server target-parameters` *`<tparam-instance>`* **`security {usm|snmpv1|snmpv2}`** Allows you to select the security model to be used when generating the SNMP messages. **Command mode:** config
`snmp-server target-parameters` *`<tparam-instance>`* **`user-name`** *`<string>`* Defines the name that identifies the user in the USM table (page 133) on whose behalf the SNMP messages are generated using this entry. **Command mode:** config

Table 4-17 Target Parameters Table Configuration Commands

Command Syntax and Usage
`snmp-server target-parameters` *`<tparam-instance>`* **`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:** config
`no snmp-server target-parameters` *`<tparam-instance>`* Deletes the `targetParamsTable` entry. **Command mode:** config
`show snmp-server target-parameters` *`<tparam-instance>`* Displays the current `targetParamsTable` configuration. Command mode: Any

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` *`<notify-instance>`* **`name`** *`<string>`* Defines a locally arbitrary, but unique, identifier associated with this SNMP notify entry. **Command mode:** config
`snmp-server notify` *`<notify-instance>`* **`tag`** *`<string>`* Allows you to configure a tag of 255 characters maximum 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:** config
`no snmp-server notify` *`<notify-instance>`* Deletes the notify table entry. **Command mode:** config
`show snmp-server notify` *`<notify-instance>`* Displays the current notify table configuration. **Command mode:** Any

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: `config`

`[no] access http enable` Enables or disables HTTP (Web) access to the Browser-Based Interface. It is enabled by default. **Command mode:** config
`access http port` *`<port-number>`* Sets the switch port used for serving switch Web content. The default is HTTP port 80. Command mode: config
`[no] access snmp {read-only|read-write}` Disables or provides read-only/write-read SNMP access. **Command mode:** config
`[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:** config
`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:** config
`show access` Displays the current system access parameters. **Command mode:** Any

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` *`<ip-address> <ip-mask>`*

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.

Command mode: config

`no access management-network` *`<ip-address> <ip-mask>`*

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

Command mode: config

`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` *`<user-id>`*

Configures the User ID.

Command mode: config

`access user eject <`*`user name`***`>`**

Ejects the specified user from the GbESM.

Command mode: config

`access user user-password`

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: config

Table 4-21 User Access Control Configuration Commands

Command Syntax and Usage
`access user operator-password` 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:** config
`access user administrator-password` 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:** config
`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` *`<user-id>`* **`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:** config
`access user` *`<user-id>`* **`name`** *`<string>`* Defines the user name of maximum eight characters. **Command mode:** config
`access user` *`<user-id>`* **`password`** Sets the user password of up to 15 characters maximum. **Command mode:** config
`access user` *`<user-id>`* **`enable`** Enables the user ID. **Command mode:** config
`no access user` *`<user-id>`* **`enable`** Disables the user ID. **Command mode:** config

Table 4-22 User ID Configuration Commands

Command Syntax and Usage
`no access user` *`<user-id>`* Deletes the user ID. **Command mode:** config
`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:** config
`no access user strong-password` Disables Strong Password requirement. **Command mode:** config
`access user strong-password expiry <`*`1-365`***`>`** Configures the number of days allowed before the password must be changed. **Command mode:** config
`access user strong-password warning <`*`1-365`***`>`** Configures the number of days before password expiration, that a warning is issued to users. **Command mode:** config
`access user strong-password faillog <`*`1-265`***`>`** Configures the number of failed login attempts allowed before a security notification is logged. **Command mode:** config
`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: config

`access https port` *`<port-number>`*

Defines the HTTPS Web server port number.

Command mode: config

`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) []: Nortel Networks
- Organizational Unit Name (for example, section) []: Alteon
- Common Name (for example, user's name) []: Mr Smith
- Email (for example, email address) []: info@nortelnetworks.com

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: config

`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: config

`show access`

Displays the current SSL Web Access configuration.

Command mode: All except User EXEC

Port Configuration

These commands enable you to configure settings for individual switch ports (except MGT). This command is enabled by default.

Table 4-25 Port Configuration Commands

Command Syntax and Usage
`dot1p {0-7}` Configures the port's 802.1p priority level. **Command mode:** interface port
`pvid {`*`<vlan-instance>`***`}`** 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 {`*`<name-string>`***`}`** 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.
`[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
`[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

Table 4-25 Port Configuration Commands

Command Syntax and Usage

`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 149.)

Command mode: interface port

`show interface port {`*`<port-identifier>`*`}`

Displays current port parameters.

Command mode: Any

Port Link Configuration

You can use these commands to set port parameters such as speed, flow control, and negotiation mode for the port link.

Table 4-26 Port Link Configuration Commands

Command Syntax and Usage

`speed {10|100|1000|auto}`

Sets the link speed. Not all options are valid on all ports. The choices include:

- 10 Mbps
- 100 Mbps
- 1000 Mbps
- 10000 Mbps
- "Auto," for auto negotiation

Command mode: interface port

`duplex {full|half|any}`

Sets the operating mode. The choices include:

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

Command mode: interface port

Table 4-26 Port Link Configuration Commands

Command Syntax and Usage

`flowcontrol {receive|send|both}`
`no flowcontrol`

Sets the flow control. The choices include:

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

Command mode: interface port

`show interface port {`*`<port-identifier>`*`}`

Displays current port parameters.

Command mode: Any

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 identifier> 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 231 for other operations-level commands.

ACL Port Configuration

Table 4-27 ACL/QoS Configuration Commands

Command Syntax and Usage

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

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` *`<ACL list-number>`*

Deletes the specified ACL list from the port.

Command mode: interface port

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

Adds the specified ACL Group to the port. You can add multiple ACL Groups to a port.

Command mode: interface port

Table 4-27 ACL/QoS Configuration Commands

Command Syntax and Usage
no access-control group *<ACL group-number>* Removes the specified ACL from the port. **Command mode:** interface port
show interface port *<port-identifier>* **access-control** Displays current ACL QoS parameters. **Command mode:** Any

Layer 2 Configuration

Table 4-28 Layer 2 Configuration Commands

Command Syntax and Usage
`vlan {<vlan-identifier>}` Configures the VLAN. **Command mode:** config To view command options, see page 170.
`[no] spanning-tree fast-uplink` 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 65500 for all STGs and path cost by 3000 for all external STP ports. **Command mode:** config
`spanning-tree fast-uplink update-rate <rate-value>` Configures the station update rate. The default value is 40. **Command mode:** config
`show layer2` Displays current Layer 2 parameters. **Command mode:** Any

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 4-29 802.1x Configuration Commands

Command Syntax and Usage
`dot1x enable` Globally enables 802.1x. **Command mode:** config
`no dot1x enable` Globally disables 802.1x. **Command mode:** config
`show dot1x` Displays current 802.1x parameters. **Command mode:** Any

802.1x Global Configuration

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

Table 4-30 802.1x Global Configuration Commands

Command Syntax and Usage

`dot1x mode {[force-unauthorized|auto|force-authorized]}`

Sets the type of access control for all ports:

- **`force-unauthorized`** - the port is unauthorized unconditionally.
- **`auto`** - the port is unauthorized until it is successfully authorized by the RADIUS server.
- **`force-authorized`** - the port is authorized unconditionally, allowing all traffic.

The default value is `force-authorized`.

Command mode: config

`dot1x quiet-time {`*`<interval-value>`*`}`

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: config

`dot1x transmit-interval {`*`<interval-value>`*`}`

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: config

`dot1x supplicant-timeout {`*`<timeout-value>`*`}`

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: config

`dot1x server-timeout {`*`<timeout-value>`*`}`

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: config

`dot1x max-request {`*`<request-value>`*`}`

Sets the maximum number of times the authenticator retransmits an EAP-Request packet to the supplicant (client). The default value is 2.

Command mode: config

Table 4-30 802.1x Global Configuration Commands

Command Syntax and Usage
`dot1x re-authentication-interval {<`*`interval-value`*`>}` 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:** config
`dot1x re-authenticate` Sets the re-authentication status to `on`. The default value is `off`. **Command mode:** config
`[no] dot1x re-authenticate` Sets the re-authentication status to `off`. The default value is `off`. **Command mode:** config
`default dot1x` Resets the global 802.1x parameters to their default values. **Command mode:** config
`show dot1x` Displays current global 802.1x parameters. **Command mode:** Any

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 4-31 802.1x 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-authized`.

Command mode: interface

`dot1x quiet-time {`*`<interval-value>`*`}`

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

`dot1x transmit-interval {`*`<interval-value>`*`}`

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

`dot1x supplicant-timeout {`*`<timeout-value>`*`}`

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

`dot1x server-timeout {`*`<timeout-value>`*`}`

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: interface

`dot1x max-request {`*`<request-value>`*`}`

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

Table 4-31 802.1x Port Commands

Command Syntax and Usage
dot1x re-authentication-interval {<*interval-value*>**}** 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
dot1x re-authenticate Sets the re-authentication status to on. The default value is off. **Command mode:** interface
[no] dot1x re-authenticate Sets the re-authentication status off. The default value is off. **Command mode:** interface
default dot1x Resets the 802.1x port parameters to their default values. **Command mode:** config
dot1x apply-global Applies current global 802.1x configuration parameters to the port. **Command mode:** interface
show interface port <*port-identifier*> **dot1x** Displays current 802.1x port parameters. **Command mode:** Any

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 on the switch. MRST is turned off by default.

NOTE – When Multiple Spanning Tree is turned on, VLAN 4095 is moved from Spanning Tree Group 32 to the Common Internal Spanning Tree (CIST). When Multiple Spanning Tree is turned off, VLAN 4095 is moved back to Spanning Tree Group 32.

Table 4-32 Multiple Spanning Tree Configuration Commands

Command Syntax and Usage
`spanning-tree mstp name {`*`<name-string>`***`}`** Configures a name for the MSTP region. All devices within a MSTP region must have the same region name. **Command mode:** config
`spanning-tree mstp version {`*`<version-value>`***`}`** 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:** config
`spanning-tree mstp maximum-hop` *`<hop-value>`* 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:** config
`spanning-tree mrst mode {mst|rstp}` Selects either Rapid Spanning Tree mode (`rstp`) or Multiple Spanning Tree mode (`mstp`). The default mode is RSTP. **Command mode:** config
`spanning-tree mrst enable` Globally turns RSTP/MSTP ON. **Note**: When RSTP is turned on, the configuration parameters for STG 1 apply to RSTP. **Command mode:** config

Table 4-32 Multiple Spanning Tree Configuration Commands

Command Syntax and Usage
`no spanning-tree mrst enable` Globally turns RSTP/MSTP `off`. **Command mode:** config
`show spanning-tree mrst` Displays the current RSTP/MSTP configuration. **Command mode:** Any

Common Internal Spanning Tree Configuration

Table 4-33 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 4-33 CIST Configuration Commands

Command Syntax and Usage
`default spanning-tree mstp cist` Resets all CIST parameters to their default values. **Command mode:** config
`show spanning-tree mstp cist` Displays the current CIST configuration. **Command mode:** Any

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 4-34 CIST Bridge Configuration Commands

Command Syntax and Usage
`spanning-tree mstp cist-bridge priority {`*`<priority-value>`*`}` 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 32768. **Command mode:** config
`spanning-tree mstp cist-bridge maximum-age {`*`<age-value>`*`}` 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:** config
`spanning-tree mstp cist-bridge forward-delay {`*`<delay-value>`*`}` 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:** config
`show spanning-tree mstp cist` Displays the current CIST bridge configuration. **Command mode:** Any

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 4-35 CIST Port Configuration Commands

Command Syntax and Usage

`spanning-tree mstp cist interface-priority {`*`<priority-value>`***`}`**

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

`spanning-tree mstp cist path-cost {`*`<cost-value>`***`}`**

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

`spanning-tree mstp cist hello {`*`<time-value>`***`}`**

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

`spanning-tree mstp cist link-type {auto|p2p|shared}`

Defines the type of link connected to the port, as follows:
`auto`: Configures the port to detect the link type, and automatically match its settings.
`p2p`: Configures the port for Point-To-Point protocol.
`shared`: Configures the port to connect to a shared medium (usually a hub).

The default link type is **`auto`**.

Command mode: interface

`[no] spanning-tree mst cist edge`

Enables or disables this port as an edge port. An edge port is not connected to a bridge, and can begin forwarding traffic as soon as the link is up. Configure server ports as edge ports (enabled).
This command is disabled by default.

Command mode: interface

`spanning-tree mst cist enable`

Enables MRST on the port.

Command mode: interface

Table 4-35 CIST Port Configuration Commands

Command Syntax and Usage
`no spanning-tree mst cist enable` Disables MRST on the port. **Command mode:** interface
`show interface port {<port-identifier>} spanning-tree mstp cist` Displays the current CIST port configuration. **Command mode:** Any

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 32 Spanning Tree Groups can be configured on the switch (STG 32 is reserved for management).

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

Table 4-36 Spanning Tree Configuration Commands

Command Syntax and Usage
`spanning-tree stp {<stg-identifier>} vlan {<vlan-list>}` Associates a VLAN with a spanning tree and requires an external VLAN ID as a parameter. **Command mode:** config
`no spanning-tree stp {<stg-identifier>} vlan {<vlan-list>}` Breaks the association between a VLAN and a spanning tree and requires an external VLAN ID as a parameter. **Command mode:** config
`no spanning-tree stp {<stg-identifier>} vlan all` Removes all VLANs from a spanning tree. **Command mode:** config
`spanning-tree stp {<stg-identifier>} enable` Globally enables Spanning Tree Protocol. STG is turned on by default. **Command mode:** config
`no spanning-tree stp {<stg-identifier>} enable` Globally disables Spanning Tree Protocol. **Command mode:** config

Table 4-36 Spanning Tree Configuration Commands

Command Syntax and Usage
`default spanning-tree` *`<stg-identifer>`* Restores a spanning tree instance to its default configuration. **Command mode:** config
`show spanning-tree stp {`*`<stg-identifier>`***`}`** Displays current Spanning Tree Protocol parameters. **Command mode:** Any

Bridge Spanning Tree Configuration 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 4-37 Bridge Spanning Tree Configuration Commands

Command Syntax and Usage
`spanning-tree stp {`*`<stg-identifier>`***`} bridge priority {`***`<priority-value>`***`}`** 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 32768. **RSTP/MSTP**: The range is 0 to 61440, in steps of 4096 (0, 4096, 8192...), and the default is 32768. **Command mode:** config
`spanning-tree stp {`*`<stg-identifier>`***`} bridge hello-time {`***`<time-value>`***`}`** 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:** config

Table 4-37 Bridge Spanning Tree Configuration Commands

Command Syntax and Usage
spanning-tree stp {*<stg-identifier>***} bridge maximum-age {***<age-value>***}** 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:** config
spanning-tree stp {*<stg-identifier>***} bridge forward-delay {***<delay-value>***}** 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:** config
spanning-tree stp {*<stg-identifier>***} bridge aging {***<aging-value>***}** 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:** config
show spanning-tree stp {*<stg-identifier>***} bridge** Displays the current bridge STG parameters. **Command mode:** Any

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

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

Spanning Tree Port Configuration 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 4-38 Spanning Tree Port Commands

Command Syntax and Usage
spanning-tree stp {<*stg-identifier*>} priority {<*priority-value*>} 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. **RSTP/MSTP**: The range is 0 to 240, in steps of 16 (0, 16, 32...) and the default is 128. **Command mode:** interface
spanning-tree stp {<*stg-identifier*>} path-cost {<*cost-value*>} 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 range is 1 to 65535. The default is 19 for 100Mbps ports, 4 for 1Gb ports and 2 for 10 Gb ports. A value of 0 indicates that the default cost will be computed for an auto negotiated link speed. **Command mode:** interface
spanning-tree stp {<*stg-identifier*>} link {auto|p2p|shared} Defines the type of link connected to the port, as follows: **auto**: Configures the port to detect the link type, and automatically match its settings. **p2p**: Configures the port for Point-To-Point protocol. **shared**: Configures the port to connect to a shared medium (usually a hub). **Command mode:** interface
[no] spanning-tree stp {<*stg-identifier*>} edge Enables or disables this port as an edge port. An edge port is not connected to a bridge, and can begin forwarding traffic as soon as the link is up. Configure server ports as edge ports (enabled). **Command mode:** interface
spanning-tree stp {<*stg-identifier*>} enable Enables STG on the port. **Command mode:** interface
no spanning-tree stp {<*stg-identifier*>} enable Disables STG on the port. **Command mode:** interface
show interface port {<*port-identifier*>} spanning-tree stp {<*stg-identifier*>} Displays the current STG port parameters. **Command mode:** Any

Trunk Configuration 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 11 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 4 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 4-39 Trunk Configuration Commands

Command Syntax and Usage
mlt {<*mlt-identifier*>} member {<*port-identifier*>} Adds a physical port to the current trunk group. **Command mode:** config
no mlt {<*mlt-identifier*>} member {<*port-identifier*>} Removes a physical port from the current trunk group. **Command mode:** config
mlt {<*mlt-identifier*>} enable Enables the current trunk group. **Command mode:** config
no mlt {<*mlt-identifier*>} enable Disables the current trunk group. **Command mode:** config
no mlt {<*mlt-identifier*>} Removes the current trunk group configuration. **Command mode:** config
show mlt {<*mlt-identifier*>} Displays current trunk group parameters. **Command mode:** Any

IP Trunk Hash Configuration

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

Table 4-40 IP Trunk Hash commands

Command Syntax and Usage
`show mlt hash` Display current trunk hash configuration. Command mode: Any

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 4-41 Layer 2 IP Trunk Hash commands

Command Syntax and Usage
`mlt hash source-mac-address` Enable trunk hashing on the source MAC. **Command mode:** config
`mlt hash destination-mac-address` Enable trunk hashing on the destination MAC. **Command mode:** config
`mlt hash source-ip-address` Enable trunk hashing on the source IP. **Command mode:** config

Table 4-41 Layer 2 IP Trunk Hash commands

Command Syntax and Usage
`mlt hash destination-ip-address` Enable trunk hashing on the destination IP. **Command mode:** config
`mlt hash source-destination-ip` Enable trunk hashing on the source and destination IP. **Command mode:** config
`mlt hash source-destination-mac` Enable trunk hashing on the source and destination MAC address. **Command mode:** config
`show mlt hash` Display current layer 2 trunk hash setting. **Command mode:** Any

Link Aggregation Control Protocol Configuration

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

Table 4-42 Link Aggregation Control Protocol Commands

Command Syntax and Usage
`lacp system-priority {`*`<priority-value>`*`}` Defines the priority value (1 through 65535) for the GbESM. Lower numbers provide higher priority. The default value is 32768. **Command mode:** config
`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**: Nortel Networks recommends 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:** config
`show lacp` Display current LACP configuration. **Command mode:** Any

LACP Port Configuration

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

Table 4-43 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 {`*`<priority-value>`*`}` Sets the priority value for the selected port. Lower numbers provide higher priority. Default is 128. **Command mode:** interface port
`lacp key {`*`<key-value>`*`}` 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-identifier>`*`} lacp` Displays the current LACP configuration for this port. **Command mode:** Any

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 4-44 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:** config
`[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:** config
`failover enable` Globally turns L2 failover `on`. **Command mode:** config
`no failover enable` Globally turns L2 failover `off`. **Command mode:** config
`show failover` Displays current L2 failover parameters. **Command mode:** Any

Failover Trigger Configuration

Table 4-45 Failover Trigger Configuration Commands

Command Syntax and Usage

[no] failover trigger <*trigger-id*> enable

Enables or disables the Failover trigger.

Command mode: config

failover trigger <*trigger-id*> limit <*0-2*>

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: config

show failover trigger <*trigger-id*>

Displays the current failover trigger settings.

Auto Monitor Configuration

Table 4-46 Auto Monitor Configuration Commands

Command Syntax and Usage

failover trigger <*trigger-id*> amon trunk <*1-11*>

Adds a trunk group to the Auto Monitor.

Command mode: config

no failover trigger <*trigger-id*> amon trunk <*1-13*>

Removes a trunk group from the Auto Monitor.

Command mode: config

failover trigger <*trigger-id*> 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: config

no failover trigger <*trigger-id*> amon admin-key <*1-65535*>

Removes a LACP admin key from the Auto Monitor.

Command mode: config

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 4-47 VLAN Configuration Commands

Command Syntax and Usage
`protocol-vlan {<PVLAN-identifier>}` Configures the Protocol-based VLAN (PVLAN). **Command mode:** vlan
`name {<name-string>}` Assigns a name to the VLAN or changes the existing name. The default VLAN name is the first one. **Command mode:** vlan
`stg {<stg-identifier>}` Assigns a VLAN to a Spanning Tree Group. **Command mode:** vlan
`member {<port-identifier>}` Adds port(s) to the VLAN membership. **Command mode:** vlan
`no member {<port-identifier>}` 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 4-47 VLAN Configuration Commands

Command Syntax and Usage
no vlan {<*vlan-identifier*>**}** Deletes this VLAN. **Command mode:** vlan
show vlan [<*vlan-identifier*>**]** Displays the current VLAN configuration. **Command mode:** Any

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 4-48 Protocol VLAN Menu commands

Command Syntax and Usage
protocol-vlan {<*pvlan-identifier*>**} 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 {<*pvlan-identifier*>**} priority {**<*0-7*>**}** Configures the priority value for this PVLAN. **Command mode:** vlan
protocol-vlan {<*pvlan-identifier*>**} member {**<*port-identifier*>**}** Adds a port to the selected PVLAN. **Command mode:** vlan
no protocol-vlan {<*pvlan-identifier*>**} member {**<*port-identifier*>**}** Removes a port from the selected PVLAN. **Command mode:** vlan

Table 4-48 Protocol VLAN Menu commands

Command Syntax and Usage
`no protocol-vlan {`*`<pvlan-identifier>`***`}`** Deletes the selected protocol configuration from the VLAN. **Command mode:** vlan
`protocol-vlan {`*`<pvlan-identifier>`***`} enable`** Enables the selected protocol on the VLAN. **Command mode:** vlan
`no protocol-vlan {`*`<pvlan-identifier>`***`} enable`** Disables the selected protocol on the VLAN. **Command mode:** vlan
`[no] protocol-vlan {`*`<pvlan-identifier>`***`} tag-pvlan`** Enables or disables port tagging on this PVLAN. **Command mode:** vlan
`[no] protocol-vlan {`*`<pvlan-identifier>`***`} tag-pvlan {`***`<port-identifier>`***`}`** Defines a port that will be tagged by the selected protocol on this VLAN. **Command mode:** vlan
`show protocol-vlan {`*`<pvlan-identifier>`***`}`** Displays current parameters for the selected PVLAN. **Command mode:** Any

Layer 3 Configuration

Table 4-49 Layer 3 Configuration Commands

Command Syntax and Usage
`interface ip {<`*`interface-instance`***`>}`** Configures the IP Interface. **Command mode:** config To view command options, see page 174.
`router rip` Configures the Routing Interface Protocol. **Command mode:** config To view command options, see page 184.
`router ospf` Configures OSPF. **Command mode:** config To view command options, see page 187.
`router bg` Configures Border Gateway Protocol. **Command mode:** config To view command options, see page 195.
`router vrrp` Configures Virtual Router Redundancy. **Command mode:** config To view command options, see page 208.
`ip router-id` *`<ip-address>`* Sets the router ID. **Command mode:** config
`show layer3` Displays the current IP configuration. **Command mode:** Any

IP Interface Configuration

The GbE Switch Module can be configured with up to 128 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 4-50 IP Interface Configuration Commands

Command Syntax and Usage

ip address {*<ip-address>***}{***<ip-netmask>***}**

Configures the IP address of the switch interface, or the IP subnet address mask for the interface, using dotted decimal notation.

Command mode: interface ip

vlan {*<vlan-instance>***}**

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

no interface ip {*<interface-instance>***}**

Removes this IP interface.

Command mode: config

show interface ip {*<interface-identifier>***}**

Displays the current interface settings.

Command mode: Any

Default Gateway Configuration

NOTE – The switch can be configured with up to 132 gateways. Gateways one to four are reserved for default gateways. Gateway 132 is reserved for the management VLAN.

This option is disabled by default.

Table 4-51 Default Gateway Commands

Command Syntax and Usage
`ip gateway {<`*`gateway-instance`***`>} address {<`***`ip-address`***`>}`** Configures the IP address of the default IP gateway using dotted decimal notation. **Command mode:** config
`ip gateway {<`*`gateway-instance`***`>} interval {<`***`interval-value`***`>}`** 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:** config
`ip gateway {<`*`gateway-instance`***`>} retry {<`***`retry-value`***`>}`** 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:** config
`[no] ip gateway {<`*`gateway-instance`***`>} arp-health-check`** Enables or disables Address Resolution Protocol (ARP) health checks. This command is disabled by default. **Command mode:** config
`ip gateway {<`*`gateway-instance`***`>} vlan {<`***`vlan-instance`***`>}`** Sets the VLAN to be assigned to this default IP gateway. **Command mode:** config
`ip gateway {<`*`gateway-instance`***`>} enable`** Enables the gateway for use. **Command mode:** config
`no ip gateway {<`*`gateway-instance`***`>} enable`** Disables the gateway. **Command mode:** config

Table 4-51 Default Gateway Commands

Command Syntax and Usage
`no ip gateway {`*`<gateway-instance>`***`}`** Deletes the gateway from the configuration. **Command mode:** config
`show ip gateway {`*`<gateway-instance>`***`}`** Displays the current gateway settings. **Command mode:** All except User EXEC

Default Gateway Metrics

For information about configuring which gateway is selected when multiple default gateways are enabled, see page 176.

IP Static Route Configuration

Up to 128 static routes can be configured.

Table 4-52 IP Static Route Configuration Commands

Command Syntax and Usage
`ip route` *`<ip-subnet> <ip-netmask> <ip-nexthop>`* **`[`***`<ip-interface-value>`***`]`** 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:** config
`no ip route {`*`<ip-subnet>`***`}{`***`<ip-netmask>`***`}`** Removes a static route. The destination address of the route to remove must be specified using dotted decimal notation. **Command mode:** config
`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 4-53 IP Multicast Route Configuration Commands

Command Syntax and Usage
ip mroute *<IPMC destination> <vlan> <port> <primary|backup|host> <vr id|none>* 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. **Command mode:** config
no ip mroute *<IPMC destination> <vlan> <port> <primary|backup|host> <vr id|none>* Removes a static multicast route. The destination address, VLAN, and member port of the route to remove must be specified. **Command mode:** config
show ip mroute Displays the current IP multicast routes. **Command mode:** All except User EXEC

ARP Configuration

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

Table 4-54 ARP Configuration Commands

Command Syntax and Usage
ip arp rearp {*<rearp-value>***}** Defines re-ARP period in minutes. You can set this duration between 2 and 120 minutes. **Command mode:** config
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 4-55 ARP Static Configuration Commands

Command Syntax and Usage
ip arp *<ip-address> <mac-address> <vlan-instance> <port-instance>* Adds a permanent ARP entry. **Command mode:** config
no ip arp {*<ip-address>***}** Deletes a permanent ARP entry. **Command mode:** config
show ip arp Displays current static ARP configuration. **Command mode:** All except User EXEC

IP Forwarding Configuration

Table 4-56 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: config

`ip routing`

Enables IP forwarding (routing) on the GbE Switch Module.

Command mode: config

`no ip routing`

Disables IP forwarding (routing) on the GbE Switch Module. Forwarding is turned off by default.

Command mode: config

`show ip routing`

Displays the current IP forwarding settings.

Command mode: All except User EXEC

Network Filter Configuration

Table 4-57 IP Network Filter Configuration Commands

Command Syntax and Usage

`ip match-address` *`<match-id> <ip-address> <mask>`*

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

Command mode: config.

`ip match-address` *`<match-id>`* **`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: config

`ip match-address` *`<match-id>`* **`enable`**

Enables the Network Filter configuration.

Command mode: config

Table 4-57 IP Network Filter Configuration Commands

Command Syntax and Usage

`no ip match-address <match-id> enable`

Disables the Network Filter configuration.

Command mode: config

`no ip match-address <match-id>`

Deletes the Network Filter configuration.

Command mode: config

`show ip match-address [<match-id>]`

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 4-58 Routing Map Configuration Commands

Command Syntax and Usage

`[no] access-list <alist-id>`

Configures the Access List.

Command mode: route-map

For more information, see page 182.

`[no] as-path-list <pathlist-id>`

Configures the Autonomous System (AS) Filter.

Command mode: route-map

For more information, see page 183.

`[no] as-path-preference <preference-value>`

Sets the AS path preference of the matched route. One to three path preferences can be configured.

Command mode: route-map

`[no] local-preference <preference-value>`

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

Table 4-58 Routing Map Configuration Commands

Command Syntax and Usage

`[no] metric` *`<metric-value>`*

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.

- **Type 1**—External routes are calculated using both internal and external metrics.
- **Type 2**—External routes are calculated using only the external metrics. Type 1 routes have more cost than Type 2.
- **`none`**—Removes the OSPF metric.

Command mode: route-map

`precedence` *`<precedence-value>`*

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` *`<weigh-value>`*

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` *`<rmap-id>`*

Deletes the route map.

Command mode: config

`show route-map [`*`<rmap-id>`***`]`**

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 4-59 IP Access List Configuration Commands

Command Syntax and Usage
`[no] access-list` *`<alist-id>`* **`match-address`** *`<match-id>`* Sets the network filter number. **Command mode:** route-map See "Network Filter Configuration" on page 179 for details.
`[no] access-list` *`<alist-id>`* **`metric`** *`<metric-value>`* Sets the metric value in the AS-External (ASE) LSA. **Command mode:** route-map
`access-list` *`<alist-id>`* **`action {permit|deny}`** Permits or denies action for the access list. **Command mode:** route-map
`access-list` *`<alist-id>`* **`enable`** Enables the access list. **Command mode:** route-map
`no access-list` *`<alist-id>`* **`enable`** Disables the access list. **Command mode:** route-map
`no access-list` *`<alist-id>`* Deletes the access list. **Command mode:** route-map
`show route-map` *`<map-id>`* **`access-list {`***`<alist-id>`***`}`** Displays the current Access List configuration. **Command mode:** All except User EXEC

Autonomous System Filter Path Configuration

NOTE – The *rmap number (*1-32) and the *path number* (1-8) represent the AS path you wish to configure.

Table 4-60 AS Filter Configuration Commands

Command Syntax and Usage
as-path-list *<pathlist-id>* **as-path** *<path-number>* Sets the Autonomous System filter's path number. **Command mode:** route-map
as-path-list *<pathlist-id>* **action {permit|deny}** Permits or denies Autonomous System filter action. **Command mode:** route-map
as-path-list *<pathlist-id>* **enable** Enables the Autonomous System filter. **Command mode:** route-map
no as-path-list *<pathlist-id>* **enable** Disables the Autonomous System filter. **Command mode:** route-map
no as-path-list *<pathlist-id>* Deletes the Autonomous System filter. **Command mode:** route-map
show route-map *<rmap-id>* **as-path-list {***<pathlist-id>***}** Displays the current Autonomous System filter configuration. **Command mode:** All except User EXEC

router rip

Routing Information Protocol Configuration

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

Table 4-61 Routing Information Protocol Commands

Command Syntax and Usage
`timers update {<update-value>}` 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 4-62 Routing Information Protocol Commands

Command Syntax and Usage
`ip rip version` *`<version-value>`* Configures the RIP version used by this interface. The default value is version `1`. **Command mode:** interface ip
`[no] ip rip supply` This command is disabled by default. When enabled, the switch supplies routes to other routers. **Command mode:** interface ip
`[no] ip rip listen` This command is disabled by default. When enabled, the switch learns routes from other routers. **Command mode:** interface ip
`[no] ip rip poison` This command is disabled by default. When enabled, the switch uses split horizon with poisoned reverse. When disabled, the switch uses only split horizon. **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 `disabled`. **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 `disabled`. **Command mode:** interface ip
`[no] ip rip default-action {both|listen|supply}` 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. This command is disabled by default. **Command mode:** interface ip

Table 4-62 Routing Information Protocol Commands

Command Syntax and Usage
`[no] ip rip metric {`*`<cost-value>`***`}`** 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 {`*`<key-value>`***`}`** 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 [<`*`ip interface id`***`>] rip`** Displays the current RIP configuration. **Command mode:** All except User EXEC

`router ospf`

Open Shortest Path First Configuration

Table 4-63 OSPF Configuration Commands

Command Syntax and Usage
`area-range` *`<area-id>`* Configures summary routes for up to 16 IP addresses. **Command mode:** router ospf See page 189 to view command options.
`ip ospf` Configures the OSPF interface. **Command mode:** interface ip See page 190 to view command options.
`area-virtual-link` *`<area-id>`* Configures the Virtual Links used to configure OSPF for a Virtual Link. **Command mode:** router ospf See page 192 to view command options.
`message-digest-key` *`<key-id>`* **`md5-key`** *`<WORD>`* Assigns a string to MD5 authentication key. **Command mode:** router ospf
`host` *`<host-index>`* 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 193 to view command options.
`lsdb-limit` *`<limit-value>`* Sets the link state database limit. **Command mode:** router ospf
`[no] default-information` *`<metric-value> <as-value>`* Sets one default route among multiple choices in an area. Use `none` for no default. **Command mode:** router ospf
`enable` Enables OSPF on the GbE Switch Module. **Command mode:** router ospf

Table 4-63 OSPF Configuration Commands

Command Syntax and Usage

`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 4-64 Area Index Configuration Commands

Command Syntax and Usage

`area` *`<area-id>`* **`area-id`** *`<ip-address>`*

Defines the IP address of the OSPF area number.

Command mode: router ospf

`area` *`<area-id>`* **`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` *`<area-id>`* **`stub-metric`** *`<metric-value>`*

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 4-64 Area Index Configuration Commands

Command Syntax and Usage

[no] area *<area-id>* **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 *<area-id>* **spf-interval** *<interval-value>*

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 *<area-id>* **enable**

Enables the OSPF area.

Command mode: router ospf

no area *<area-id>* **enable**

Disables the OSPF area.

Command mode: router ospf

no area *<area-id>*

Deletes the OSPF area.

Command mode: router ospf

show ip ospf area *<area-id>*

Displays the current OSPF configuration.

Command mode: All except User EXEC

OSPF Summary Range Configuration

Table 4-65 OSPF Summary Range Configuration Commands

Command Syntax and Usage

area-range *<area-id>* **address** *<ip-address> <ip-netmask>*

Displays the base IP address or the IP address mask for the range.

Command mode: router ospf

area-range *<area-id>* **area** *<area-id>*

Displays the area index used by the GbE Switch Module.

Command mode: router ospf

Table 4-65 OSPF Summary Range Configuration Commands

Command Syntax and Usage
`[no] area-range <area-id> hide` Hides the OSPF summary range. **Command mode:** router ospf
`area-range <area-id> enable` Enables the OSPF summary range. **Command mode:** router ospf
`no area-range <area-id> enable` Disables the OSPF summary range. **Command mode:** router ospf
`no area-range <area-id>` Deletes the OSPF summary range. **Command mode:** router ospf
`show ip ospf area-range <area-id>` Displays the current OSPF summary range. **Command mode:** router ospf

OSPF Interface Configuration

Table 4-66 OSPF Interface Configuration Commands

Command Syntax and Usage
`ip ospf area <area-id>` Configures the OSPF area index. **Command mode:** interface ip
`ip ospf priority <priority-value>` 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 <cost-value>` 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 4-66 OSPF Interface Configuration Commands

Command Syntax and Usage
`ip ospf hello-interval` *`<interval-value>`* Configures the interval in seconds between the `hello` packets for the intefaces. **Command mode:** interface ip
`ip ospf dead-interval` *`<interval-value>`* 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` *`<delay-value>`* Configures the transit delay in seconds. **Command mode:** interface ip
`ip ospf retransmit-interval` *`<interval-value>`* 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` *`<key-id>`* 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` *`<interface-index>`* **`ospf`** Displays the current settings for OSPF interface. **Command mode:** All except User EXEC

OSPF Virtual Link Configuration

Table 4-67 OSPF Virtual Link Configuration Commands

Command Syntax and Usage
`area-virtual-link` *`<1-3>`* **`area`** *`<area-id>`* Configures the OSPF area index for the virtual link. **Command mode:** router ospf
`area-virtual-link` *`<1-3>`* **`hello-interval`** *`<interval-value>`* 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`** *`<interval-value>`* 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`** *`<delay-value>`* Configures the delay in transit in seconds. Default is one second. **Command mode:** router ospf
`area-virtual-link` *`<1-3>`* **`retransmit-interval`** *`<interval-value>`* 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`** *`<key-id>`* 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 4-67 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:** router ospf

OSPF Host Entry Configuration

Table 4-68 OSPF Host Entry Configuration Commands

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

OSPF Route Redistribution Configuration .

Table 4-69 OSPF Route Redistribution Configuration Commands

Command Syntax and Usage

redistribute {fixed|static|rip|ebgp|ibgp} {<*rmap-id*>}

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*>}

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 <*metric-value*> 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: router ospf

OSPF MD5 Key Configuration

Table 4-70 OSPF MD5 Key Configuration Command Options

Command Syntax and Usage

message-digest-key <*key-id*> md5-key <*key-string*>

Sets the authentication key for this OSPF packet.

Command mode: router ospf

no message-digest-key <*key-id*>

Deletes the authentication key for this OSPF packet.

Command mode: router ospf

show ip ospf message-digest-key <*key-id*>

Displays the current MD5 key configuration.

Command mode: All except User EXEC

`router bgp`

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 4-71 Border Gateway Protocol Commands

Command Syntax and Usage
`neighbor` *`<nbr-id>`* Configures each BGP *peer.* Each border router, within an autonomous system, exchanges routing information with routers on other external networks. **Command mode:** router bgp To view command options, see page 196.
`as` Set Autonomous System number. **Command mode:** router bgp
`local-preference` *`<preference-value>`* 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

Table 4-71 Border Gateway Protocol Commands

Command Syntax and Usage

`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 4-72 BGP Peer Configuration Commands

Command Syntax and Usage

`neighbor` *`<nbr-id>`* **`remote-address`** *`<ip-address>`*

Defines the IP address for the specified peer (border router), using dotted decimal notation. The default address is 0.0.0.0.

Command mode: router bgp

`neighbor` *`<nbr-id>`* **`remote-as`** *`<as-number>`*

Sets the remote autonomous system number for the specified peer.

Command mode: router bgp

`neighbor` *`<nbr-id>`* **`timers hold-time`** *`<time-value>`*

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

`neighbor` *`<nbr-id>`* **`timers keep-alive`** *`<time-value>`*

Sets the keep-alive time for the specified peer in seconds. It is set at 0 by default.

Command mode: router bgp

`neighbor` *`<nbr-id>`* **`advertisement-interval`** *`<interval-value>`*

Sets time in seconds between advertisements.

Command mode: router bgp

Table 4-72 BGP Peer Configuration Commands

Command Syntax and Usage

`neighbor` *`<nbr-id>`* **`retry-interval`** *`<interval-value>`*

Sets connection retry interval in seconds.

Command mode: router bgp

`neighbor` *`<nbr-id>`* **`route-origination-interval`** *`<interval-value>`*

Sets the minimum time between route originations in seconds.

Command mode: router bgp

`neighbor` *`<nbr-id>`* **`time-to-live`** *`<ttl-value>`*

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` *`<nbr-id>`* **`route-map in`** *`<map-id>`*

Adds route map into in-route map list.

Command mode: router bgp

`neighbor` *`<nbr-id>`* **`route-map out`** *`<map-id>`*

Adds route map into out-route map list.

Command mode: router bgp

`no neighbor` *`<nbr-id>`* **`route-map in`** *`<map-id>`*

Removes route map from in-route map list.

Command mode: router bgp

`no neighbor` *`<nbr-id>`* **`route-map out`** *`<map-id>`*

Removes route map from out-route map list.

Command mode: router bgp

`no neighbor` *`<nbr-id>`* **`shutdown`**

Enables this peer configuration.

Command mode: router bgp

`neighbor` *`<nbr-id>`* **`shutdown`**

Disables this peer configuration.

Command mode: router bgp

Table 4-72 BGP Peer Configuration Commands

Command Syntax and Usage

no neighbor *<nbr-id>*

Deletes this peer configuration.

Command mode: router bgp

show ip bgp neighbor [*<nbr-id>***]**

Displays the current BGP peer configuration.

Command mode: All except User EXEC

BGP Redistribution Configuration

Table 4-73 BGP Redistribution Configuration Commands

Command Syntax and Usage

[no] neighbor *<nbr-id>* **redistribute default-metric** *<metric-value>*

Sets default metric of advertised routes.

Command mode: router bgp

[no] neighbor *<nbr-id>* **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 even though it does not have any default routes in its routing table.

Redistribute: Default routes are either configured through default gateway or learned through other protocols and redistributed to peer. If the routes are learned from default gateway configuration, you have to enable static routes since the routes from default gateway are static routes. Similarly, if the routes are learned from a certain routing protocol, you have to enable that protocol.

Command mode: router bgp

[no] neighbor *<nbr-id>* **redistribute rip**

Enables or disables advertising RIP routes.

Command mode: router bgp

[no] neighbor *<nbr-id>* **redistribute ospf**

Enables or disables advertising OSPF routes.

Command mode: router bgp

Table 4-73 BGP Redistribution Configuration Commands

Command Syntax and Usage
`[no] neighbor` *`<nbr-id>`* **`redistribute fixed`** Enables or disables advertising fixed routes. **Command mode:** router bgp
`[no] neighbor` *`<nbr-id>`* **`redistribute static`** Enables or disables advertising static routes. **Command mode:** router bgp
`show ip bgp neighbor` *`<nbr-id>`* **`redistribute`** Displays current redistribution configuration. **Command mode:** All except User EXEC

BGP Aggregation Configuration

These commands enable you to configure filters that specify the routes/range of IP destinations a peer router will accept from other peers. A route must match a filter to be installed in the routing table. By default, the first filter is enabled and the rest of the filters are disabled.

Table 4-74 BGP Filter Configuration Commands

Command Syntax and Usage
`aggregate-address` *`<aggregation number> <ip-address> <ip-netmask>`* Defines the starting IP address for this filter, using dotted decimal notation. The default address is 0.0.0.0. **Command mode:** router bgp
`aggregate-address` *`<aggregation number>`* **`enable`** Enables this BGP filter. **Command mode:** router bgp
`no aggregate-address` *`<aggregation number>`* **`enable`** Disables this BGP filter. **Command mode:** router bgp
`no aggregate-address` *`<aggregation number>`* Deletes this BGP filter. **Command mode:** router bgp
`show ip bgp aggregate-address [` *`<aggregation number>`* **`]`** Displays the current BGP filter configuration. **Command mode:** All except User EXEC

IGMP Configuration

Table 4-75 describes the commands used to configure basic IGMP parameters.

Table 4-75 IGMP Configuration Commands

Command Syntax and Usage
`ip igmp enable` Globally turns IGMP on. **Command mode:** config
`no ip igmp` Globally turns IGMP off. **Command mode:** config
`[no] ip igmp aggregate` Enables or disables IGMP Membership Report aggregation. **Command mode:** config
`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 4-76 describes the commands used to configure IGMP Snooping.

Table 4-76 IGMP Snooping Configuration Commands

Command Syntax and Usage
`ip igmp snoop enable` Globally turns IGMP on. **Command mode:** config
`no ip igmp snoop enable` Globally turns IGMP off. **Command mode:** config

Table 4-76 IGMP Snooping Configuration Commands

Command Syntax and Usage
ip igmp snoop mrouter-timeout *<timeout-value>* 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:** config
ip igmp snoop source-ip *<IP addr>* Configures the source IP address used as a proxy for IGMP Group Specific Queries. **Command mode:** config
ip igmp snoop vlan *<vlan-instance>* Adds the selected VLAN(s) to IGMP Snooping. **Command mode:** config
no ip igmp snoop vlan *<vlan-instance>* **enable** Removes the selected VLAN(s) from IGMP Snooping. **Command mode:** config
no ip igmp snoop vlan all Removes all VLANs from IGMP Snooping. **Command mode:** config
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 4-79 describes the commands used to configure IGMP Relay.

Table 4-77 IGMP Relay Configuration Commands

Command Syntax and Usage
ip igmp relay enable Enables IGMP Relay. **Command mode:** config
no ip igmp relay enable Disables IGMP Relay. **Command mode:** config

Table 4-77 IGMP Relay Configuration Commands

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

IGMP Relay Multicast Router Configuration

Table 4-79 describes the commands used to configure muticast routers for IGMP Relay.

Table 4-78 IGMP Relay Mrouter Configuration Commands

Command Syntax and Usage
`ip igmp relay mrtr` *`<1-2>`* **`address`** *`<IP addr>`* Configures the IP address of the IGMP multicast router used for IGMP Relay. **Command mode:** config
`ip igmp relay mrtr` *`<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:** config
`ip igmp relay mrtr` *`<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:** config
`ip igmp relay version` *`<1-2>`* Configures the IGMP version (1 or 2) of the multicast router. **Command mode:** config

Table 4-78 IGMP Relay Mrouter Configuration Commands

Command Syntax and Usage
`ip igmp relay mrtr` *`<1-2>`* **`enable`** Enables the multicast router. **Command mode:** config
`no ip igmp relay mrtr` *`<1-2>`* **`enable`** Disables the multicast router. **Command mode:** config
`no ip igmp relay mrtr` *`<1-2>`* Deletes the multicast router from IGMP Relay. **Command mode:** config

IGMP Static Multicast Router Configuration

Table 4-79 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 4-79 IGMP Static Multicast Router Configuration Commands

Command Syntax and Usage
`ip igmp mrouter` *`<port-identifier> <vlan-instance> <version-number>`* 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-EXT4). **Command mode:** config
`no ip igmp mrouter` *`<port-identifier> <vlan-instance> <version-number>`* Removes a static multicast router from the selected port/VLAN combination. **Command mode:** config
`show ip igmp mrouter` Displays the current IGMP Static Multicast Router parameters. **Command mode:** All except User EXEC

IGMP Filtering Configuration

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

Table 4-80 IGMP Filtering Configuration Commands

Command Syntax and Usage
ip igmp profile *<filter-instance>* Configures the IGMP filter. **Command mode:** config To view command options, see page 204.
ip igmp filtering Enables IGMP filtering globally. **Command mode:** config
no ip igmp filtering Disables IGMP filtering globally. **Command mode:** config
show ip igmp filtering Displays the current IGMP Filtering parameters. **Command mode:** All except User EXEC

IGMP Filter Definition

Table 4-81 describes the commands used to define an IGMP filter.

Table 4-81 IGMP Filter Definition Commands

Command Syntax and Usage
ip igmp profile *<filter-instance>* **range** *<ip-address1> <ip-address2>* Configures the range of IP multicast addresses for this filter. **Command mode:** config
ip igmp profile *<filter-instance>* **action {allow|deny}** Allows or denies multicast traffic for the IP multicast addresses specified. **Command mode:** config
ip igmp profile *<filter-instance>* **enable** Enables this IGMP filter. **Command mode:** config

Table 4-81 IGMP Filter Definition Commands

Command Syntax and Usage
`no ip igmp profile` *`<filter-instance>`* **`enable`** Disables this IGMP filter. **Command mode:** config
`no ip igmp profile` *`<filter-instance>`* Deletes this filter's parameter definitions. **Command mode:** config
`show ip igmp profile` *`<filter-instance>`* Displays the current IGMP filter. **Command mode:** config

IGMP Filtering Port Configuration

Table 4-82 describes the commands used to configure a port for IGMP filtering.

Table 4-82 IGMP Filter Port Configuration Commands

Command Syntax and Usage
`[no] ip igmp filtering` Enables or disables IGMP filtering on this port. **Command mode:** interface
`ip igmp profile` *`<filter-instance>`* Adds an IGMP filter to this port. **Command mode:** interface
`no ip igmp profile` *`<filter-instance>`* Removes an IGMP filter from this port. **Command mode:** interface
`show interface port {` *`<port-identifier>`* **`} igmp-filtering`** Displays the current IGMP filter parameters for this port. **Command mode:** All except User EXEC

IGMP Advanced Configuration

Table 4-79 describes the commands used to configure advanced IGMP parameters.

Table 4-83 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:** config
`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:** config
`ip igmp timeout` *`<timeout-value>`* 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:** config
`[no] ip igmp` *`<vlan-instance>`* **`fastleave`** Enables or disables Fastleave processing. Fastleave allows the switch to immediately remove a port from the IGMP port list, if the host sends a Leave message, and the proper conditions are met. This command is disabled by default. **Command mode:** config
`[no] ip igmp flood` Configures the switch to flood unregistered IP multicast reports to all ports. **Command mode:** config

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 4-84 Domain Name Service Commands

Command Syntax and Usage
`[no] ip name-server` *`<ip-address>`* You will be prompted to set the IP address for your primary DNS server. Use dotted decimal notation. **Command mode:** config
`[no] ip name-server` *`<ip-address>`* 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. **Command mode:** config
`[no] ip domain-name` *`<name>`* Sets the default domain name used by the switch. For example: `mycompany.com` **Command mode:** config
`show ip dns` Displays the current Domain Name System settings. **Command mode:** All except User EXEC

Bootstrap Protocol Relay Configuration

The Bootstrap Protocol (BOOTP) Relay commands are used to allow hosts to obtain their configurations from a Dynamic Host Configuration Protocol (DHCP) server. The BOOTP configuration enables the switch to forward a client request for an IP address to two DHCP/BOOTP servers with IP addresses that have been configured on the GbE Switch Module.

BOOTP relay is turned off by default.

Table 4-85 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:** config
`ip bootp-relay enable` Globally turns on BOOTP relay. **Command mode:** config
`no ip bootp-relay enable` Globally turns off BOOTP relay. **Command mode:** config
`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 4-86 Virtual Router Redundancy Protocol Commands

Command Syntax and Usage
`[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 up to 128 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 4-87 VRRP Virtual Router Configuration Commands

Command Syntax and Usage

`virtual-router` *`<index>`* **`virtual-router-id`** *`<vr-id>`*

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` *`<vr-id>`* **`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` *`<vr-id>`* **`interface`** *`<interface-instance>`*

Selects a switch IP interface (between 1 and 128). 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 preempt another virtual router which has assumed master routing authority. This preemption occurs even if the `preem` option below is disabled. The default value is 1.

Command mode: router vrrp

`virtual-router` *`<vr-id>`* **`priority`** *`<pri-value>`*

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` *`<vr-id>`* **`timers advertise`** *`<interval-value>`*

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

Table 4-87 VRRP Virtual Router Configuration Commands

Command Syntax and Usage
[no] virtual-router *<vr-id>* **preemption** Enables or disables master preemption. When enabled, if this virtual router is in backup mode but has a higher priority than the current master, this virtual router will preempt the lower priority master and assume control. Note that even when `preemption` is disabled, this virtual router will always preempt 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 *<vr-id>* **enable** Enables this virtual router. **Command mode:** router vrrp
no virtual-router *<vr-id>* **enable** Disables this virtual router. **Command mode:** router vrrp
no virtual-router *<vr-id>* Deletes this virtual router from the switch configuration. **Command mode:** router vrrp
show ip vrrp virtual-router *<vr-id>* Displays the current configuration information for this virtual router. **Command mode:** All except User EXEC

Virtual Router Priority Tracking Configuration

These commands are used for modifying the priority system used when electing the master router from a pool of virtual routers. Various tracking criteria can be used to bias the election results. Each time one of the tracking criteria is met, the priority level for the virtual router is increased by an amount defined through the VRRP Tracking commands.

Criteria are tracked dynamically, continuously updating virtual router priority levels when enabled. If the virtual router preemption option is enabled, this virtual router can assume master routing authority when its priority level rises above that of the current master.

Some tracking criteria apply to standard virtual routers, otherwise called "virtual interface routers." A virtual *server* router is defined as any virtual router whose IP address is the same as any configured virtual server IP address.

Table 4-88 VRRP Priority Tracking Configuration Commands

Command Syntax and Usage
`[no] virtual-router` *`<vr-id>`* **`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` *`<vr-id>`* **`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` *`<vr-id>`* **`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` *`<vr-id>`* **`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 4-89 VRRP Virtual Router Group Configuration Commands

Command Syntax and Usage

`group virtual-router-id` *`<gvr-id>`*

Defines the virtual router ID.

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

Command mode: router vrrp

`group interface` *`<interface-instance>`*

Selects a switch IP interface (between 1 and 128). The default switch IP interface number is 1.

Command mode: router vrrp

`group priority` *`<pri-value>`*

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` *`<interval-value>`*

Defines the time interval between VRRP master advertisements. This can be any integer between 1 and 255 seconds. The default is 1.

Command mode: router vrrp

`[no] group preemption`

Enables or disables master preemption. When enabled, if the virtual router group is in backup mode but has a higher priority than the current master, this virtual router will preempt the lower priority master and assume control. Note that even when `preemption` is disabled, this virtual router will always preempt 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

Table 4-89 VRRP Virtual Router Group Configuration Commands

Command Syntax and Usage
`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 4-90 Virtual Router Group Priority Tracking Configuration Commands

Command Syntax and Usage
`[no] group 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] 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

Table 4-90 Virtual Router Group Priority Tracking Configuration Commands

Command Syntax and Usage
`[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-id* (1 to 128) 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 4-91 VRRP Interface Commands

Command Syntax and Usage
`interface` *`<interface-id>`* **`authentication {password|none}`** Defines the type of authentication that will be used: `none` (no authentication) or `password` (password authentication). **Command mode:** router vrrp
`interface` *`<interface-id>`* **`password`** *`<password>`* Defines a plain text password up to eight characters long. This password will be added to each VRRP packet transmitted by this interface when password authentication is chosen (see **`interface authentication`** above). **Command mode:** router vrrp
`no interface` *`<interface-id>`* Clears the authentication configuration parameters for this IP interface. The IP interface itself is not deleted. **Command mode:** router vrrp
`show ip vrrp interface` *`<interface-id>`* 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 211), the priority level for the virtual router is increased by a defined amount.

Table 4-92 VRRP Tracking Configuration Commands

Command Syntax and Usage
`tracking-priority-increment virtual-routers` *`<increment-value>`* 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` *`<increment-value>`* Defines the priority increment value (0 through 254) for active IP interfaces detected on this switch. The default value is 2. **Command mode:** router vrrp
`tracking-priority-increment ports` *`<increment-value>`* Defines the priority increment value (0 through 254) 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 211) 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 4-93 802.1p Configuration Commands

Command Syntax and Usage
`qos transmit-queue mapping` *`<pri> <queue-number>`* Maps the 802.1p priority of to the Class of Service queue (COSq) priority. Enter the 802.1p priority value (0-7), followed by the Class of Service queue (0-7) that handles the matching traffic. **Command mode:** config
`qos transmit-queue weight-cos` *`<queue-number> <weight-value>`* Configures the weight of the selected Class of Service queue (COSq). Enter the queue number (0-7), followed by the scheduling weight (0-15). **Command mode:** config
`qos transmit-queue number-cos {2|8}` Sets the number of Class of Service queues for switch ports. Default is 2. **Command mode:** config
`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 4-94 DSCP Configuration Commands

Command Syntax and Usage
`qos dscp dscp-mapping` *`<dscp> <dscp>`* 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:** config
`qos dscp dot1p-mapping` *`<dscp> <pri>`* 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:** config
`qos dscp re-marking` Turns on DSCP re-marking globally. **Command mode:** config
`no qos dscp re-marking` Turns off DSCP re-marking globally. **Command mode:** config
`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 4-95 General ACL Configuration Commands

Command Syntax and Usage
`[no] access-control list` *`<list-number>`* Configures an Access Control List. **Command mode:** config To view command options, see page 219.
`[no] access-control group <group-number>` Configures an ACL Group. **Command mode:** config To view command options, see page 224.
`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 4-96 ACL Configuration Commands

Command Syntax and Usage
`[no] access-control list` *`<list-number>`* **`egress-port`** *`<port-instance>`* Configures the ACL to function on egress packets. **Command mode:** config
`access-control list` *`<list-number>`* **`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:** config
`access-control list` *`<list-number>`* **`statistics`** Enables or disables the statistics collection for the Access Control List. **Command mode:** All except User EXEC

Table 4-96 ACL Configuration Commands

Command Syntax and Usage
`default access-control list` *`<list-number>`* Resets the ACL parameters to their default values. **Command mode:** config
`show access-control list` *`<list-number>`* 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 4-97 Ethernet Filtering Configuration Commands

Command Syntax and Usage
`access-control list` *`<list-number>`* **`ethernet source-mac-address`** *`<mac-address>`* Defines the source MAC address for this ACL. **Command mode:** config
`access-control list` *`<list-number>`* **`ethernet destination-mac-address`** *`<mac-address>`* Defines the destination MAC address for this ACL. **Command mode:** config
`access-control list` *`<list-number>`* **`ethernet vlan`** *`<vid> <mask>`* Defines a VLAN number and mask for this ACL. **Command mode:** config
`access-control list` *`<list-number>`* **`ethernet ethernet-type`** *`<etype>`* Defines the Ethernet type for this ACL. **Command mode:** config
`access-control list` *`<list-number>`* **`ethernet priority`** *`<0-7>`* Defines the Ethernet priority value for the ACL. **Command mode:** config

Table 4-97 Ethernet Filtering Configuration Commands

Command Syntax and Usage

`default access-control list` *`<list-number>`* **`ethernet`**

Resets Ethernet parameters for the ACL to their default values.

Command mode: config

`show access-control list {`*`<list-number>`***`} 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 4-98 IP version 4 Filtering Configuration Commands

Command Syntax and Usage

`access-control list` *`<list-number>`* **`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: config

`access-control list` *`<list-number>`* **`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: config

`access-control list` *`<list-number>`* **`ipv4 protocol`** *`<proto>`*

Defines an IP protocol for the ACL. If defined, traffic from the specified protocol matches this filter. Specify the protocol number. Listed below are some of the well-known protocols.

Number	**Name**
1	icmp
2	igmp
6	tcp
17	udp
89	ospf
112	`vrrp`

Command mode: config

Table 4-98 IP version 4 Filtering Configuration Commands

Command Syntax and Usage
`access-control list` *`<list-number>`* **`ipv4 type-of-service`** *`<tos>`* Defines a Type of Service value for the ACL. For more information on ToS, refer to RFC 1340 and 1349. **Command mode:** config
`default access-control list` *`<list-number>`* **`ipv4`** Resets the IPv4 parameters for the ACL to their default values. **Command mode:** config
`show access-control list` *`<list-number>`* **`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 4-99 TCP/UDP Filtering Configuration Commands

Command Syntax and Usage

`access-control list` *`<list-number>`* **`tcp-udp source-port`** *`<port>`*

Defines a source port for the ACL. If defined, traffic with the specified TCP or UDP source port will match this ACL. Specify the port number. Listed below are some of the well-known ports:

Number	Name
20	ftp-data
21	ftp
22	ssh
23	telnet
25	smtp
37	time
42	name
43	whois
53	domain
69	tftp
70	gopher
79	finger
80	http

Command mode: config

`access-control list` *`<list-number>`* **`tcp-udp destination-port`** *`<port>`*

Defines a destination port for the ACL. If defined, traffic with the specified TCP or UDP destination port will match this ACL. Specify the port number, just as with `sport` above.

Command mode: config

`access-control list` *`<list-number>`* **`tcp-udp flags`** *`<flag-value>`*

Defines a TCP/UDP flag for the ACL.

Command mode: config

`default access-control list` *`<list-number>`* **`tcp-udp`**

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

Command mode: config

`show access-control list` *`<list-number>`* **`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 4-100 Packet Format Filtering Configuration Commands

Command Syntax and Usage
access-control list *<list-number>* **packet-format ethernet {ether-type2|snap|llc}** Defines the Ethernet format for the ACL. **Command mode:** config
[no] access-control list *<list-number>* **packet-format tagged** Defines the tagging format for the ACL. **Command mode:** config
[no] access-control list *<list-number>* **packet-format ip {ipv4|ipv6}** Defines the IP format for the ACL. **Command mode:** config
default access-control list *<list-number>* **packet-format** Resets Packet Format parameters for the ACL to their default values. **Command mode:** config
show access-control list *<list-number>* **packet-format** 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 4-101 ACL Group Configuration Commands

Command Syntax and Usage
access-control group *<group-number>* **list** *<list number>* Adds the selected ACL to the ACL Group. **Command mode:** config

Table 4-101 ACL Group Configuration Commands

Command Syntax and Usage
`no access-control group` *`<group-number>`* **`list`** *`<list number>`* Removes the selected ACL from the ACL Group. **Command mode:** config
`show access-control group` *`<group-number>`* 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 4-102 ACL Metering Configuration Commands

Command Syntax and Usage
`access-control` *`<ACL-number>`* **`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:** config
`access-control` *`<ACL-number>`* **`meter committed-rate`** *`<rate-value>`* Configures the committed rate, in Kilobits per second. The committed rate must be a multiple of 64. **Command mode:** config
`access-control` *`<ACL-number>`* **`meter maximum-burst-size`** *`<size-value>`* 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:** config
`[no] access-control` *`<ACL-number>`* **`meter enable`** Enables or disables ACL Metering. **Command mode:** config
`access-control` *`<ACL-number>`* **`meter action {drop|pass}`** Configures the ACL Meter to either drop or pass out-of-profile traffic. **Command mode:** config
`show access-control list` *`<ACL-number>`* **`meter`** Displays current ACL Metering parameters. **Command mode:** Any

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 4-103 Re-Mark Configuration Commands

Command Syntax and Usage
`access-control list` *`<ACL-number>`* **`re-mark in-profile dscp`** *`<dscp-value>`* Sets the DiffServ Code Point (DSCP) of In-Profile packets to the selected value. **Command mode:** config
`show access-control list` *`<ACL-number>`* **`re-mark`** Displays current Re-Mark In-Profile parameters. **Command mode:** Any

Update User Priority Configuration

Table 4-104 User Priority Configuration Commands

Command Syntax and Usage
`access-control list` *`<ACL-number>`* **`re-mark in-profile dot1p`** *`<pri>`* Defines 802.1p value. The value is the priority bits information in the packet structure. **Command mode:** config
`[no] access-control list` *`<ACL-number>`* **`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:** config
`show access-control list` *`<ACL-number>`* **`re-mark`** Displays current Re-Mark In-Profile User Priority parameters. **Command mode:** Any

Re-Marking Out-of-Profile Configuration

Table 4-105 Out-of-Profile Configuration Commands

Command Syntax and Usage
`access-control list` *`<ACL-number>`* **`re-mark out-profile dscp`** *`<dscp-value>`* 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:** config
`show access-control list` *`<ACL-number>`* **`re-mark`** Displays current Re-Mark Out-of-Profile parameters. **Command mode:** Any

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 4-106 Port Mirroring Configuration Commands

Command Syntax and Usage
`[no] port-mirroring enable` Enables or disables port mirroring. **Command mode:** config
`show port-mirroring` Displays current settings of the mirrored and monitoring ports. **Command mode:** All except User EXEC

Port-Mirroring Configuration

Table 4-107 Port-Based Port-Mirroring Configuration Commands

Command Syntax and Usage

port-mirroring monitor-port *<port-instance>* **mirroring-port** *<port-identifier>* **{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: config

no port-mirroring monitor-port *<port-instance>* **mirroring-port** *<port-identifier>*

Removes the mirrored port.

Command mode: config

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 229.

`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 tftp
```

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 tftp`** 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 tftp running-config
```

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
`clear logging` Clears all Syslog messages. **Command Mode**: `Priv EXEC`
`ntp send` Allows the user to send requests to the NTP server. **Command Mode**: `Priv EXEC`

Operations-Level Port Options

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

Table 5-2 Port Operations Commands

Command Syntax and Usage
`no interface port` *`<port-identifier>`* **`shutdown`** Temporarily enables the port. The port will be returned to its configured operation mode when the switch is reset. **Command Mode**: `Priv EXEC`
`interface port` *`<port-identifier>`* **`shutdown`** Temporarily disables the port. The port will be returned to its configured operation mode when the switch is reset. **Command Mode**: `Priv EXEC`
`show interface port` *`<port-identifier>`* **`operation`** Displays the port interface operational state. **Command Mode**: `Priv EXEC`

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-identifier>`* **`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: `Priv EXEC`

`interface port` `{` *`<port-indentifier>`* `}` **`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: `Priv EXEC`

Operations-Level VRRP Options

Table 5-4 Virtual Router Redundancy Operations Commands

Command Syntax and Usage

`router vrrp backup` *`<router number>`*

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: `Priv EXEC`

Operations-Level BGP Options

Table 5-5 IP BGP Operations Commands

Command Syntax and Usage
`router bgp start` *`<peer number>`* Starts the peer session. **Command Mode**: `Priv EXEC`
`router bgp stop` *`<peer number>`* Stops the peer session. **Command Mode**: `Priv EXEC`
`show ip bgp state` Displays the current BGP operational state. **Command Mode**: `Priv 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 <time value>` Configures the switch reset time. **Command Mode**: `config`
`no boot schedule` Cancels the switch reset time. **Command Mode**: `config`
`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/pc/support`

Click on software updates. Use the **`show boot`** command to determine the current software version.

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>}
```

or

```
Router# copy ftp {<image1|image2|boot-image>}
```

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> or <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
```

or

```
Router# copy {<image1|image2|boot-image>} ftp
```

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> or <Enter>
```

5. **The system then requests confirmation of what you have entered. To have the file uploaded, enter Y.**

```
image2 currently contains Software Version 1.2.0
 that was downloaded at  0:23:39 Thu Jan  1, 2005.
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 reenter 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 NNCLI:

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

The default command-line interface for the GbESM is the Alteon OS CLI. To access the NNCLI, enter the following command and reset the GbESM:

```
Main# boot/mode nncli
```

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 249.
`copy flash-dump tftp` Saves the system dump information via TFTP. **Command mode:** All except User EXEC For details, see page 250.
`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 251.

`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 `xxxxxxxxxxxx` format (such as `080020123456`). **Command mode:** All except User EXEC
`show mac-address-table port {<port-identifier>}` Displays all FDB entries for a particular port. **Command mode:** All except User EXEC
`show mac-address-table vlan {<vlan-identifier>}` 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:** Any
`no mac-address-table <mac-address> [<vlan-instance>]` 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` Displays the Management Processor trace buffer. Header information similar to the following is shown: `MP trace buffer at 13:28:15 Fri May 25, 2001; mask: 0x2ffdf748` The buffer information is displayed after the header. **Command mode:** All except User EXEC
`debug mp-snap` Displays the Management Processor snap (or post-mortem) trace buffer. This buffer contains information traced at the time that a reset occurred. **Command mode:** All except User EXEC
`clear flash-config` Deletes all flash configuration blocks. **Command mode:** All except User EXEC

ARP Cache Maintenance

Table 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-instance>`* Shows ARP entries on a single port. **Command mode:** All except User EXEC
`show ip arp vlan` *`<vlan-instance>`* 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 63.

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|multicast}` Shows routes of a single type. **Command mode:** All except User EXEC For a description of IP routing types, see Table 2-23 on page 62
`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 2-24 on page 63
`show ip route interface` *`<interface-instance>`* 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 60.

IGMP Group Information

Table 7-7 describes the IGMP Snooping maintenance commands.

Table 7-7 IGMP Multicast Group Maintenance Commands

Command Syntax and Usage
`show ip igmp groups address` *<ip-address>* Displays a single IGMP multicast group by its IP address. **Command mode:** All except User EXEC
`show ip igmp groups vlan` *<vlan-instance>* Displays all IGMP multicast groups on a single VLAN. **Command mode:** All except User EXEC
`show ip igmp groups interface` *<port-instance>* Displays all IGMP multicast groups on a single port. **Command mode:** All except User EXEC
`show ip igmp groups trunk` *<trunk-id>* Displays all IGMP multicast groups on a single trunk group. **Command mode:** All except User EXEC
`show ip igmp groups` Displays information for all multicast groups. **Command mode:** All except User EXEC
`clear ip igmp snoop` Clears the IGMP group table. **Command mode:** All except User EXEC

Uuencode Flash Dump

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

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

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

NOTE – Dump information is not cleared automatically. In order for any subsequent dump information to be written to flash memory, you must manually clear the dump region. For more information on clearing the dump region, see page 251.

To access dump information, enter:

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

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

```
No FLASH dump available.
```

TFTP or FTP System Dump Put

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

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

To save dump information via TFTP, enter:

```
Router# copy flash-dump tftp <server> <filename>
```

Where *server* is the TFTP server IP address or hostname, and *filename* is the target dump file.

To save dump information via FTP, enter:

```
Router# copy flash-dump ftp <server> <filename>
```

Where *server* is the FTP server IP address or hostname, and *filename* is 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.
Booting complete  0:01:01 Thu Jul  1, 2006:
Version 1.2.0 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, 2006. 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