IBM System Networking RackSwitch G7028/G7052

ISCLI—Industry Standard CLI Command Reference

for IBM Networking OS 7.6

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

Second Edition (October 2014)

IBM Networking OS™ 7.6 ISCLI—Industry Standard CLI Command Reference for the RackSwitch G7028/G7052

Contents

Preface

The *IBM Networking OS™ 7.6 ISCLI—Industry Standard CLI Command Reference for the RackSwitch G7028/G7052* describes how to configure and use the IBM N/OS 7.6 software with your G7028/G7052. This guide lists each command, together with the complete syntax and a functional description, from the IS Command Line Interface (ISCLI).

Note: This *Command Reference* is applicable to G7028/G7052 product family. In some places “G7028” is used in examples. Unless explicitly mentioned, all commands and descriptions are applicable to both the G7028 and G7052.

For documentation on installing the switches physically, see the *Installation Guide* for your G7028/G7052. For details about configuration and operation of your G7028/G7052, see the *IBM N/OS 7.6 Application Guide*.

Who Should Use This Book

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

How This Book Is Organized

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

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

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

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

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

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

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

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

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

"Index" includes pointers to the description of the key words used throughout the book.

Typographic Conventions

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

Table 1. Typographic Conventions

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

Table 1. Typographic Conventions (continued)

Typeface or Symbol	Meaning
braces { }	Indicate required elements in syntax descriptions where there is more than one option. You must choose only one of the options. Do not type the braces when entering the command. Example: If the command syntax is `show portchannel {<1-16>|hash|information}` you enter: **show** `portchannel <1-16>` or show `portchannel` hash or show `portchannel` information

brackets [ ]	Indicate optional elements in syntax descriptions. Do not type the brackets when entering the command.
	
	Example: If the command syntax is
	`show interface ip` **[**`<1-4>`**]**
	
	you enter
	`show interface ip`
	
	or
	`show interface ip <1-4>`

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 `show portchannel {<1-16>|hash|information}` you must enter: **show** `portchannel <1-16>` or show `portchannel` hash or show `portchannel` information

How to Get Help

If you need help, service, or technical assistance, call IBM Technical Support:

US toll free calls: 1-800-414-5268

International calls: 1-408-834-7871

You also can visit our web site at the following address:

`http://www.ibm.com`

Click the **Support** tab.

The warranty card received with your product provides details for contacting a customer support representative. If you are unable to locate this information, please contact your reseller. Before you call, prepare the following information:

- Serial number of the switch unit
- Software release version number
- Brief description of the problem and the steps you have already taken
- Technical support dump information (`# show tech-support`)

Chapter 1. ISCLI Basics

Your G7028/G7052 is ready to perform basic switching functions right out of the box. Some of the more advanced features, however, require some administrative configuration before they can be used effectively.

This guide describes the individual ISCLI commands available for the G7028/G7052.

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

This chapter explains how to access the IS Command Line Interface (ISCLI) for the switch.

ISCLI Command Modes

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

- **User EXEC mode**

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

- **Privileged EXEC mode**

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

- **Global Configuration mode**

  This mode allows you to make changes to the running configuration. If you save the configuration, the settings survive a reload of the G7028/G7052. Several sub-modes can be accessed from the Global Configuration mode. For more details, see Table 2.

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

Table 2. lists the ISCLI command modes.

Table 2. ISCLI Command Modes

Command Mode/Prompt	Command used to enter or exit
User EXEC `RS G7028>`	Default mode, entered automatically on console Exit: `exit` or `logout`
Privileged EXEC `RS G7028#`	Enter Privileged EXEC mode, from User EXEC mode: `enable` Exit to User EXEC mode: `disable` Quit ISCLI: `exit` or `logout`
Global Configuration `RS G7028(config)#`	Enter Global Configuration mode, from Privileged EXEC mode: `configure terminal` Exit to Privileged EXEC: `end` or `exit`
Interface IP `RS G7028(config-ip-if)#`	Enter Interface IP Configuration mode, from Global Configuration mode: `interface ip` *<interface number>* Exit to Global Configuration mode: `exit` Exit to Privileged EXEC mode: `end`
Interface port `RS G7028(config-if)#`	Enter Port Configuration mode, from Global Configuration mode: `interface port` *<port number or alias>* Exit to Privileged EXEC mode: `exit` Exit to Global Configuration mode: `end`

Table 2. ISCLI Command Modes (continued)

Command Mode/Prompt	Command used to enter or exit
Interface PortChannel `RS G7028(config-PortChannel)#`	Enter PortChannel (trunk group) Configuration mode, from Global Configuration mode: `interface portchannel {<`*trunk number*`>|lacp <`*key*`>}` Exit to Privileged EXEC mode: `exit` Exit to Global Configuration mode: `end`
VLAN `RS G7028(config-vlan)#`	Enter VLAN Configuration mode, from Global Configuration mode: `vlan <`*VLAN number*`>` Exit to Global Configuration mode: `exit` Exit to Privileged EXEC mode: `end`

Global Commands

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

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

Table 3. Description of Global Commands

Command	Action
`?`	Provides more information about a specific command or lists commands available at the current level.
`list`	Lists the commands available at the current level.
`exit`	Go up one level in the command mode structure. If already at the top level, exit from the command line interface and log out.
`copy running-config startup-config`	Write configuration changes to non-volatile flash memory.
`logout`	Exit from the command line interface and log out.
`ping`	Use this command to verify station-to-station connectivity across the network. The format is as follows: `ping` *<host name>*`|`*<IP address>* `[-n` *<tries (0-4294967295)>*`]` `[-w` *<msec delay (0-4294967295)>*`]` `[-l` *<length (0/32-65500/2080)>*`]` `[-s` *<IP source>*`]` `[-v` *<tos (0-255)>*`]` `[-f]` `[-t]` `[-m|-mgt|-d|-data]` Where: – `-n`: Sets the number of attempts (optional). – `-w`: Sets the number of milliseconds between attempts (optional). – `-l`: Sets the ping request payload size (optional). – `-s`: Sets the IP source address for the IP packet (optional). – `-v`: Sets the Type Of Service bits in the IP header. – `-f`: Sets the *don't fragment* bit in the IP header (only for IPv4 addresses). – `-t`: Pings continuously (same as `-n 0`). By default, the `-m` or `-mgt` option for management port is used. To use data ports, specify the `-d` or `-data` option.

Table 3. Description of Global Commands

Command	Action
`traceroute`	Use this command to identify the route used for station-to-station connectivity across the network. The format is as follows: `traceroute` <*hostname*>|<*IP address*> [<*max-hops (1-32)*> [<*msec-delay (1-4294967295)*>]] `[-m|-mgt|-d|-data]` Where *hostname/IP address* is the hostname or IP address of the target station, *max-hops* (optional) is the maximum distance to trace (1-32 devices), and *msec-delay* (optional) is the number of milliseconds to wait for the response. By default, the `-m` or `-mgt` option for management port is used. To use data ports, specify the `-d` or `-data` option. As with `ping`, the DNS parameters must be configured if specifying hostnames.
`telnet`	This command is used to form a Telnet session between the switch and another network device. The format is as follows: `telnet {`<*hostname*>|<*IP address*>`}` [<*port*>] `[-m|-mgt|-d|-data]` Where *IP address* or *hostname* specifies the target station. Use of a hostname requires DNS parameters to be configured on the switch. *Port* is the logical Telnet port or service number. By default, the `-m` or `-mgt` option for management port is used. To use data ports, specify the `-d` or `-data` option.
`show history`	This command displays the last ten issued commands.
`show who`	Displays a list of users who are currently logged in.
`show line`	Displays a list of users who are currently logged in, in table format.

Command Line Interface Shortcuts

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

CLI List and Range Inputs

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

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

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

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

Do not use spaces within list and range specifications.

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

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

Command Abbreviation

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

```
RS G7028(config)# spanning-tree stp 2 bridge hello 2
```

or

```
RS G7028(config)# sp stp 2 br h 2
```

Tab Completion

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

If multiple commands share the typed characters, when you press <Tab>, the ISCLI completes the common part of the shared syntax.

User Access Levels

To enable better switch management and user accountability, three levels or *classes* of user access have been implemented on the G7028/G7052. 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 G7028/G7052. Users may display information that has no security or privacy implications, such as switch statistics and current operational state information.

- **oper**

  Operators can make temporary changes on the G7028/G7052. These changes are lost when the switch is rebooted/reset. Operators have access to the switch management features used for daily switch operations. Because any changes an operator makes are undone by a reset of the switch, operators cannot severely impact switch operation.

- **admin**

  Administrators are the only ones that may make permanent changes to the switch configuration—changes that are persistent across a reboot/reset of the switch. Administrators can access switch functions to configure and troubleshoot problems on the G7028/G7052. Because administrators can also make temporary (operator-level) changes as well, they must be aware of the interactions between temporary and permanent changes.

Access to switch functions is controlled through the use of unique surnames and passwords. Once you are connected to the switch via local Telnet, remote Telnet, or SSH, you are prompted to enter a password. The default user names/password for each access level are listed in the following table.

Note: It is recommended that you change default switch passwords after initial configuration and as regularly as required under your network security policies.

Table 4. User Access Levels

User Account	Description and Tasks Performed	Password
User	The User has no direct responsibility for switch management. He or she can view all switch status information and statistics, but cannot make any configuration changes to the switch.	`user`
Operator	The Operator can make temporary changes that are lost when the switch is rebooted/reset. Operators have access to the switch management features used for daily switch operations.	
Administrator	The superuser Administrator has complete access to all command modes, information, and configuration commands on the G7028/G7052, including the ability to change both the user and administrator passwords.	`admin`

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

Idle Timeout

By default, the switch will disconnect your Telnet session after ten minutes of inactivity. This function is controlled by the following command, which can be set from 1 to 60 minutes, or disabled when set to 0:

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

Command mode: Global Configuration

Chapter 2. Information Commands

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

Table 5. Information Commands

Command Syntax and Usage
`show interface status` *<port alias or number>* Displays configuration information about the selected port(s), including: – Port alias and number – Port speed – Duplex mode (half, full, or auto) – Flow control for transmit and receive (no, yes, or both) – Link status (up, down, or disabled) **Command mode:** All For details, see page 74.
`show interface trunk` *<port alias or number>* Displays port status information, including: – Port alias and number – Whether the port uses VLAN Tagging or not – Port VLAN ID (PVID) – Port name – VLAN membership – FDB Learning status – Flooding status For details, see page 74. **Command mode:** All
`show interface transceiver` Displays the status of the port transceiver module on each port. For details, see page 75. **Command mode:** All
`show information-dump` Dumps all switch information available (10K or more, depending on your configuration). If you want to capture dump data to a file, set your communication software on your workstation to capture session data prior to issuing the dump commands. **Command mode:** All

System Information

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

Table 6. System Information Options

Command Syntax and Usage
`show sys-info` Displays system information, including: – System date and time – Switch model name and number – Switch name and location – Time of last boot – MAC address of the switch management processor – IP address of management interface – Hardware version and part number – Software image file and version number – Configuration name – Log-in banner, if one is configured – Internal temperatures – Fan status – Power supply status For details, see page 33. **Command mode:** All
`show logging [severity <0-7>] [reverse]` Displays the current syslog configuration, followed by the most recent 2000 syslog messages, as displayed by the `show logging messages` command. For details, see page 34. **Command mode:** All
`show access user` Displays configured user names and their status. **Command mode:** All

CLI Display Information

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

Table 7. CLI Display Information Options

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

Error Disable and Recovery Information

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

Table 8. Error Disable Information Options

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

SNMPv3 System Information

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

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

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

Table 9. SNMPv3 Information Options

Command Syntax and Usage
`show snmp-server v3 user` Displays User Security Model (USM) table information. To view the table, see page 26. **Command mode:** All
`show snmp-server v3 view` Displays information about view, subtrees, mask and type of view. To view a sample, see page 27. **Command mode:** All
`show snmp-server v3 access` Displays View-based Access Control information. To view a sample, see page 28. **Command mode:** All
`show snmp-server v3 group` Displays information about the group, including the security model, user name, and group name. To view a sample, see page 29. **Command mode:** All
`show snmp-server v3 community` Displays information about the community table information. To view a sample, see page 29. **Command mode:** All
`show snmp-server v3 target-address` Displays the Target Address table information. To view a sample, see page 30. **Command mode:** All
`show snmp-server v3 target-parameters` Displays the Target parameters table information. To view a sample, see page 31. **Command mode:** All

Table 9. SNMPv3 Information Options (continued)

Command Syntax and Usage
`show snmp-server v3 notify` Displays the Notify table information. To view a sample, see page 31. **Command mode:** All
`show snmp-server v3` Displays all the SNMPv3 information. To view a sample, see page 32. **Command mode:** All

SNMPv3 USM User Table Information

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

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

Command mode: All

The USM user table contains the following information:

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

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

Table 10. USM User Table Information Parameters

Field	Description
User Name	A string representing the user name you can use to access the switch.
Protocol	Whether messages sent from this user are protected from disclosure using a privacy protocol. IBM N/OS supports DES algorithm for privacy and two authentication algorithms: MD5 and HMAC-SHA.

SNMPv3 View Table Information

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

The following command displays the SNMPv3 View Table:

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

Command mode: All

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

Table 11. SNMPv3 View Table Information Parameters

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

SNMPv3 Access Table Information

The access control subsystem provides authorization services.

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

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

The following command displays SNMPv3 access information:

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

Command mode: All

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

Table 12. SNMPv3 Access Table Information

Field	Description
Group Name	Displays the name of group.
Model	Displays the security model used, for example, SNMPv1, or SNMPv2 or USM.
Level	Displays the minimum level of security required to gain rights of access. For example, `noAuthNoPriv`, `authNoPriv`, or `authPriv`.
ReadV	Displays the MIB view to which this entry authorizes the read access.
WriteV	Displays the MIB view to which this entry authorizes the write access.
NotifyV	Displays the Notify view to which this entry authorizes the notify access.

SNMPv3 Group Table Information

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

The following command displays SNMPv3 group information:

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

Command mode: All

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

Table 13. SNMPv3 Group Table Information Parameters

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

SNMPv3 Community Table Information

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

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

Command mode: All

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

Table 14. SNMPv3 Community Table Information Parameters

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

SNMPv3 Target Address Table Information

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

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

Command mode: All

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

Table 15. SNMPv3 Target Address Table Information Parameters

Field	Description
Name	Displays the locally arbitrary, but unique identifier associated with this `snmpTargetAddrEntry`.
Transport Addr	Displays the transport addresses.
Port	Displays the SNMP UDP port number.
Taglist	This column contains a list of tag values which are used to select target addresses for a particular SNMP message.
Params	The value of this object identifies an entry in the `snmpTargetParamsTable`. The identified entry contains SNMP parameters to be used when generating messages to be sent to this transport address.

SNMPv3 Target Parameters Table Information

The following command displays SNMPv3 target parameters information:

```
show snmp-server v3 target-parameters
```

Command mode: All

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

Table 16. 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 the system does not support.
Sec Level	Displays the level of security used when generating SNMP messages using this entry.

SNMPv3 Notify Table Information

The following command displays the SNMPv3 Notify Table:

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

Command mode: All

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

Table 17. SNMPv3 Notify Table Information

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

SNMPv3 Dump Information

The following command displays SNMPv3 information:

```
show snmp-server v3
```

Command mode: All

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

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

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

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

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

snmpNotify Table:
Name                 Tag
-------------------- --------------------

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

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

General System Information

The following command displays system information:

```
show sys-info
```

Command mode: All

```
System Information at 12:58:43 Thu Nov 21, 2013
Time zone: No timezone configured
Daylight Savings Time Status: Disabled

IBM Networking Operating System RackSwitch G7028

Switch has been up for 0 days, 0 hours, 1 minute and 52 seconds.
Last boot: 12:57:21 Thu Nov 21, 2013 (reset from console)

MAC address: 00:00:01:02:03:04    IP (If 1) address: 192.168.49.50
Management Port MAC Address: 00:00:01:02:03:fe
Management Port IP Address (if 4): 192.168.50.50
Hardware Part No: 00D9853
Switch Serial No: Y030PZ23H00E
Manufacturing date: 12/11

MTM Value: 1455-24L
ESN: 1000001

Software Version 7.6.1 (FLASH image1), active configuration.


Temperature MAC        : 31 C, Threshold:60 C
Temperature 10G PHY    : 31 C, Threshold:63 C
Temperature CPU        : 26 C, Threshold:55 C
Temperature Air Inlet  : 24 C, Threshold:53 C
Temperature 1G PHY     : 31 C, Threshold:54 C
Temperature Air Outlet : 31 C, Threshold:56 C

Fan 1 : RPM=9000 PWM=100% Back-To-Front [J]
Fan 2 : RPM=9000 PWM=100% Back-To-Front [J]
Fan 3 : RPM=9000 PWM=100% Back-To-Front [J]

Internal  Power Supply: On
Redundant Power Supply: Not Installed

  Power Faults: ()
    Fan Faults: ()
Service Faults: ()
```

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

System information includes:

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

Show Specific System Information

Table 18 lists commands used for displaying specific entries from the general system information screen

Table 18. Specific System Information Options

Command Syntax and Usage
`show environment fan` Displays information about internal temperatures and fan status. **Command mode:** All
`show environment power` Displays information about power supply status. **Command mode:** All
`show version brief` Displays the software version number, image file, and configuration name. **Command mode:** All

Show Recent Syslog Messages

The following command displays system log messages:

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

Command mode: All

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

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

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

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

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

User Status

The following command displays user status information:

```
show access user
```

Command mode: All except User EXEC

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

This command displays the status of the configured usernames.

Layer 2 Information

Table 19. Layer 2 Information Commands

Command Syntax and Usage
`show vlag information` Displays vLAG Information. For details, see page 52. Command mode: All
`show dot1x information` Displays 802.1X Information. For details, see page 39. **Command mode:** All
`show spanning-tree` Displays Spanning Tree information, including the status (on or off), Spanning Tree mode (RSTP, PVRST, or MSTP), and VLAN membership. In addition to seeing if STG is enabled or disabled, you can view the following STG bridge information: – Priority – Hello interval – Maximum age value – Forwarding delay – Aging time You can also see the following port-specific STG information: – Port alias and priority – Cost – State **Command mode:** All
`show spanning-tree root` Displays the root bridge ID for every spanning-tree instance and the path cost associated with it. **Command mode:** All For details, see page 55.
`show spanning-tree blockedports` Lists the ports blocked by each STP instance. **Command mode:** All
`show spanning-tree stp` *<1-128>* `information` Displays information about a specific Spanning Tree Group. **Command mode:** All For details, see page 53.

Table 19. Layer 2 Information Commands (continued)

Command Syntax and Usage
`show spanning-tree mst <0-32> information` Displays Spanning Tree information for the specified instance. A value of 0 indicates CIST. CIST bridge information includes: – Priority – Hello interval – Maximum age value – Forwarding delay – Root bridge information (priority, MAC address, path cost, root port) CIST port information includes: – Port number and priority – Cost – State For details, see page 56. **Command mode:** All
`show spanning-tree mst configuration` Displays the current MSTP settings. **Command mode:** All
`show portchannel information` Displays the state of each port in the various trunk groups. For details, see page 59. **Command mode:** All
`show vlan` Displays VLAN configuration information for all configured VLANs, including: – VLAN Number – VLAN Name – Status – Port membership of the VLAN For details, see page 59. **Command mode:** All
`show failover trigger <trigger number> information` Displays Layer 2 Failover information. For details, see page 45. **Command mode:** All
`show hotlinks information` Displays Hot Links information. For details, see page 47. **Command mode:** All

Table 19. Layer 2 Information Commands (continued)

Command Syntax and Usage
`show lldp information` Displays Link Layer Discovery Protocol (LLDP) information. For details, see page 47. **Command mode:** All
`show layer2 information` Dumps all Layer 2 switch information available (10K or more, depending on your configuration). If you want to capture dump data to a file, set your communication software on your workstation to capture session data prior to issuing the dump commands. **Command mode:** All

802.1X Information

The following command displays 802.1X information:

```
show dot1x information
```

Command mode: All

```
System capability : Authenticator
System status : disabled
Protocol version : 1
Guest VLAN status : disabled
Guest VLAN : none
Authenticator Backend Assigned
Port Auth Mode Auth Status PAE State Auth State VLAN
----- ------------ ------------ -------------- ---------- --------
*1 force-auth unauthorized initialize initialize none
*2 force-auth unauthorized initialize initialize none
*3 force-auth unauthorized initialize initialize none
```

The following table describes the IEEE 802.1X parameters.

Table 20. 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

Table 20. 802.1X Parameter Descriptions (continued)

Parameter	Description
Backend Auth State	Displays the Backend Authorization State. The Backend Authorization state can be one of the following: – initialize – request – response – success – fail – timeout – idle
Assigned VLAN	Displays the corresponding VLAN associated with the port.

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 8K MAC address entries on the MP per switch.

Table 21. FDB Information Options

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

Table 21. FDB Information Options (continued)

Command Syntax and Usage
`show mac-address-table counters` Displays all forwarding database statistics. **Command mode:** All
`show mac-address-table` Displays all unicast and multicast entries in the Forwarding Database. **Command mode:** All

FDB Multicast Information

The following commands display FDB multicast information.

Table 22. Multicast FDB Information Options

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

Show All FDB Information

The following command displays Forwarding Database information:

`show mac-address-table`

Command mode: All

```
     MAC address     VLAN  Port  Trnk  State  Permanent
-----------------  ----  ----  ----  -----  ---------
00:04:38:90:54:18     1  4            FWD
00:09:6b:9b:01:5f     1  13           FWD
00:11:43:c4:79:83     1  4            FWD       P
```

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

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

Clearing Entries from the Forwarding Database

To clear the entire FDB, refer to “Forwarding Database Maintenance” on page 267.

Link Aggregation Control Protocol Information

Use these commands to display LACP status information about each port on the G7028/G7052.

Table 23. LACP Information Options

Command Syntax and Usage
`show lacp aggregator` *<aggregator ID>* Displays detailed information about the LACP aggregator. **Command mode:** All
`show interface port` *<port alias or number>* `lacp information` Displays LACP information about the selected port. **Command mode:** All
`show lacp information` Displays a summary of LACP information. For details, see page 44. **Command mode:** All
`show lacp information state {down|off|up}` Displays a summary of LACP information for the interfaces that are down, off, or up. **Command mode:** All

Link Aggregation Control Protocol

The following command displays LACP information:

```
show lacp information
```

Command mode: All

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

LACP dump includes the following information for each port in the G7028/G7052:

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

- `trunk` This value represents the LACP trunk group number.
- `status` Displays the status of LACP on the port (up, down or standby).
- `minlinks` Displays the minimum number of active links in the LACP trunk.

Layer 2 Failover Information

Table 24. Layer 2 Failover Information Options

Command Syntax and Usage
`show failover trigger` <*trigger number*> `information` Displays detailed information about the selected Layer 2 Failover trigger. **Command mode:** All
`show failover trigger information` Displays a summary of Layer 2 Failover information. For details, see page 45. **Command mode:** All

Layer 2 Failover Information

The following command displays Layer 2 Failover information:

`show failover trigger information`

Command mode: All

```
Failover: On

Trigger 1 Manual Monitor: Enabled
Trigger 1 limit: 0
Monitor State: Up
Member      Status
---------   -----------
 17         Operational
Control State: Auto Controlled
Member      Status
---------   -----------
Physical ports
 1          Operational

Trigger 2: Disabled

Trigger 3: Disabled

Trigger 4: Disabled

Trigger 5: Disabled

Trigger 6: Disabled

Trigger 7: Disabled

Trigger 8: Disabled
```

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

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

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

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

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

Hot Links Information

The following command displays Hot Links information:

```
show hotlinks information
```

Command mode: All

```
Hot Links Info: Trigger

Current global Hot Links setting: ON
bpdu disabled
sndfdb disabled

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

Active state: None

Master settings:
port 1
Backup settings:
port 2
```

Hot Links information includes the following:

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

LLDP Information

The following commands display LLDP information.

Table 25. LLDP Information Options

Command Syntax and Usage
`show lldp transmit` Displays information about the LLDP transmit state machine. **Command mode:** All
`show lldp receive` Displays information about the LLDP receive state machine. **Command mode:** All
`show lldp remote-device [<1-256>|detail]` Displays information received from LLDP-capable devices. For more information, see page 48. **Command mode:** All

Table 25. LLDP Information Options

Command Syntax and Usage
`show lldp remote-device port` *<port number>* Displays information received from LLDP-capable devices for a specific port. A given list of ports needs to be delimited by ',' and a range of ports delimited by '-'. **Command mode:** All
`show lldp information` Displays all LLDP information. **Command mode:** All

LLDP Remote Device Information

The following command displays LLDP remote device information:

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

Command mode: All

```
LLDP Remote Devices Information
Legend(possible values in DMAC column) :
NB   - Nearest Bridge          - 01-80-C2-00-00-0E
NnTB - Nearest non-TPMR Bridge - 01-80-C2-00-00-03
NCB  - Nearest Customer Bridge - 01-80-C2-00-00-00
Total number of current entries: 9
LocalPort | Index | Remote Chassis ID   | Remote Port  | Remote System Name  | DMAC
----------|-------|---------------------|--------------|---------------------|------
XGE2      | 1     | 34 40 b5 6d ce 00   | 17           |                     | NB
1         | 2     | 00 00 00 00 11 00   | 30           |                     | NB
XGE4      | 3     | 00 e0 00 01 00 00   | 62           |                     | NB
```

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

```
Local Port Alias: 1
        Remote Device Index     : 15
        Remote Device TTL       : 99
        Remote Device RxChanges : false
        Chassis Type            : Mac Address
        Chassis Id              : 00-18-b1-33-1d-00
        Port Type               : Locally Assigned
        Port Id                 : 23
        Port Description        : 23

        System Name        :
        System Description : IBM Networking Operating System RackSwitch G7028, IBM
Networking OS: version 7.6.0,13 Boot image: version 7.6.0.13
        System Capabilities Supported : bridge, router
        System Capabilities Enabled   : bridge, router

        Remote Management Address:
                Subtype             : IPv4
                Address             : 10.100.120.181
                Interface Subtype   : ifIndex
                Interface Number    : 128
                Object Identifier   :
```

Unidirectional Link Detection Information

Table 26. UDLD Information Options

Command Syntax and Usage
`show interface port` <*port alias or number*> `udld` Displays UDLD information about the selected port. **Command mode:** All
`show udld` Displays all UDLD information. **Command mode:** All

UDLD Port Information

The following command displays UDLD information for the selected port:

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

Command mode: All

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

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

UDLD information includes the following:

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

802.1x Discovery Information

Table 27. 802.1x Discovery Information Options

Command Syntax and Usage
`show interface port` <*port alias or number*> `dot1x` Displays 802.1x information about the selected port. **Command mode:** All
`show dot1x` Displays all 802.1x information. **Command mode:** All

802.1x Port Information

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

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

Command mode: All

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

vLAG Information

Table 28. vLAG Information Options

Command Syntax and Usage
`show vlag adminkey` *<1-65535>* Displays vLAG LACP information. **Command mode:** All
`show vlag portchannel` *<trunk group number>* Displays vLAG static trunk group information. **Command mode:** All
`show vlag isl` Displays vLAG Inter-Switch Link (ISL) information. **Command mode:** All
`show vlag information` Displays all vLAG information. **Command mode:** All

vLAG Trunk Information

The following command displays vLAG information for the trunk group:

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

Command mode: All

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

Spanning Tree Information

The following command displays Spanning Tree information:

`show spanning-tree stp <1-128> information`

Command mode: All

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

Current Root:            Path-Cost  Port Hello MaxAge FwdDel
 8000 00:25:03:49:29:00        0       0    2     20     15

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

   Port    Prio   Cost     State  Role Designated Bridge      Des Port     Type
---------- ---- ---------- -----  ---- ---------------------- -------- ------------
1    (pc12)  128      490!+  FWD   DESG 8000-00:25:03:49:29:00     8026 P2P
2    (pc12)  128      490!+  FWD   DESG 8000-00:25:03:49:29:00     8026 P2P
3    (pc12)  128      490!+  FWD   DESG 8000-00:25:03:49:29:00     8026 P2P
4    (pc12)  128      490!+  FWD   DESG 8000-00:25:03:49:29:00     8026 P2P
MGT           0        0    FWD *
* = STP turned off for this port.
! = Automatic path cost.
+ = Portchannel cost, not the individual port cost.
```

The switch software uses the Per VLAN Rapid Spanning Tree Protocol (PVRST) spanning tree mode, with IEEE 802.1w Rapid Spanning Tree Protocol (RSTP) or IEEE 802.1s Multiple Spanning Tree Protocol (MSTP), as alternatives.

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

Table 29. PVRST/RSTP/MSTP Bridge Parameter Descriptions

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

Table 29. PVRST/RSTP/MSTP Bridge Parameter Descriptions (continued)

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

The following port-specific information is also displayed:

Table 30. PVRST/RSTP/MSTP Port Parameter Descriptions

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

Spanning Tree Bridge Information

The following command displays Spanning Tree bridge information:

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

Command mode: All

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

Table 31. Bridge Parameter Descriptions

Parameter	Description
VLAN	VLANs that are part of the Spanning Tree Group
Priority	The bridge priority parameter controls which bridge on the network will become the STP root bridge. The lower the value, the higher the priority.
Hello	The hello time parameter specifies, in seconds, how often the root bridge transmits a configuration bridge protocol data unit (BPDU). Any bridge that is not the root bridge uses the root bridge hello value.
MaxAge	The maximum age parameter specifies, in seconds, the maximum time the bridge waits without receiving a configuration bridge protocol data unit before it reconfigures the STP network.
FwdDel	The forward delay parameter specifies, in seconds, the amount of time that a bridge port has to wait before it changes from learning state to forwarding state.
Protocol	The STP protocol run by the Spanning Tree Group

Spanning Tree Root Information

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

```
show spanning-tree root
```

Command mode: All

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

Table 32. Bridge Parameter Descriptions

Parameter	Description
Instance	Spanning Tree instance
Root ID	Indicates the root switch MAC address and port number.
Path-Cost	The port path cost is used to help determine the designated port for a segment. Port path cost is based on the port speed.
Hello	The hello time parameter specifies, in seconds, how often the root bridge transmits a configuration bridge protocol data unit (BPDU). Any bridge that is not the root bridge uses the root bridge hello value.

Table 32. Bridge Parameter Descriptions (continued)

Parameter	Description
MaxAge	The maximum age parameter specifies, in seconds, the maximum time the bridge waits without receiving a configuration bridge protocol data unit before it reconfigure the STP network.
FwdDel	The forward delay parameter specifies, in seconds, the amount of time that a bridge port has to wait before it changes from learning state to forwarding state.
Root Port	Port number allocated to the STP instance on the root switch.

Multiple Spanning Tree Information

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

`show spanning-tree mst <0-32> information`

Command mode: All

```
Mstp Digest: 0xac36177f50283cd4b83821d8ab26de62

Common Internal Spanning Tree:

VLANs MAPPED:  1-4094
VLANs:  1 2 4095

Current Root:            Path-Cost  Port MaxAge FwdDel
 8000 00:11:58:ae:39:00      2026     0     20     15

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

Parameters:  Priority  MaxAge  FwdDel  Hops
              32768      20      15    20

Port  Prio  Cost     State  Role Designated Bridge      Des Port Hello Type
----- ---- --------- -----  ---- ---------------------- -------- ----- ----
1     128     2000!  FWD  ROOT fffe-00:13:0a:4f:7d:d0    8011   2   P2P#
23    128     2000!  DISC ALTN fffe-00:22:00:24:46:00    8012   2   P2P#
MGT     0        0   FWD *

* = STP turned off for this port.
! = Automatic path cost.
# = PVST Protection enabled for this port.
```

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

Table 33. CIST Parameter Descriptions

Parameter	Description
CIST Root	The CIST Root shows information about the root bridge for the Common Internal Spanning Tree (CIST). Values on this row of information refer to the CIST root.
CIST Regional Root	The CIST Regional Root shows information about the root bridge for this MSTP region. Values on this row of information refer to the regional root.
Priority (bridge)	The bridge priority parameter controls which bridge on the network will become the STP root bridge.
Hello	The hello time parameter specifies, in seconds, how often the root bridge transmits a configuration bridge protocol data unit (BPDU). Any bridge that is not the root bridge uses the root bridge hello value.
MaxAge	The maximum age parameter specifies, in seconds, the maximum time the bridge waits without receiving a configuration bridge protocol data unit before it reconfigure the STP network.
FwdDel	The forward delay parameter specifies, in seconds, the amount of time that a bridge port has to wait before it changes from learning state to forwarding state.
Hops	The maximum number of bridge hops a packet can traverse before it is dropped. The default value is 20.

The following port-specific CIST information is also displayed:

Table 34. CIST Parameter Descriptions

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

Table 34. CIST Parameter Descriptions (continued)

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

Trunk Group Information

The following command displays Trunk Group information:

`show portchannel information`

Command mode: All

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

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

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

VLAN Information

Table 35. VLAN Information Options

Command Syntax and Usage
`show vlan` *<VLAN number>* Displays general VLAN information. **Command mode:** All
`show protocol-vlan` *<protocol number (1-8)>* Displays Protocol VLAN information. **Command mode:** All
`show vlan private-vlan` – Displays Private VLAN information. **Command mode:** All s
`show vlan information` Displays information about all VLANs, including: – VLAN number and name – Port membership – VLAN status (enabled or disabled) – Protocol VLAN status – Private VLAN status – Spanning Tree membership **Command mode:** All

The following command displays VLAN information:

```
show vlan
```

Command mode: All

```
VLAN               Name                Status          Ports
----  --------------------------------  ------ -------------------------
1     Default VLAN                       ena   1-20
2     VLAN 2                             dis   21-22
100   VLAN 100                           ena   empty
200   VLAN 200                           ena   empty
300   VLAN 300                           ena   empty
4095  Mgmt VLAN                          ena   MGT

Primary       Secondary    Type           Ports
------------  ------------ --------- ---------------
100           200          isolated  14
100           300          community 12
```

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

VLAN information includes:

- VLAN Number
- VLAN Name
- Status
- Port membership of the VLAN
- Protocol VLAN information (if available)
- Private VLAN information (if available)

Layer 3 Information

Table 36. Layer 3 Information Commands

Command Syntax and Usage
`show ip igmp groups` Displays IGMP Information. For more IGMP information options, see page 61. **Command mode**: All
`show interface ip` Displays IP interface Information. For details, see page 65. **Command mode:** All
`show ip interface brief` Displays IP Information. For details, see page 66. IP information, includes: – IP interface information: Interface number, IP address, subnet mask, VLAN number, and operational status. – Default gateway information: Metric for selecting which configured gateway to use, gateway number, IP address, and health status – IP forwarding settings, network filter settings **Command mode:** All
`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 before issuing the dump commands. **Command mode:** All

IGMP Multicast Group Information

Table 37. IGMP Multicast Group Information Commands

Command Syntax and Usage
`show ip igmp querier vlan` *<VLAN number>* Displays IGMP Querier information. For details, see page 63. **Command mode:** All
`show ip igmp snoop` Displays IGMP Snooping information. **Command mode:** All

Table 37. IGMP Multicast Group Information Commands (continued)

Command Syntax and Usage
`show ip igmp mrouter information` Displays IGMP Multicast Router information. For details, see page 63. **Command mode:** All
`show ip igmp mrouter vlan` *<VLAN number>* Displays IGMP Multicast Router information for the specified VLAN. **Command mode:** All
`show ip igmp filtering` Displays current IGMP Filtering parameters. **Command mode:** All
`show ip igmp profile` *<1-16>* Displays information about the current IGMP filter. **Command mode:** All
`show ip igmp groups address` *<IP address>* Displays a single IGMP multicast group by its IP address. **Command mode:** All
`show ip igmp groups vlan` *<VLAN number>* Displays all IGMP multicast groups on a single VLAN. **Command mode:** All
`show ip igmp groups interface port` *<port alias or number>* Displays all IGMP multicast groups on a single port. **Command mode:** All
`show ip igmp groups portchannel` *<trunk number>* Displays all IGMP multicast groups on a single trunk group. **Command mode:** All
`show ip igmp groups detail` *<IP address>* Displays details about an IGMP multicast group, including source and timer information. **Command mode:** All
`show ip igmp groups` Displays information for all multicast groups. For details, see page 64. **Command mode:** All
`show ip igmp ipmcgrp` Displays information for all IPMC groups. For details, see page 65. **Command mode:** All

Table 37. IGMP Multicast Group Information Commands (continued)

Command Syntax and Usage
`show ip igmp counters` Displays IGMP counters for all VLANs. **Command mode:** All
`show ip igmp vlan <VLAN number> counter` Displays IGMP counters for a specific VLAN. **Command mode:** All

IGMP Querier Information

The following command displays IGMP Querier information:

`show ip igmp querier vlan <VLAN number>`

Command mode: All

```
Current IGMP Querier information:
 IGMP Querier information for vlan 1:
 Other IGMP querier - none
 Switch-querier enabled, current state: Querier
 Switch-querier type: Ipv4, address 1.1.1.1,
 Switch-querier general query interval: 125 secs,
 Switch-querier max-response interval: 100 'tenths of secs',
 Switch-querier startup interval: 31 secs, count: 2
 Switch-querier robustness: 2
 IGMP configured version is v3
 IGMP Operating version is v3
```

IGMP Querier information includes:

- VLAN number
- Querier status
  - Other IGMP querier—none
  - IGMP querier present, address: (IP or MAC address)
    Other IGMP querier present, interval (minutes:seconds)
- Querier election type (IPv4 or MAC) and address
- Query interval
- Querier startup interval
- Maximum query response interval
- Querier robustness value
- IGMP version number

IGMP Group Information

The following command displays IGMP Group information:

```
show ip igmp groups
```

Command mode: All

```
Total entries: 5  Total IGMP groups: 3
Note: The <Total IGMP groups> number is computed as
      the number of unique (Group, Vlan) entries!
Note: Local groups (224.0.0.x) are not snooped/relayed and will not appear.
     Source         Group       VLAN    Port   Version   Mode  Expires  Fwd
 -------------- --------------- ------- ------ --------  ----- -------  ---
 10.1.1.1       232.1.1.1        2      4       V3       INC    4:16    Yes
 10.1.1.5       232.1.1.1        2      4       V3       INC    4:16    Yes
    *           232.1.1.1        2      4       V3       INC     -      No
 10.10.10.43    235.0.0.1        9      1       V3       INC    2:26    Yes
    *           236.0.0.1        9      1       V3       EXC     -      Yes
```

IGMP Group information includes:

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

IGMP Multicast Router Information

The following command displays Mrouter information:

```
show ip igmp mrouter information
```

Command mode: All

```
Total entries: 3 Total number of dynamic mrouters: 2
Total number of installed static mrouters: 1
SrcIP               VLAN    Port       Version   Expires   MRT       QRV   QQIC

------------------- ------- -------    --------- --------  -------   ----  ----
10.1.1.1             2       21         V3        4:09     128        2     125
10.1.1.5             2       23         V2        4:09     125        -       -
*                    9       24         V2       static              -       -
```

IGMP Mrouter information includes:

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

- Querier's Query Interval Code (QQIC)

IPMC Group Information

The following command displays IGMP IPMC group information:

```
show ip igmp ipmcgrp
```

Command mode: All

```
Total number of displayed ipmc groups: 4
Legend(possible values in Type column) :
SH - static host      DR - dynamic registered
SP - static primary   DU - dynamic unregistered
SB - static backup     M - mrouter
 O - other
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
     Source          Group      Vlan    Port      Type          Timeleft
============== =============== ==== ============ = ============ ==========
       *           232.0.0.1     1      -         DU            6 sec
       *           232.0.0.2     1      -         DU            6 sec
       *           232.0.0.3     1      -         DU            6 sec
       *           232.0.0.4     1      -         DU            6 sec
```

IGMP IPMC Group information includes:

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

Interface Information

The following command displays interface information:

```
show interface ip
```

Command mode: All

```
Interface information:
  1: IP4 192.168.49.50   255.255.255.0   192.168.49.255,  vlan 1,    DOWN
  3: IP6 2001:0:0:0:0:0:0:2/64                          , vlan 4095, up
         fe80::200:1ff:fe02:300
  4: IP4 192.168.50.50   255.255.255.0   192.168.50.255,  vlan 4095, up
```

For each interface, the following information is displayed:

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

IP Information

The following command displays Layer 3 information:

`show ip interface brief`

Command mode: All

```
IP information:
Flood unregistered IPMC: ena

Interface information:
  1: IP4 192.168.49.50   255.255.255.0   192.168.49.255,  vlan 1,    DOWN
  3: IP6 2001:0:0:0:0:0:0:2/64                          , vlan 4095, up
         fe80::200:1ff:fe02:300
  4: IP4 192.168.50.50   255.255.255.0   192.168.50.255,  vlan 4095, up


Default gateway information: metric strict

Default IP6 gateway information:
```

IP information includes:

- IP interface information: Interface number, IP address, subnet mask, broadcast address, VLAN number, and operational status.
- Default gateway information: Metric for selecting which configured gateway to use, gateway number, IP address, and health status

Quality of Service Information

Table 38. QoS information Options

Command Syntax and Usage
`show qos transmit-queue` Displays mapping of 802.1p value to Class of Service queue number, and COS queue weight value. **Command mode:** All
`show qos transmit-queue information` Displays all 802.1p information. **Command mode:** All For details, see page 67.
`show qos random-detect` Displays WRED and ECN information. **Command mode:** All For details, see page 68.

802.1p Information

The following command displays 802.1p information:

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

Command mode: All

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

Current port priority information:
Port   Priority  COSq  Weight
-----  --------  ----  ------
1           0       0      1
2           0       0      1
3           0       0      1
4           0       0      1
5           0       0      1
6           0       0      1
7           0       0      1
8           0       0      1
9           0       0      1
10          0       0      1
...
```

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

Table 39. 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 40. 802.1p Port Priority Parameter Descriptions

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

WRED and ECN Information

The following command displays WRED and ECN information:

```
show qos random-detect
```

Command mode: All

```
Current wred and ecn configuration:
Global ECN:  Disable
Global WRED: Disable

--WRED--TcpMinThr--TcpMaxThr--TcpDrate--NonTcpMinThr--NonTcpMaxThr--NonTcpDrate--
        TQ0:   Dis       0          0          0          0             0
0
        TQ1:   Dis       0          0          0          0             0
0
        TQ2:   Dis       0          0          0          0             0
0
        TQ3:   Dis       0          0          0          0             0
0
        TQ4:   Dis       0          0          0          0             0
0
        TQ5:   Dis       0          0          0          0             0
0
        TQ6:   Dis       0          0          0          0             0
0
        TQ7:   Dis       0          0          0          0             0
0
```

Access Control List Information Commands

Table 41. ACL Information Options

Command Syntax and Usage
`show access-control list` *<ACL number>* Displays ACL list information. For details, see page 69. **Command mode:** All
`show access-control list6` *<ACL number>* Displays IPv6 ACL list information. **Command mode:** All
`show access-control group` *<ACL group number>* Displays ACL group information. **Command mode:** All

Access Control List Information

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

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

Command mode: All

```
Current ACL List information:
-----------------------
Filter 1 profile:
   Ethernet
     - SMAC       : 00:00:aa:aa:01:fe/ff:ff:ff:ff:ff:ff
     - DMAC       : 00:0d:60:9c:ec:d5/ff:ff:ff:ff:ff:ff
     - VID        : 10/0xfff
     - Ethertype  : IP (0x0800)
     - Priority   : 3
   Meter
     - Set to disabled
     - Set committed rate : 64
     - Set max burst size : 32
   Re-Mark
     - Set use of TOS precedence to disabled
   Packet Format
     - Ethernet format : None
     - Tagging format  : Any
     - IP format       : None
   Actions        : Deny
   Statistics   : enabled

Mirror Target Configuration:
        Mirror target destination: port
        Egress port for mirror target: 4
```

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

Table 42. ACL List Parameter Descriptions

Parameter	Description
Filter x profile	Indicates the ACL number.
Ethernet	Displays the ACL Ethernet header parameters, if configured.
IPv4	Displays the ACL IPv4 header parameters, if configured.
TCP/UDP	Displays the ACL TCP/UDP header parameters, if configured.
Meter	Displays the ACL meter parameters.
Re-Mark	Displays the ACL re-mark parameters.
Packet Format	Displays the ACL Packet Format parameters, if configured.
Actions	Displays the configured action for the ACL.
Statistics	Displays status of ACL statistics (enabled or disabled).

Table 42. ACL List Parameter Descriptions

Parameter	Description
Mirror Target Configuration	Displays ACL port mirroring parameters.
Filter x profile	Indicates the ACL number.

RMON Information Commands

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

Table 43. RMON Information Options

Command Syntax and Usage
`show rmon history` Displays RMON History information. For details, see page 71. **Command mode:** All
`show rmon alarm` Displays RMON Alarm information. For details, see page 72. **Command mode:** All
`show rmon event` Displays RMON Event information. For details, see page 73. **Command mode:** All
`show rmon` Displays all RMON information. **Command mode:** All

RMON History Information

The following command displays RMON History information:

```
show rmon history
```

Command mode: All

```
RMON History group configuration:

Index IFOID                          Interval Rbnum Gbnum
----- ------------------------------ -------- ----- -----
   1  1.3.6.1.2.1.2.2.1.1.24               30     5     5
   2  1.3.6.1.2.1.2.2.1.1.22               30     5     5
   3  1.3.6.1.2.1.2.2.1.1.20               30     5     5
   4  1.3.6.1.2.1.2.2.1.1.19               30     5     5
   5  1.3.6.1.2.1.2.2.1.1.24             1800     5     5

Index                      Owner
-----  -------------------------------------------
    1  dan
```

The following table describes the RMON History Information parameters.

Table 44. RMON History Parameter Descriptions

Parameter	Description
Index	Displays the index number that identifies each history instance.
IFOID	Displays the MIB Object Identifier.
Interval	Displays the time interval for each sampling bucket.
Rbnum	Displays the number of requested buckets, which is the number of data slots into which data is to be saved.
Gbnum	Displays the number of granted buckets that may hold sampled data.
Owner	Displays the owner of the history instance.

RMON Alarm Information

The following command displays RMON alarm information:

```
show rmon alarm
```

Command mode: All

```
RMON Alarm group configuration:

Index  Interval  Sample   Type      rLimit       fLimit     last value
-----  --------  ------  -------  -----------  -----------  ----------
    1      1800     abs   either            0            0       7822

Index  rEvtIdx  fEvtIdx                    OID
-----  -------  -------  ----------------------------------------
    1        0        0  1.3.6.1.2.1.2.2.1.10.1

Index                        Owner
-----  ------------------------------------------
    1  dan
```

The following table describes the RMON Alarm Information parameters.

Table 45. RMON Alarm Parameter Descriptions

Parameter	Description
Index	Displays the index number that identifies each alarm instance.
Interval	Displays the time interval over which data is sampled and compared with the rising and falling thresholds.
Sample	Displays the method of sampling the selected variable and calculating the value to be compared against the thresholds, as follows: – `abs`–absolute value, the value of the selected variable is compared directly with the thresholds at the end of the sampling interval. – `delta`–delta value, the value of the selected variable at the last sample is subtracted from the current value, and the difference compared with the thresholds.
Type	Displays the type of alarm, as follows: – `falling`–alarm is triggered when a falling threshold is crossed. – `rising`–alarm is triggered when a rising threshold is crossed. – `either`–alarm is triggered when either a rising or falling threshold is crossed.
rLimit	Displays the rising threshold for the sampled statistic.
fLimit	Displays the falling threshold for the sampled statistic.
Last value	Displays the last sampled value.

Table 45. RMON Alarm Parameter Descriptions (continued)

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

RMON Event Information

The following command displays RMON event information:

```
show rmon event
```

Command mode: All

```
RMON Event group configuration:

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

Index                       Owner
-----  -----------------------------------------------
    1  dan
```

The following table describes the RMON Event Information parameters.

Table 46. RMON Event Parameter Descriptions

Parameter	Description
Index	Displays the index number that identifies each event instance.
Type	Displays the type of notification provided for this event, as follows: `none, log, trap, both`.
Last sent	Displays the time that passed since the last switch reboot, when the most recent event was triggered. This value is cleared when the switch reboots.
Description	Displays a text description of the event.
Owner	Displays the owner of the alarm instance.

Link Status Information

The following command displays link information:

`show interface status` <*port alias or number*>

Command mode: All

```
-------------------------------------------------------------------------
Alias   Port   Speed    Duplex     Flow Ctrl      Link     Description
------- ----   -----   --------  --TX-----RX--   ------   -------------
1        1       any     auto      no     no      down       1
2        2       any     auto      no     no      down       2
3        3       any     auto      no     no      down       3
4        4       any     auto      no     no      down       4
5        5       any     auto      no     no      down       5
```

Use this command to display link status information about each port on the G7028, including:

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

Port Information

The following command displays port information:

`show interface trunk` <*port alias or number*>

Command mode: All

```
Alias Port Tag RMON Lrn Fld PVID   DESCRIPTION   VLAN(s)
           Trk              NVLAN
----- ---- --- ---- --- --- ----- -------------- --------------------
1     1     n   d    e   e     1                 1
2     2     n   d    e   e     1                 1
3     3     n   d    e   e     1                 1
4     4     n   d    e   e     1                 1
5     5     n   d    e   e     1                 1
...
MGT   65    n   d    e   e  4095                 4095

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

Port information includes:

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

Port Transceiver Status

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

```
show interface transceiver
```

Command mode: All

```
Port             Link  Transceiver    Vendor           Part             Approve
---------------- ----- -------------- ---------------- ---------------- --------
XGE1 SFP+ 1      LINK  LimDAC 1.0m    IBM-Amphenol     46K6182-L36836B  Approved
XGE2 SFP+ 2      < NO Device Installed >
XGE3 SFP+ 3      LINK  LimDAC 1.0m    IBM-Amphenol     46K6182-L36836B  Approved
XGE4 SFP+ 4      < NO Device Installed >
```

This command displays information about the transceiver module on each port, as follows:

- Name identifies the port number and media type
- Link status
- Media/Transceiver type (LX, LR, SX, SR)
- Vendor name
- Part number
- Approval status

Information Dump

The following command dumps switch information:

```
show information-dump
```

Command mode: All

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

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

Chapter 3. Statistics Commands

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

Table 47. Statistics Commands

Command Syntax and Usage
`show layer3 counters` Displays Layer 3 statistics. **Command mode:** All
`show snmp-server counters` **Command mode:** All Displays SNMP statistics. See page 122 for sample output.
`show ntp counters` Displays Network Time Protocol (NTP) Statistics. **Command mode:** All See page 126 for a sample output and a description of NTP Statistics.
`clear mp-counters` Clears all MP-related statistics. **Command mode:** Privileged EXEC
`clear cpu` Clears all CPU utilization statistics. **Command mode:** Privileged EXEC
`clear interface port` <*port number*> `counters` Clears all statistics for the specified port. **Command mode:** All
`show counters` Dumps all switch statistics. Use this command to gather data for tuning and debugging switch performance. If you want to capture dump data to a file, set your communication software on your workstation to capture session data prior to issuing the dump command. **Command mode:** All For details, see page 128.

Port Statistics

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

Table 48. Port Statistics Commands

Command Syntax and Usage
`show interface port <port alias or number> bitrate-usage` Displays the traffic rate in kilobits per second. **Command mode:** All
`show interface port <port alias or number> bridging-counters` Displays bridging (“dot1”) statistics for the port. **Command mode:** All See page 80 for sample output.
`show interface port <port alias or number> bridging-rate` Displays per-second bridging (“dot1”) statistics for the port. **Command mode:** All
`show interface port <port alias or number> ethernet-counters` Displays Ethernet (“dot3”) statistics for the port. **Command mode:** All See page 81 for sample output.
`show interface port <port alias or number> ethernet-rate` Displays per-second Ethernet (“dot3”) statistics for the port. **Command mode:** All
`show interface port <port alias or number> interface-counters` Displays interface statistics for the port. See page 84 for sample output. **Command mode:** All
`show interface port <port alias or number> interface-rate` Displays per-second interface statistics for the port. **Command mode:** All
`show interface port <port alias or number> link-counters` Displays link statistics for the port. See page 85 for sample output. **Command mode:** All
`show interface port <port alias or number> rmon-counters` Displays Remote Monitoring (RMON) statistics for the port. See page 86 for sample output. **Command mode:** All

Table 48. Port Statistics Commands (continued)

Command Syntax and Usage
`clear interface port` *<port alias or number>* `counters` Clears all statistics for the port. **Command mode:** Privileged EXEC
`clear counters` Clears statistics for all ports. **Command mode:** Privileged EXEC

Bridging Statistics

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

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

Command mode: All

```
Bridging statistics for port 1:
dot1PortInFrames:                   63242584
dot1PortOutFrames:                  63277826
dot1PortInDiscards:                        0
dot1TpLearnedEntryDiscards:                0
dot1StpPortForwardTransitions:             0
```

Table 49. Bridging Statistics of a Port

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

Ethernet Statistics

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

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

Command mode: All

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

Table 50. Ethernet Statistics of a Port

Statistics	Description
dot3StatsAlignment Errors	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.

Table 50. Ethernet Statistics of a Port (continued)

Statistics	Description
dot3StatsSingleCollision Frames	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.
dot3StatsMultipleCollision Frames	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.
dot3StatsExcessive Collisions	A count of frames for which transmission on a particular interface fails due to excessive collisions.
dot3StatsInternalMac TransmitErrors	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.

Table 50. Ethernet Statistics of a Port (continued)

Statistics	Description
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.
dot3StatsInternalMac ReceiveErrors	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 alias or number>* `interface-counters`

Command mode: All.

```
Interface statistics for port 1:
                     ifHCIn Counters       ifHCOut Counters
Octets:                  51697080313            51721056808
UcastPkts:                  65356399               65385714
BroadcastPkts:                     0                   6516
MulticastPkts:                     0                      0
FlowCtrlPkts:                      0                      0
Discards:                          0                      0
Errors:                            0                  21187
```

Table 51. Interface Statistics of a Port

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

Table 51. Interface Statistics of a Port (continued)

Statistics	Description
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 toa 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`.
ifOutFlowControlPkts	The total number of flow control `pause` packets transmitted out of the interface.
ifOutDiscards	The number of outbound packets which were chosen to be discarded even though no errors had been detected to prevent their being transmitted. One possible reason for discarding such a packet could be to free up buffer space.
ifOutErrors	For packet-oriented interfaces, the number of outbound packets that could not be transmitted because of errors. For character-oriented or fixed-length interfaces, the number of outbound transmission units that could not be transmitted because of errors.

Link Statistics

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

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

Command mode: All

```
Link statistics for port 1:
linkStateChange:            1
```

Table 52. Link Statistics of a Port

Statistics	Description
linkStateChange	The total number of link state changes.

RMON Statistics

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

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

Command mode: All.

```
RMON statistics for port EXT2:

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

Table 53. RMON Statistics of a Port

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

Table 53. RMON Statistics of a Port (continued)

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

Table 53. RMON Statistics of a Port (continued)

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

Trunk Group Statistics

Table 54. Trunk Group Statistics Commands

Command Syntax and Usage
`show interface portchannel` <*trunk group number*> `interface-counters` Displays interface statistics for the trunk group. **Command mode:** All
`clear interface portchannel` <*trunk group number*> `counters` Clears all the statistics on the selected trunk group. **Command mode:** All except User EXEC

Layer 2 Statistics

Table 55. Layer 2 Statistics Commands

Command Syntax and Usage
`show mac-address-table counters` Displays FDB statistics. See page 89 for sample output. **Command mode:** All
`clear mac-address-table counters` Clears FDB statistics. **Command mode:** Privileged EXEC
`show interface port` *<port alias or number>* `lacp counters` Displays Link Aggregation Control Protocol (LACP) statistics. See page 90 for sample output. **Command mode:** All
`clear interface port` *<port alias or number>* `lacp counters` Clears Link Aggregation Control Protocol (LACP) statistics. **Command mode:** Privileged EXEC
`show hotlinks counters` Displays Hot Links statistics. See page 91 for sample output. **Command mode:** All
`clear hotlinks` Clears all Hot Links statistics. **Command mode:** Privileged EXEC
`show interface port` *<port alias or number>* `lldp counters` Displays LLDP statistics. See page 92 for sample output. **Command mode:** All

FDB Statistics

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

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

Command mode: All

```
FDB statistics:
 current:           83   hiwat:             855
```

FDB statistics are described in the following table:

Table 56. Forwarding Database Statistics

Statistic	Description
current	Current number of entries in the Forwarding Database.
hiwat	Highest number of entries recorded at any given time in the Forwarding Database.

LACP Statistics

Use the following command to display Link Aggregation Control Protocol (LACP) statistics:

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

Command mode: All

```
Port 1:
 -------------------------------------
 Valid LACPDUs received:         - 870
 Valid Marker PDUs received:     - 0
 Valid Marker Rsp PDUs received: - 0
 Unknown version/TLV type:       - 0
 Illegal subtype received:       - 0
 LACPDUs transmitted:            - 6031
 Marker PDUs transmitted:        - 0
 Marker Rsp PDUs transmitted:    - 0
```

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

Table 57. LACP Statistics

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

Table 57. LACP Statistics

Statistic	Description
Marker PDUs transmitted	Total number of LACP marker data units transmitted.
Marker Rsp PDUs transmitted	Total number of LACP marker response data units transmitted.

Hotlinks Statistics

Use the following command to display Hot Links statistics:

```
show hotlinks counters
```

Command mode: All

```
Hot Links Trigger Stats:

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

The following table describes the Hotlinks statistics:

Table 58. Hotlinks Statistics

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

LLDP Port Statistics

Use the following command to display LLDP statistics:

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

Command mode: All

```
LLDP Port 1 Statistics
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
Frames Transmitted          : 0
Frames Received             : 0
Frames Received in Errors   : 0
Frames Discarded            : 0
TLVs Unrecognized           : 0
Neighbors Aged Out          : 0
...
```

The following table describes the LLDP port statistics:

Table 59. LLDP port Statistics

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

Layer 3 Statistics

Table 60. Layer 3 Statistics Commands

Command Syntax and Usage
`show ip counters` Displays IP statistics. See page 95 for sample output. **Command mode:** All
`clear ip counters` Clears IPv4 statistics. Use this command with caution as it deletes all the IPv4 statistics. **Command mode:** Privileged EXEC
`show ipv6 counters` Displays IPv6 statistics. See page 97 for sample output. **Command mode:** All
`show ip dns counters` Displays Domain Name System (DNS) statistics. See page 101 for sample output. **Command mode:** All
`show ip icmp counters` Displays ICMP statistics. See page 101 for sample output. **Command mode:** All
`show ip tcp counters` Displays TCP statistics. See page 103 for sample output. **Command mode:** All
`show ip udp counters` Displays UDP statistics. See page 105 for sample output. **Command mode:** All
`show ip igmp counters` Displays IGMP statistics. See page 106 for sample output. **Command mode:** All
`show layer3 igmp-groups` Displays the total number of IGMP groups that are registered on the switch. **Command mode:** All
`show layer3 ipmc-groups` Displays the total number of current IP multicast groups that are registered on the switch. **Command mode:** All

Table 60. Layer 3 Statistics Commands (continued)

Command Syntax and Usage
`clear ip dns counters` Clears Domain Name System (DNS) statistics. **Command mode:** Privileged EXEC
`clear ip icmp counters` Clears Internet Control Message Protocol (ICMP) statistics. **Command mode:** Privileged EXEC
`clear ip tcp counters` Clears Transmission Control Protocol (TCP) statistics. **Command mode:** Privileged EXEC
`clear ip udp counters` Clears User Datagram Protocol (UDP) statistics. **Command mode:** Privileged EXEC
`clear ip igmp [`<*VLAN number*>`] counters` Clears IGMP statistics. **Command mode:** Privileged EXEC
`clear ip counters` Clears IP statistics. Use this command with caution as it will delete all the IP statistics. **Command mode:** Privileged EXEC
`show layer3 counters` Dumps all Layer 3 statistics. Use this command to gather data for tuning and debugging switch performance. If you want to capture dump data to a file, set your communication software on your workstation to capture session data prior to issuing the dump command. **Command mode:** All

IPv4 Statistics

The following command displays IPv4 statistics:

```
show ip counters
```

Command mode: All

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

Use the following command to clear IPv4 statistics:

```
clear ip counters
```

Table 61. IPv4 Statistics

Statistics	Description
ipInReceives	The total number of input datagrams received from interfaces, including those received in error.
ipInHdrErrors	The number of input datagrams discarded due to errors in their IP headers, including bad `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.
ipInUnknownProtos	The number of locally addressed datagrams received successfully but discarded because of an unknown or unsupported protocol.
ipInDiscards	The number of input IP datagrams for which no problems were encountered to prevent their continued processing, but which were discarded (for example, for lack of buffer space). Note that this counter does not include any datagrams discarded while awaiting re-assembly.
ipInDelivers	The total number of input datagrams successfully delivered to IP user-protocols (including ICMP).

Table 61. IPv4 Statistics (continued)

Statistics	Description
ipOutRequests	The total number of IP datagrams which local IP user-protocols (including ICMP) supplied to IP in requests for transmission. Note that this counter does not include any datagrams counted in `ipForwDatagrams`.
ipOutDiscards	The number of output IP datagrams for which no problem was encountered to prevent their transmission to their destination, but which were discarded (for example, for lack of buffer space). Note that this counter would include datagrams counted in `ipForwDatagrams` if any such packets met this (discretionary) discard criterion.
ipDefaultTTL	The default value inserted into the `Time-To-Live` (TTL) field of the IP header of datagrams originated at this entity (the switch), whenever a TTL value is not supplied by the transport layer protocol.

IPv6 Statistics

The following command displays IPv6 statistics:

```
show ipv6 counters
```

Command mode: All

```
    IPv6 Statistics
    ***************
144  Rcvd          0    HdrErrors     0    TooBigErrors
0    AddrErrors    0    FwdDgrams     0    UnknownProtos
0    Discards      144  Delivers      130  OutRequests
0    OutDiscards   0    OutNoRoutes   0    ReasmReqds
0    ReasmOKs      0    ReasmFails
0    FragOKs       0    FragFails     0    FragCreates
7    RcvdMCastPkt  2    SentMcastPkts 0    TruncatedPkts
0    RcvdRedirects 0    SentRedirects
    ICMP Statistics
    ***************
    Received :
33  ICMPPkts     0 ICMPErrPkt      0 DestUnreach  0 TimeExcds
0   ParmProbs    0 PktTooBigMsg    9 ICMPEchoReq  10 ICMPEchoReps
0   RouterSols   0 RouterAdv       5 NeighSols    9 NeighAdv
0   Redirects    0 AdminProhib     0 ICMPBadCode
    Sent
19  ICMPMsgs     0 ICMPErrMsgs     0 DstUnReach   0 TimeExcds
0   ParmProbs    0 PktTooBigs      10 EchoReq     9 EchoReply
0   RouterSols   0 RouterAdv       11 NeighSols   5 NeighborAdv
0   RedirectMsgs 0 AdminProhibMsgs
    UDP statistics
    **************
    Received :
0 UDPDgrams    0 UDPNoPorts       0 UDPErrPkts
    Sent :
0 UDPDgrams
```

Table 62. describes the IPv6 statistics.

Table 62. IPv6 Statistics

Statistic	Description
Rcvd	Number of datagrams received from interfaces, including those received in error.
HdrErrors	Number of datagrams discarded due to errors in their IP headers, including bad `checksums`, version number mismatch, other format errors, time-to-live exceeded, errors discovered in processing their IP options, and so forth.
TooBigErrors	The number of input datagrams that could not be forwarded because their size exceeded the link MTU of outgoing interface.

Table 62. IPv6 Statistics (continued)

Statistic	Description
AddrErrors	Number of datagrams discarded because the IP address in their IP header's destination field was not a valid address to be received at this entity (the switch). This count includes invalid addresses. For entities which are not IP Gateways and therefore do not forward datagrams, this counter includes datagrams discarded because the destination address was not a local address.
FwdDgrams	Number of input datagrams for which this entity (the switch) was not their final IP destination, as a result of which an attempt was made to find a route to forward them to that final destination. In entities which do not act as IP Gateways, this counter will include only those packets, which were Source-Routed via this entity (the switch), and the Source-Route option processing was successful.
UnknownProtos	Number of locally addressed datagrams received successfully but discarded because of an unknown or unsupported protocol.
Discards	Number of IP datagrams for which no problems were encountered to prevent their continued processing, but which were discarded (for example, for lack of buffer space). Note that this counter does not include any datagrams discarded while awaiting re-assembly.
Delivers	Number of datagrams successfully delivered to IP user-protocols (including ICMP).
OutRequests	Number of IP datagrams which local IP user-protocols (including ICMP) supplied to IP in requests for transmission.
OutDiscards	Number of output IP datagrams for which no problem was encountered to prevent their transmission to their destination, but which were discarded (for example, for lack of buffer space).
OutNoRoutes	Number of IP datagrams discarded because no route could be found to transmit them to their destination. Note that this includes any datagrams which a host cannot route because all of its default gateways are down.
ReasmReqds	Number of IP fragments received which needed to be reassembled at this entity (the switch).
ReasmOKs	Number of IP datagrams successfully re- assembled.
ReasmFails	Number of failures detected by the IP re- assembly algorithm (for whatever reason: timed out, errors, and so forth). Note that this is not necessarily a count of discarded IP fragments since some algorithms (notably the algorithm in RFC 815) can lose track of the number of fragments by combining them as they are received.
FragOKs	Number of IP datagrams that have been successfully fragmented at this entity (the switch).

Table 62. IPv6 Statistics (continued)

Statistic	Description
FragFails	Number of IP datagrams that have been discarded because they needed to be fragmented at this entity (the switch) but could not be, for example, because their `Don't Fragment` flag was set.
FragCreates	Number of IP datagram fragments that have been generated as a result of fragmentation at this entity (the switch).
RcvdMCastPkt	The number of multicast packets received by the interface.
SentMcastPkts	The number of multicast packets transmitted by the interface.
TruncatedPkts	The number of input datagrams discarded because datagram frame didn't carry enough data.
RcvdRedirects	The number of Redirect messages received by the interface.
SentRedirects	The number of Redirect messages sent.

The following table describes the IPv6 ICMP statistics.

Table 63. ICMP Statistics

Statistic	Description
Received	
ICMPPkts	Number of ICMP messages which the entity (the switch) received.
ICMPErrPkt	Number of ICMP messages which the entity (the switch) received but determined as having ICMP-specific errors (bad ICMP `checksums`, bad length, and so forth).
DestUnreach	Number of ICMP Destination Unreachable messages received.
TimeExcds	Number of ICMP Time Exceeded messages received.
ParmProbs	Number of ICMP Parameter Problem messages received.
PktTooBigMsg	The number of ICMP Packet Too Big messages received by the interface.
ICMPEchoReq	Number of ICMP Echo (request) messages received.
ICMPEchoReps	Number of ICMP Echo Reply messages received.
RouterSols	Number of Router Solicitation messages received by the switch.
RouterAdv	Number of Router Advertisements received by the switch.
NeighSols	Number of Neighbor Solicitations received by the switch.
NeighAdv	Number of Neighbor Advertisements received by the switch.
Redirects	Number of ICMP Redirect messages received.
AdminProhib	The number of ICMP destination unreachable/communication administratively prohibited messages received by the interface.
ICMPBadCode	The number of ICMP Parameter Problem messages received by the interface.

Table 63. ICMP Statistics

Statistic	Description
Sent	
ICMPMsgs	Number of ICMP messages which this entity (the switch) attempted to send.
ICMPErrMsgs	Number of ICMP messages which this entity (the switch) did not send due to problems discovered within ICMP such as a lack of buffer. This value should not include errors discovered outside the ICMP layer such as the inability of IP to route the resultant datagram. In some implementations there may be no types of errors that contribute to this counter's value.
DstUnReach	Number of ICMP Destination Unreachable messages sent.
TimeExcds	Number of ICMP Time Exceeded messages sent.
ParmProbs	Number of ICMP Parameter Problem messages sent.
PktTooBigs	The number of ICMP Packet Too Big messages sent by the interface.
EchoReq	Number of ICMP Echo (request) messages sent.
EchoReply	Number of ICMP Echo Reply messages sent.
RouterSols	Number of Router Solicitation messages sent by the switch.
RouterAdv	Number of Router Advertisements sent by the switch.
NeighSols	Number of Neighbor Solicitations sent by the switch.
NeighAdv	Number of Neighbor Advertisements sent by the switch.
RedirectMsgs	Number of ICMP Redirect messages sent. For a host, this object will always be zero, since hosts do not send redirects.
AdminProhibMsgs	Number of ICMP destination unreachable/communication administratively prohibited messages sent.

Table 64. describes the UDP statistics.

Table 64. UDP Statistics

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

DNS Statistics

The following command displays Domain Name System statistics.

```
show ip dns counters
```

Command mode: All

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

Table 65. DNS Statistics

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

ICMP Statistics

The following command displays ICMP statistics:

```
show ip icmp counters
```

Command mode: All

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

Table 66. ICMP Statistics

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

Table 66. ICMP Statistics (continued)

Statistic	Description
icmpOutParmProbs	The number of ICMP Parameter Problem messages sent.
icmpOutSrcQuenchs	The number of ICMP Source Quench (buffer almost full, stop sending data) messages sent.
icmpOutRedirects	The number of ICMP Redirect messages sent. For a host, this object will always be zero, since hosts do not send redirects.
icmpOutEchos	The number of ICMP Echo (request) messages sent.
icmpOutEchoReps	The number of ICMP Echo Reply messages sent.
icmpOutTimestamps	The number of ICMP Timestamp (request) messages sent.
icmpOutTimestampReps	The number of ICMP Timestamp `Reply` messages sent.
icmpOutAddrMasks	The number of ICMP Address Mask Request messages sent.
icmpOutAddrMaskReps	The number of ICMP Address Mask Reply messages sent.

TCP Statistics

The following command displays TCP statistics:

```
show ip tcp counters
```

Command mode: All

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

Table 67. TCP Statistics

Statistic	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.
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`).

Table 67. TCP Statistics (continued)

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

UDP Statistics

The following command displays UDP statistics:

```
show ip udp counters
```

Command mode: All

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

Table 68. UDP Statistics

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

IGMP Statistics

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

```
show ip igmp counters
```

Command mode: All

```
IGMP vlan 2 statistics:
------------------------------------------------------------------------
rxIgmpValidPkts:                0   rxIgmpInvalidPkts:                0
rxIgmpGenQueries:               0   rxIgmpGrpSpecificQueries:         0
rxIgmpGroupSrcSpecificQueries:  0   rxIgmpDiscardPkts:                0
rxIgmpLeaves:                   0   rxIgmpReports:                    0
txIgmpReports:                  0   txIgmpGrpSpecificQueries:         0
txIgmpLeaves:                   0   rxIgmpV3CurrentStateRecords:      0
rxIgmpV3SourceListChangeRecords:0   rxIgmpV3FilterChangeRecords:      0
txIgmpGenQueries:                    18
```

Table 69. IGMP Statistics

Statistic	Description
rxIgmpValidPkts	Total number of valid IGMP packets received
rxIgmpInvalidPkts	Total number of invalid packets received
rxIgmpGenQueries	Total number of General Membership Query packets received
rxIgmpGrpSpecificQueries	Total number of Membership Query packets received from specific groups
rxIgmpGroupSrcSpecificQueries	Total number of Group Source-Specific Queries (GSSQ) received
rxIgmpDiscardPkts	Total number of IGMP packets discarded
rxIgmpLeaves	Total number of Leave requests received
rxIgmpReports	Total number of Membership Reports received
txIgmpReports	Total number of Membership reports transmitted
txIgmpGrpSpecificQueries	Total number of Membership Query packets transmitted to specific groups
txIgmpLeaves	Total number of Leave messages transmitted
rxIgmpV3CurrentStateRecords	Total number of Current State records received
rxIgmpV3SourceListChangeRecords	Total number of Source List Change records received.

Table 69. IGMP Statistics (continued)

Statistic	Description
rxIgmpV3FilterChangeRecords	Total number of Filter Change records received.
txIgmpGenQueries	Total number of General Membership Query packets transmitted

Management Processor Statistics

Table 70. Management Processor Statistics Commands

Command Syntax and Usage
`show mp packet counters` Displays packet statistics, to check for leads and load. To view a sample output and a description of the stats, see page 110. **Command mode:** All
`show mp tcp-block` Displays all TCP control blocks that are in use. To view a sample output and a description of the stats, see page 116. **Command mode:** All
`show mp udp-block` Displays all UDP control blocks that are in use. To view a sample output, see page 117. **Command mode:** All
`show processes cpu` Displays CPU utilization for periods of up to 1, 4, and 64 seconds. To view a sample output and a description of the stats, see page 117. **Command mode:** All

MP Packet Statistics

Table 71. Packet Statistics Commands

Command Syntax and Usage
`show mp packet counters` Displays packet statistics, to check for leads and load. To view a sample output and a description of the stats, see page 110. **Command mode:** All
`show mp packet logs` Displays a log of all packets received by the CPU. **Command mode:** All
`show mp packet last` <*number of logs*> Displays a list of the most recent packets received by the CPU. **Command mode:** All
`show mp packet parse rx|tx` <*parsing_option*> Displays a list of received or sent packets that fit the parsing option. For a list of parsing options, see page 113. **Command mode:** All
`show mp packet dump` Displays all packet statistics and logs. **Command mode:** All

The following command displays MP packet statistics:

`show mp packet counters`

Command mode: All

```
CPU packet statistics at 16:57:24 Sat Apr  5, 2011

Packet rate:         Incoming            Outgoing
------------         --------            --------
1-second:                   0                   1
4-seconds:                  0                   0
64-seconds:                 0                   0

Packet counters:     Received                Sent
-----------------    --------                ----
Total packets:           3687               40802
Since bootup:            3687               40802
BPDUs:                      3               37160
Cisco packets:              0                   0
ARP Requests:               0                   0
ARP Replies:                0                   0
LACP packets:               0                   0
IPv4 packets:            1207                1165
 ICMP Requests:             0                   0
 ICMP Replies:              0                   0
 IGMP packets:              0                   0
 PIM packets:               0                   0
 VRRP packets:              0                   0
 TCP  packets:              0                   0
  FTP                       0                   0
  HTTP                      0                   0
  SSH                       0                   0
  TACACS                    0                   0
  TELNET                    0                   0
  TCP other                 0                   0
 UDP packets:               0                1165
  DHCP                      0                1165
  NTP                       0                   0
  RADIUS                    0                   0
  SNMP                      0                   0
  TFTP                      0                   0
  UDP other                 0                   0
 RIP packets:               0                   0
 OSPF packets:              0                   0
 BGP packets:               0                   0
IPv6 packets:               0                   0
LLDP PDUs:               2478                2478
ECP PDUs:                   0                   0
MgmtSock Packets:           0                   0
Other:                      0                   0
```

```
Packet Buffer Statistics:
-------------------------
 allocs:         14311
 frees:          14311
 failures:           0
 dropped:            0

 small packet buffers:
 ---------------------
   current:                  0
   max:                   2048
   threshold:              512
   hi-watermark:             1
   hi-water time:   14:59:46 Sat Apr  5, 2011

 medium packet buffers:
 ----------------------
   current:                  0
   max:                   2048
   threshold:              512
   hi-watermark:             1
   hi-water time:   14:59:49 Sat Apr  5, 2011

 jumbo packet buffers:
 ---------------------
   current:                  0
   max:                      4
   hi-watermark:             0

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

Table 72. Packet Statistics

Statistics	Description
Packets received by CPU	
Total packets	Total number of packets received
BPDUs	Total number of spanning-tree Bridge Protocol Data Units received.
Cisco packets	Total number of UniDirectional Link Detection (UDLD) packets and Cisco Discovery Protocol (CDP) packets received.
ARP packets	Total number of Address Resolution Protocol packets received.
IPv4 packets	Total number of IPv4 packets received.
IPv6 packets	Total number of IPv6 packets received.
LLDP PDUs	Total number of Link Layer Discovery Protocol data units received.
Other	Total number of other packets received.

Table 72. Packet Statistics (continued)

Statistics	Description
Packet Buffer Statistics	
allocs	Total number of packet allocations from the packet buffer pool by the TCP/IP protocol stack.
frees	Total number of times the packet buffers are freed (released) to the packet buffer pool by the TCP/IP protocol stack.
failures	Total number of packet allocation failures from the packet buffer pool by the TCP/IP protocol stack.
small packet buffers	
current	Total number of packet allocations with size less than 128 bytes from the packet buffer pool by the TCP/IP protocol stack.
max	Maximum number of small packet allocations supported.
threshold	Threshold value for small packet allocations, beyond which only high-priority small packets are allowed.
hi-watermark	The highest number of packet allocation with size less than 128 bytes from the packet buffer pool by the TCP/IP protocol stack.
hi-water time	Time stamp that indicates when the hi-watermark was reached.
medium packet buffers	
current	Total number of packet allocations with size between 128 to 1536 bytes from the packet buffer pool by the TCP/IP protocol stack.
max	Maximum number of medium packet allocations supported
threshold	Threshold value for medium packet allocations, beyond which only high-priority medium packets are allowed.
hi-watermark	The highest number of packet allocation with size between 128 to 1536 bytes from the packet buffer pool by the TCP/IP protocol stack.
hi-water time	Time stamp that indicates when the hi-watermark was reached.
jumbo packet buffers	
current	Total number of packet allocations with more than 1536 bytes from the packet buffer pool by the TCP/IP protocol stack.
max	Maximum number of jumbo packet allocations supported

Table 72. Packet Statistics (continued)

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

Logged Packet Statistics

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

`show mp packet parse rx|tx` <*parsing_option*>

The filter options are described in Table 73.

Table 73. Packet Log Parsing Options

Command Syntax and Usage
`show mp packet parse rx|tx bpdu` Displays only BPDUs logged **Command mode:** All
`show mp packet parse rx|tx cisco` Displays only Cisco packets (BPDU/CDP/UDLD) logged. **Command mode:** All
`show mp packet parse rx|tx lacp` Displays only LACP PDUs logged. **Command mode:** All
`show mp packet parse rx|tx ipv4` Displays only IPv4 packets logged. **Command mode:** All
`show mp packet parse rx|tx igmp` Displays only IGMP packets logged. **Command mode:** All

Table 73. Packet Log Parsing Options (continued)

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

Table 73. Packet Log Parsing Options (continued)

Command Syntax and Usage
`show mp packet parse rx|tx radius` Displays only RADIUS packets logged. **Command mode:** All
`show mp packet parse rx|tx snmp` Displays only SNMP packets logged. **Command mode:** All
`show mp packet parse rx|tx tftp` Displays only TFTP packets logged. **Command mode:** All
`show mp packet parse rx|tx udpother` Displays only UDP other-port packets logged. **Command mode:** All
`show mp packet parse rx|tx ipv6` Displays only IPv6 packets logged. **Command mode:** All
`show mp packet parse rx|tx lldp` Displays only LLDP PDUs logged. **Command mode:** All
`show mp packet parse rx|tx vlan` <*VLAN_number*> Displays only logged packets with the specified VLAN. **Command mode:** All
`show mp packet parse rx|tx port` <*port_number*> Displays only logged packets with the specified port. **Command mode:** All
`show mp packet parse rx|tx mac` <*MAC_address*> Displays only logged packets with the specified MAC address. **Command mode:** All
`show mp packet parse rx|tx ip-addr` <*IPv4_address*> Displays only logged packets with the specified IPv4 address. **Command mode:** All
`show mp packet parse rx|tx other` Displays logs of all packets not explicitly selectable. **Command mode:** All
`show mp packet parse rx|tx raw` Displays raw packet buffer in addition to headers. **Command mode:** All

TCP Statistics

The following command displays TCP statistics:

```
show mp tcp-block
```

Command mode: All

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


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

Table 74. MP Specified TCP Statistics

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

UDP Statistics

The following command displays UDP statistics:

`show mp udp-block`

Command mode: All

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

CPU Statistics

The following command displays CPU use statistics:

Command mode: All

`show processes cpu`

Command mode: All

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

Table 75. CPU Statistics

Statistics	Description
Thread ID	The thread ID number.
Thread Name	The name of the thread.
1sec	The percent of CPU use over 1 second.
5sec	The percent of CPU use over 5 seconds.

Table 75. CPU Statistics

Statistics	Description
1Min	The percent of CPU use over 1 minute.
5Min	The percent of CPU use over 5 minutes.
Status	The status of the process.

CPU Statistics History

The following command displays a history of CPU use statistics:

```
show processes cpu history
```

Command mode: All

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

QoS Statistics

Table 76. QoS Statistics Commands

Command Syntax and Usage
`show qos protocol-packet-control protocol-counters` <*packet type*> Displays the total packet count of the selected packet type received by hardware. **Command mode:** All
`show qos protocol-packet-control queue-counters` Displays the total number of packets received by each queue. **Command mode:** All
`clear qos protocol-packet-control protocol-counters` <*packet type*> Clears packet queue statistics for the selected packet type. **Command mode:** All
`clear qos protocol-packet-control queue-counters` <*queue number*> Clears packet queue statistics for the selected queue. **Command mode:** All
`clear qos protocol-packet-control all` Clears all packet queue statistics. **Command mode:** All

Access Control List Statistics

Table 77. ACL Statistics Commands

Command Syntax and Usage
`show access-control list <ACL number> counters` Displays the Access Control List statistics for a specific ACL. **Command mode:** All
`show access-control list6 <ACL number> counters` Displays the IPv6 ACL statistics for a specific ACL. **Command mode:** All
`show access-control macl <MACL number> counters` Displays the ACL statistics for a specific management ACL (MACL). **Command mode:** All
`show access-control counters` Displays all ACL statistics. **Command mode:** All
`clear access-control list {<ACL number>|all} counters` Clears ACL statistics. **Command mode:** Privileged EXEC
`clear access-control list6 {<ACL number>|all} counters` Clears IPv6 ACL statistics. **Command mode:** Privileged EXEC
`clear access-control macl {<ACL number>|all} counters` Clears Management ACL (MACL) statistics. **Command mode:** Privileged EXEC
`show access-control meter <meter number> counters` Displays ACL meter statistics. **Command mode:** All
`clear access-control meter <meter number> counters` Clears ACL meter statistics. **Command mode:** Privileged EXEC

ACL Statistics

This option displays ACL statistics.

```
show access-control counters
```

Command mode: All

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

SNMP Statistics

The following command displays SNMP statistics:

```
show snmp-server counters
```

Command mode: All

```
SNMP statistics:
snmpInPkts:             150097   snmpInBadVersions:              0
snmpInBadC'tyNames:          0   snmpInBadC'tyUses:              0
snmpInASNParseErrs:          0   snmpEnableAuthTraps:            0
snmpOutPkts:            150097   snmpInBadTypes:                 0
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 78. SNMP Statistics

Statistic	Description
snmpInPkts	The total number of Messages delivered to the SNMP entity from the transport service.
snmpInBadVersions	The total number of SNMP Messages, which were delivered to the SNMP protocol entity and were for an unsupported SNMP version.
snmpInBadC'tyNames	The total number of SNMP Messages delivered to the SNMP entity which used an SNMP community name not known to the said entity (the switch).
snmpInBadC'tyUses	The total number of SNMP Messages delivered to the SNMP protocol entity which represented an SNMP operation which was not allowed by the SNMP community named in the Message.

Table 78. SNMP Statistics (continued)

Statistic	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.
snmpEnableAuthTraps	An object to enable or disable the authentication traps generated by this entity (the switch).
snmpOutPkts	The total number of SNMP Messages which were passed from the SNMP protocol entity to the transport service.
snmpInBadTypes	The total number of SNMP Messages which failed ASN parsing.
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.

Table 78. SNMP Statistics (continued)

Statistic	Description
snmpInGenErrs	The total number of SNMP Protocol Data Units (PDUs), which were delivered to the SNMP protocol entity and for which the value of the error-status field is `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).
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.

Table 78. SNMP Statistics (continued)

Statistic	Description
snmpOutGenErrs	The total number of SNMP Protocol Data Units (PDUs), which were generated by the SNMP protocol entity and for which the value of the error-status field is `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.
snmpOutGetResponses	The total number of SNMP Get-Response Protocol Data Units (PDUs), which have been generated by the SNMP protocol entity.
snmpOutTraps	The total number of SNMP Trap Protocol Data Units (PDUs), which have been generated by the SNMP protocol entity.
snmpSilentDrops	The total number of `GetRequest`-PDUs, `GetNextRequest`-PDUs, `GetBulkRequest`-PDUs, `SetRequest`-PDUs, and `InformRequest`-PDUs delivered to the OSPFSNMPv2 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

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

The following command displays NTP statistics:

```
show ntp counters
```

Command mode: All

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

Table 79. 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.

Table 79. NTP Statistics

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

The following command displays information about NTP associated peers:

```
show ntp associations
```

Command mode: All

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

Table 80. NTP Associations

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

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 81. General Configuration Commands

Command Syntax and Usage
`show running-config` Dumps current configuration to a script file. For details, see page 245. **Command mode:** Privileged EXEC
`show running-config diff` Displays running configuration changes that have been applied but not saved to flash memory. **Command mode:** Privileged EXEC
`copy running-config backup-config` Copy the current (running) configuration from switch memory to the `backup-config` partition. For details, see page 246. **Command mode:** Privileged EXEC
`copy running-config startup-config` Copy the current (running) configuration from switch memory to the `startup-config` partition. **Command mode:** Privileged EXEC
`write memory` Copy the current (running) configuration from switch memory to the `active-config` partition. **Command mode:** Privileged EXEC
`copy running-config {ftp|tftp}[data-port|mgt-port]` Backs up current configuration to a file on the selected FTP/TFTP server. **Command mode:** Privileged EXEC
`copy {ftp|tftp} running-config [data-port|mgt-port]` Restores current configuration from a FTP/TFTP server. **Command mode:** Privileged EXEC For details, see page 247.

Viewing and Saving Changes

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

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

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

Saving the Configuration

You must save configuration settings to flash memory, so the G7028 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:

```
RS G7028(config)# 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 258.

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.ele

Table 82. System Configuration Options

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

Table 82. System Configuration Options (continued)

Command Syntax and Usage
`no line vty` Sets `line vty length` to the default value of 28. **Command mode:** Global configuration
`system idle` *<0-60>* Sets the idle timeout for CLI sessions in minutes. The default value is 10 minutes. A value of 0 disables system idle. **Command mode:** Global configuration
`system notice` *<maximum 1024 character multi-line login notice>* `<'.' to end>` Displays a login notice immediately before the “Enter password:” prompt. This notice can contain up to 1024 characters and new lines. **Command mode:** Global configuration
`[no] banner` *<1-80 characters>* Configures a login banner of up to 80 characters. When a user or administrator logs into the switch, the login banner is displayed. It is also displayed as part of the output from the `show sys-info` command. **Command mode:** Global configuration
`[no] hostname` *<character string>* Enables or disables displaying of the host name (system administrator’s name) in the Command Line Interface (CLI). **Command mode:** Global configuration
`[no] system dhcp` Enables or disables Dynamic Host Control Protocol for setting the IP address on interface 4. When enabled, the IP address obtained from the DHCP server overrides the static IP address. The default setting is `enabled`. **Command mode:** Global configuration
`[no] system reset-control` Enables or disables the reset control flag. When enabled, the switch continues to function after a crash of the main processor, using the last known Layer 2/3 information. **Command mode:** Global configuration
`[no] system packet-logging` Enables or disables logging of packets that come to the CPU. The default setting is `enabled`. **Command mode:** Global configuration
`show system` Displays the current system parameters. **Command mode:** All

System Error Disable and Recovery Configuration

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

Table 83. Error Disable Configuration Options

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

Link Flap Dampening Configuration

The Link Flap Dampening feature allows the switch to automatically disable a port if too many link flaps (link up/link down) are detected on the port during a specified time interval. The port remains in the error-disabled state until it is re-enabled manually, or re-enabled automatically by the switch after a timeout period has elapsed.

Table 84. Link Flap Dampening Configuration Options

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

System Host Log Configuration

Table 85. Host Log Configuration Options

Command Syntax and Usage
[no] logging host <*1-2*> address <*IP address*> Sets the IP address of the first or second syslog host. **Command mode:** Global configuration
logging host <*1-2*> severity <*0-7*> This option sets the severity level of the first or second syslog host displayed. The default is 7, which means log all severity levels. **Command mode:** Global configuration
logging host <*1-2*> facility <*0-7*> This option sets the facility level of the first or second syslog host displayed. The default is 0. **Command mode:** Global configuration
logging console Enables delivering syslog messages to the console. It is enabled by default. **Command mode:** Global configuration
no logging console Disables delivering syslog messages to the console. When necessary, disabling console ensures the switch is not affected by syslog messages. It is enabled by default. **Command mode:** Global configuration
[no] logging synchronous [level <*0-7*> | all] Enables or disables synchronous logging messages. When enabled, logging messages are displayed asynchronously. The level parameter sets the message severity level. Messages with a severity level equal to or higher than this value are displayed asynchronously. Low numbers indicate greater severity. All displays all messages asynchronously, regardless the severity level. The default setting is 2. **Command mode:** Global configuration
logging console severity <*0-7*> This option sets the severity level of syslog messages delivered via the console, telnet, and SSH. The system displays only messages with the selected severity level and above. For example, if you set the console severity to 2, only messages with severity level of 1 and 2 are displayed. The default is 7, which means log all severity levels. **Command mode:** Global configuration
no logging console severity Disables delivering syslog messages to the console based on severity. **Command mode:** Global configuration

Table 85. Host Log Configuration Options (continued)

Command Syntax and Usage
[no] logging log [<*feature*>] Displays a list of features for which syslog messages can be generated. You can choose to enable/disable specific features (such as vlans, stg, or ssh), or enable/disable syslog on all available features. **Command mode:** Global configuration
logging buffer severity <*0-7*> Sets the severity level of the syslog messages saved to flash memory. The default is 7, which means log all severity levels. **Command mode:** Global configuration
show logging [severity <*severity level*>] [reverse] Displays the current syslog settings, followed by the most recent 2000 syslog messages, as displayed by the show logging messages command. For details, see page 34. **Command mode:** All

SSH Server Configuration

For the G7028/G7052, these commands enable Secure Shell access from any SSH client.

Table 86. SSH Server Configuration Options

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

RADIUS Server Configuration

Table 87. RADIUS Server Configuration Options

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

Table 87. RADIUS Server Configuration Options (continued)

Command Syntax and Usage
`[no] radius-server backdoor` Enables or disables the RADIUS backdoor for Telnet/SSH/HTTP/HTTPS. The default value is `disabled`. To obtain the RADIUS backdoor password for your switch, contact your Service and Support line. **Command mode:** Global configuration
`[no] radius-server secure-backdoor` Enables or disables the RADIUS back door using secure password for telnet/SSH/HTTP/HTTPS. This command does not apply when backdoor (`telnet`) is enabled. **Command mode:** Global configuration
`radius-server enable` Enables the RADIUS server. **Command mode:** Global configuration
`no radius-server enable` Disables the RADIUS server. **Command mode:** Global configuration
`show radius-server` Displays the current RADIUS server parameters. **Command mode:** All

TACACS+ Server Configuration

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

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

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

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

Table 88. TACACS+ Server Configuration Options

Command Syntax and Usage
[no] tacacs-server primary-host <*IP address*> Defines the primary TACACS+ server address. **Command mode:** Global configuration
[no] tacacs-server secondary-host <*IP address*> Defines the secondary TACACS+ server address. **Command mode:** Global configuration
[no] tacacs-server primary-host <*IP address*> key <*1-32 characters*> This is the primary shared secret between the switch and the TACACS+ server(s). **Command mode:** Global configuration
[no] tacacs-server secondary-host <*IP address*> key <*1-32 characters*> This is the secondary shared secret between the switch and the TACACS+ server(s). **Command mode:** Global configuration
[no] tacacs-server chpassp <*1-32 characters*> Defines the password for the primary TACACS+ server. **Command mode:** Global configuration
[no] tacacs-server chpasss <*1-32 characters*> Defines the password for the secondary TACACS+ server. **Command mode:** Global configuration

Table 88. TACACS+ Server Configuration Options (continued)

Command Syntax and Usage
`[default] tacacs-server port` *<TCP port number>* Enter the number of the TCP port to be configured, between 1 and 65000. The default is 49. **Command mode:** Global configuration
`tacacs-server retransmit` *<1-3>* Sets the number of failed authentication requests before switching to a different TACACS+ server. The default is 3 requests. **Command mode:** Global configuration
`tacacs-server attempts` *<1-10>* Sets the number of failed login attempts before disconnecting the user. The default is 2 attempts. **Command mode:** Global configuration
`tacacs-server timeout` *<4-15>* Sets the amount of time, in seconds, before a TACACS+ server authentication attempt is considered to have failed. The default is 5 seconds. **Command mode:** Global configuration
`[no] tacacs-server user-mapping {`*<0-15>* `user|oper|admin}` Maps a TACACS+ authorization level to a switch user level. Enter a TACACS+ authorization level (0-15), followed by the corresponding switch user level. **Command mode:** Global configuration
`[no] tacacs-server backdoor` Enables or disables the TACACS+ back door for Telnet, SSH/SCP, or HTTP/HTTPS. Enabling this feature allows you to bypass the TACACS+ servers. It is recommended that you use Secure Backdoor to ensure the switch is secured, because Secure Backdoor disallows access through the back door when the TACACS+ servers are responding. The default setting is `disabled`. To obtain the TACACS+ backdoor password for your G7028/G7052, contact your Service and Support line. **Command mode:** Global configuration
`[no] tacacs-server secure-backdoor` Enables or disables TACACS+ secure back door access through Telnet, SSH/SCP, or HTTP/HTTPS only when the TACACS+ servers are not responding. This feature is recommended to permit access to the switch when the TACACS+ servers become unresponsive. If no back door is enabled, the only way to gain access when TACACS+ servers are unresponsive is to use the back door via the console port. The default is `disabled`. **Command mode:** Global configuration

Table 88. TACACS+ Server Configuration Options (continued)

Command Syntax and Usage
`[no] tacacs-server privilege-mapping` Enables or disables TACACS+ privilege-level mapping. The default value is `disabled`. **Command mode:** Global configuration
`[no] tacacs-server password-change` Enables or disables TACACS+ password change. The default value is `disabled`. **Command mode:** Global configuration
`primary-password` Configures the password for the primary TACACS+ server. The CLI will prompt you for input. **Command mode:** Global configuration
`secondary-password` Configures the password for the secondary TACACS+ server. The CLI will prompt you for input. **Command mode:** Global configuration
`[no] tacacs-server command-authorization` Enables or disables TACACS+ command authorization. **Command mode:** Global configuration
`[no] tacacs-server command-logging` Enables or disables TACACS+ command logging. **Command mode:** Global configuration
`[no] tacacs-server directed-request` Enables or disables TACACS+ directed request, which uses a specified TACACS+ server for authentication, authorization, accounting. When enabled, When directed-request is enabled, each user must add a configured TACACS+ server hostname to the username (for example, `username@hostname`) during login. This command allows the following options: – Restricted: Only the username is sent to the specified TACACS+ server. – No-truncate: The entire login string is sent to the TACACS+ server. **Command mode:** Global configuration
`[no] tacacs-server accounting-enable` Enables or disables TACACS+ accounting. **Command mode:** Global configuration
`[no] tacacs-server enable` Enables or disables the TACACS+ server. By default, the server is disabled. **Command mode:** Global configuration

Table 88. TACACS+ Server Configuration Options (continued)

Command Syntax and Usage
`[no] tacacs-server enable-bypass` Enables or disables the enable-bypass for administrator privilege. By default, enable-bypass is enabled. **Command mode:** Global configuration
`show tacacs-server` Displays current TACACS+ configuration parameters. **Command mode:** All

LDAP Server Configuration

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

Table 89. LDAP Server Configuration Options

Command Syntax and Usage
[no] ldap-server primary-host <*IP address*> Sets the primary LDAP server address. **Command mode:** Global configuration
[no] ldap-server secondary-host <*IP address*> Sets the secondary LDAP server address. **Command mode:** Global configuration
[default] ldap-server port <*UDP port number*> Enter the number of the UDP port to be configured, between 1 - 65000. The default is 389. **Command mode:** Global configuration
ldap-server retransmit <*1-3*> Sets the number of failed authentication requests before switching to a different LDAP server. The default is 3 requests. **Command mode:** Global configuration
ldap-server timeout <*4-15*> Sets the amount of time, in seconds, before a LDAP server authentication attempt is considered to have failed. The default is 5 seconds. **Command mode:** Global configuration
ldap-server domain [<*1-128 characters*>|none] Sets the domain name for the LDAP server. Enter the full path for your organization. For example: ou=people,dc=mydomain,dc=com **Command mode:** Global configuration
[no] ldap-server backdoor Enables or disables the LDAP back door for Telnet, SSH/SCP, or HTTP/HTTPS. The default setting is disabled. To obtain the LDAP back door password for your G7028/G7052, contact your Service and Support line. **Command mode:** Global configuration

Table 89. LDAP Server Configuration Options (continued)

Command Syntax and Usage
`ldap-server enable` Enables the LDAP server. **Command mode:** Global configuration
`no ldap-server enable` Disables the LDAP server. **Command mode:** Global configuration
`show ldap-server` Displays the current LDAP server parameters. **Command mode:** All

NTP Server Configuration

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

Table 90. NTP Server Configuration Options

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

Table 90. NTP Server Configuration Options (continued)

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

System SNMP Configuration

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

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

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

SNMP parameters that can be modified include:

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

Table 91. System SNMP Options

Command Syntax and Usage
`snmp-server name` *<1-64 characters>* Configures the name for the system. The name can have a maximum of 64 characters. **Command mode:** Global configuration
`snmp-server location` *<1-64 characters>* Configures the name of the system location. The location can have a maximum of 64 characters. **Command mode:** Global configuration
`snmp-server contact` *<1-64 characters>* Configures the name of the system contact. The contact can have a maximum of 64 characters. **Command mode:** Global configuration
`snmp-server read-community` *<1-32 characters>* Configures the SNMP read community string. The read community string controls SNMP “get” access to the switch. It can have a maximum of 32 characters. The default read community string is *public*. **Command mode:** Global configuration

Table 91. System SNMP Options (continued)

Command Syntax and Usage
`[no] snmp-server read-community-additional` *<1-32 characters>* Adds or removes an additional SNMP read community string. Up to 7 additional read community strings are supported. **Command mode:** Global configuration
`[no] snmp-server write-community-additional` *<1-32 characters>* Adds or removes an additional SNMP write community string. Up to 7 additional write community strings are supported. **Command mode:** Global configuration
`snmp-server write-community` *<1-32 characters>* Configures the SNMP write community string. The write community string controls SNMP "set" and "get" access to the switch. It can have a maximum of 32 characters. The default write community string is *private*. **Command mode:** Global configuration
`snmp-server trap-source` *<interface number>* Configures the source interface for SNMP traps. **Command mode:** Global configuration
`snmp-server host` *<trap host IP address> <trap host community string>* Adds a trap host server. **Command mode:** Global configuration
`no snmp-server host` *<trap host IP address>* Removes the trap host server. **Command mode:** Global configuration
`snmp-server timeout` *<1-30>* Sets the timeout value for the SNMP state machine, in minutes. **Command mode:** Global configuration
`[no] snmp-server authentication-trap` Enables or disables the use of the system authentication trap facility. The default setting is `disabled`. **Command mode:** Global configuration
`[no] snmp-server link-trap` Enables or disables globally the sending of SNMP link up and link down traps. The default setting is `enabled`. **Command mode:** Global configuration

Table 91. System SNMP Options (continued)

Command Syntax and Usage
`[no] snmp-server link-trap port` *<port alias or number>* Enables or disables the sending of SNMP link up and link down traps for a specific system port. The default setting is `disabled`. **Command mode:** Global configuration
`show snmp-server` Displays the current SNMP configuration. **Command mode:** All

SNMPv3 Configuration

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

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

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

Table 92. SNMPv3 Configuration Options

Command Syntax and Usage
`snmp-server user` *<1-16>* This command allows you to create a user security model (USM) entry for an authorized user. You can also configure this entry through SNMP. **Command mode:** Global configuration To view command options, see page 152.
`snmp-server view` *<1-128>* This command allows you to create different MIB views. **Command mode:** Global configuration To view command options, see page 153.
`snmp-server access` *<1-32>* This command allows you to specify access rights. The View-based Access Control Model defines a set of services that an application can use for checking access rights of the user. You need access control when you have to process retrieval or modification request from an SNMP entity. **Command mode:** Global configuration To view command options, see page 154.

Table 92. SNMPv3 Configuration Options (continued)

`snmp-server group <1-16>` A group maps the user name to the access group names and their access rights needed to access SNMP management objects. A group defines the access rights assigned to all names that belong to a particular group. **Command mode:** Global configuration To view command options, see page 155.
`snmp-server community <1-16>` The community table contains objects for mapping community strings and version-independent SNMP message parameters. **Command mode:** Global configuration To view command options, see page 156.
`snmp-server target-address <1-16>` This command allows you to configure destination information, consisting of a transport domain and a transport address. This is also termed as transport endpoint. The SNMP MIB provides a mechanism for performing source address validation on incoming requests, and for selecting community strings based on target addresses for outgoing notifications. **Command mode:** Global configuration To view command options, see page 157.
`snmp-server target-parameters <1-16>` This command allows you to configure SNMP parameters, consisting of message processing model, security model, security level, and security name information. There may be multiple transport endpoints associated with a particular set of SNMP parameters, or a particular transport endpoint may be associated with several sets of SNMP parameters. **Command mode:** Global configuration To view command options, see page 158.
`snmp-server notify <1-16>` A notification application typically monitors a system for particular events or conditions, and generates Notification-Class messages based on these events or conditions. **Command mode:** Global configuration To view command options, see page 159.
`snmp-server version {v1v2v3|v3only}` This command allows you to enable or disable the access to SNMP versions 1, 2 or 3. This command is enabled by default. **Command mode:** Global configuration
`show snmp-server v3` Displays the current SNMPv3 configuration. **Command mode:** All

User Security Model Configuration

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

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

Table 93. User Security Model Configuration Options

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

Table 93. User Security Model Configuration Options

Command Syntax and Usage
`no snmp-server user <1-16>` Deletes the USM user entries. **Command mode:** Global configuration
`show snmp-server v3 user <1-16>` Displays the USM user entries. **Command mode:** All

SNMPv3 View Configuration

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

Table 94. SNMPv3 View Configuration Options

Command Syntax and Usage
`snmp-server view <1-128> name <1-32 characters>` This command defines the name for a family of view subtrees. **Command mode:** Global configuration
`snmp-server view <1-128> tree <1-64 characters>` This command defines MIB tree, which when combined with the corresponding mask defines a family of view subtrees. **Command mode:** Global configuration
`[no] snmp-server view <1-128> mask <1-32 characters>` This command defines the bit mask, which in combination with the corresponding tree defines a family of view subtrees. **Command mode:** Global configuration
`snmp-server view <1-128> type {included|excluded}` This command indicates whether the corresponding instances of `vacmViewTreeFamilySubtree` and `vacmViewTreeFamilyMask` define a family of view subtrees, which is included in or excluded from the MIB view. **Command mode:** Global configuration
`no snmp-server view <1-128>` Deletes the `vacmViewTreeFamily` group entry. **Command mode:** Global configuration
`show snmp-server v3 view <1-128>` Displays the current `vacmViewTreeFamily` configuration. **Command mode:** All

View-based Access Control Model Configuration

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

Table 95. View-based Access Control Model Options

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

SNMPv3 Group Configuration

Table 96. SNMPv3 Group Configuration Options

Command Syntax and Usage
`snmp-server group <1-16> security {usm|snmpv1|snmpv2}` Defines the security model. **Command mode:** Global configuration
`snmp-server group <1-16> user-name <1-32 characters>` Sets the user name as defined in the following command on page 152: `snmp-server user <1-16> name <1-32 characters>` **Command mode:** Global configuration
`snmp-server group <1-16> group-name <1-32 characters>` The name for the access group as defined in the following command: `snmp-server access <1-32> name <1-32 characters>` on page 152. **Command mode:** Global configuration
`no snmp-server group <1-16>` Deletes the `vacmSecurityToGroup` entry. **Command mode:** Global configuration
`show snmp-server v3 group <1-16>` Displays the current `vacmSecurityToGroup` configuration. **Command mode:** All

SNMPv3 Community Table Configuration

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

Table 97. SNMPv3 Community Table Configuration Options

Command Syntax and Usage
`snmp-server community <1-16> index <1-32 characters>` Allows you to configure the unique index value of a row in this table. **Command string:** Global configuration
`snmp-server community <1-16> name <1-32 characters>` Defines the user name as defined in the following command on page 152: `snmp-server user <1-16> name <1-32 characters>` **Command string:** Global configuration
`snmp-server community <1-16> user-name <1-32 characters>` Defines a readable string that represents the corresponding value of an SNMP community name in a security model. **Command mode:** Global configuration
`snmp-server community <1-16> tag <1-255 characters>` Allows you to configure a tag. This tag specifies a set of transport endpoints to which a command responder application sends an SNMP trap. **Command mode:** Global configuration
`no snmp-server community <1-16>` Deletes the community table entry. **Command mode:** Global configuration
`show snmp-server v3 community <1-16>` Displays the community table configuration. **Command mode:** All

SNMPv3 Target Address Table Configuration

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

Table 98. Target Address Table Configuration Options

Command Syntax and Usage
`snmp-server target-address` *<1-16>* `address` *<IP address>* `name` *<1-32 characters>* Allows you to configure the locally arbitrary, but unique identifier, target address name associated with this entry. **Command mode:** Global configuration
`snmp-server target-address` *<1-16>* `name` *<1-32 characters>* `address` *<transport IP address>* Configures a transport IPv4 or IPv6 address that can be used in the generation of SNMP traps. IPv6 addresses are not displayed in the configuration, but they do receive traps. **Command mode:** Global configuration
`snmp-server target-address` *<1-16>* `port` *<port range>* Allows you to configure a transport address port that can be used in the generation of SNMP traps. **Command mode:** Global configuration
`snmp-server target-address` *<1-16>* `taglist` *<1-255 characters>* Allows you to configure a list of tags that are used to select target addresses for a particular operation. **Command mode:** Global configuration
`snmp-server target-address` *<1-16>* `parameters-name` *<1-32 characters>* Defines the name as defined in the following command on page 158: `snmp-server target-parameters` *<1-16>* `name` *<1-32 characters>* **Command mode:** Global configuration
`no snmp-server target-address` *<1-16>* Deletes the Target Address Table entry. **Command mode:** Global configuration
`show snmp-server v3 target-address` *<1-16>* Displays the current Target Address Table configuration. **Command mode:** All

SNMPv3 Target Parameters Table Configuration

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

Table 99. Target Parameters Table Configuration Options

Command Syntax and Usage
`snmp-server target-parameters` *<1-16>* `name` *<1-32 characters>* Allows you to configure the locally arbitrary, but unique, identifier that is associated with this entry. **Command mode:** Global configuration
`snmp-server target-parameters` *<1-16>* `message {snmpv1|snmpv2c|snmpv3}` Allows you to configure the message processing model that is used to generate SNMP messages. **Command mode:** Global configuration
`snmp-server target-parameters` *<1-16>* `security {usm|snmpv1|snmpv2}` Allows you to select the security model to be used when generating the SNMP messages. **Command mode:** Global configuration
`snmp-server target-parameters` *<1-16>* `user-name` *<1-32 characters>* Defines the name that identifies the user in the USM table (page 152) on whose behalf the SNMP messages are generated using this entry. **Command mode:** Global configuration
`snmp-server target-parameters` *<1-16>* `level {noAuthNoPriv|authNoPriv|authPriv}` Allows you to select the level of security to be used when generating the SNMP messages using this entry. The level `noAuthNoPriv` means that the SNMP message will be sent without authentication and without using a privacy protocol. The level `authNoPriv` means that the SNMP message will be sent with authentication but without using a privacy protocol. The `authPriv` means that the SNMP message will be sent both with authentication and using a privacy protocol. **Command mode:** Global configuration
`no snmp-server target-parameters` *<1-16>* Deletes the `targetParamsTable` entry. **Command mode:** Global configuration
`show snmp-server v3 target-parameters` *<1-16>* Displays the current `targetParamsTable` configuration. **Command mode:** All

SNMPv3 Notify Table Configuration

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

Table 100. Notify Table Options

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

System Access Configuration

Table 101. System Access Configuration Options

Command Syntax and Usage
`access user user-password` Sets the user (`user`) password. The user has no direct responsibility for switch management. The user view switch status information and statistics, but cannot make any configuration changes. This command will prompt for required information: current admin password, new password (up to 128 characters) and confirmation of the new password. **Note:** To disable the user account, set the password to null (no password). **Command Mode**: Global configuration
`access user operator-password` Sets the operator (`oper`)password. The operator manages all functions of the switch. The operator can view all switch information and statistics and can reset ports. This command will prompt for required information: current admin password, new password (up to 128 characters) and confirmation of the new password. **Note:** To disable the operator account, set the password to null (no password). The default setting is disabled (no password). **Command Mode**: Global configuration
`access user administrator-password` Sets the administrator (`admin`) password. The administrator has complete access to all menus, information, and configuration commands on the G7028/G7052, including the ability to change both the user and administrator passwords. This command will prompt for required information: current admin password, new password (up to 128 characters) and confirmation of the new password. Access includes "`oper`" functions. **Note:** You cannot disable the administrator password. **Command Mode**: Global configuration
`[no] access http enable` Enables or disables HTTP (Web) access to the Browser-Based Interface. It is enabled by default. **Command mode:** Global configuration
`[default] access http port [`<*port alias or number*>`]` Sets the switch port used for serving switch Web content. The default is HTTP port 80. **Command mode:** Global configuration

Table 101. System Access Configuration Options (continued)

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

Management Network Configuration

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

Table 102. Management Network Configuration Options

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

User Access Control Configuration

The following table describes user-access control commands.

Passwords can be a maximum of 128 characters.

Table 103. User Access Control Configuration Options

Command Syntax and Usage
`access user` *<1-10>* Configures the User ID. **Command mode:** Global configuration
`access user eject` {*<user name>*|*<session ID>*} Ejects the specified user from the G7028. **Command mode:** Global configuration

Table 103. User Access Control Configuration Options

Command Syntax and Usage
`clear line <1-12>` Ejects the user with the corresponding session ID from the G7028/G7052. **Command mode:** Privileged EXEC
`[no] access user administrator-enable` Enables or disables the default administrator account. **Command mode:** Global configuration
`access user user-password` Sets the user (`user`) password. This command will prompt for required information: current admin password, new password (up to 128 characters) and confirmation of the new password. **Command mode:** Global configuration
`access user operator-password` Sets the operator (`oper`) password. This command will prompt for required information: current admin password, new password (up to 128 characters) and confirmation of the new password. **Command mode:** Global configuration
`access user administrator-password` Sets the administrator (`admin`) password. This command will prompt for required information: current admin password, new password (up to 128 characters) and confirmation of the new password. Access includes "`oper`" functions. **Command mode:** Global configuration
`show access user` Displays the current user status. **Command mode:** All except User EXEC

System User ID Configuration

Table 104. User ID Configuration Options

Command Syntax and Usage
`access user <1-10> level {user|operator|administrator}` Sets the Class-of-Service to define the user's authority level. IBM N/OS defines these levels as: User, Operator, and Administrator, with User being the most restricted level. **Command mode:** Global configuration
`access user <1-10> name <1-64 characters>` Defines the user name of maximum eight characters. **Command mode:** Global configuration
`access user <1-10> password` Sets the user (`user`) password. This command will prompt for required information: current admin password, new password (up to 128 characters) and confirmation of the new password. **Command mode:** Global configuration
`access user <1-10> enable` Enables the user ID. **Command mode:** Global configuration
`no access user <1-10> enable` Disables the user ID. **Command mode:** Global configuration
`no access user <1-10>` Deletes the user ID. **Command mode:** Global configuration
`show access user` Displays the current user ID configuration. **Command mode:** All except User EXEC

Strong Password Configuration

Table 105. Strong Password Configuration Options

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

HTTPS Access Configuration

Table 106. HTTPS Access Configuration Options

Command Syntax and Usage
`[no] access https enable` Enables or disables BBI access (Web access) using HTTPS. **Command mode:** Global configuration
`[default] access https port [<`*TCP port number*`>]` Defines the HTTPS Web server port number. The default port is 443. **Command mode:** Global configuration
`access https generate-certificate` Allows you to generate a certificate to connect to the SSL to be used during the key exchange. A default certificate is created when HTTPS is enabled for the first time. The user can create a new certificate defining the information that they want to be used in the various fields. For example: – Country Name (2 letter code): CA – State or Province Name (full name): Ontario – Locality Name (for example, city): Ottawa – Organization Name (for example, company): IBM – Organizational Unit Name (for example, section): Operations – Common Name (for example, user's name): Mr Smith – Email (for example, email address): info@ibm.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:** Global configuration
`access https save-certificate` Allows the client, or the Web browser, to accept the certificate and save the certificate to Flash to be used when the switch is rebooted. **Command mode:** Global configuration
`show access` Displays the current SSL Web Access configuration. **Command mode:** All except User EXEC

Custom Daylight Saving Time Configuration

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

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

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

Table 107. Custom DST Options

Command Syntax and Usage

`system custom-dst start-rule <WDDMMhh>`
Configures the start date for custom DST, as follows:
`WDMMhh`
W = week (0-5, where 0 means use the calendar date)
D = day of the week (01-07, where 01 is Monday)
MM = month (1-12)
hh = hour (0-23)
Note: Week 5 is always considered to be the last week of the month.
Command mode: Global configuration

`system custom-dst end-rule <WDDMMhh>`
Configures the end date for custom DST, as follows:
`WDMMhh`
W = week (0-5, where 0 means use the calendar date)
D = day of the week (01-07, where 01 is Monday)
MM = month (1-12)
hh = hour (0-23)
Note: Week 5 is always considered to be the last week of the month.
Command mode: Global configuration

`system custom-dst enable` Enables the Custom Daylight Saving Time settings. **Command mode:** Global configuration
`no system custom-dst enable` Disables the Custom Daylight Saving Time settings. **Command mode:** Global configuration
`show custom-dst` Displays the current Custom DST configuration. **Command mode:** All except User EXEC

Port Configuration

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

Table 108. Port Configuration Options

Command Syntax and Usage
`interface port` *<port alias or number>* Enter Interface port mode. **Command mode:** Global configuration
`interface portchannel` *<trunk number>*`|lacp` *<1-65535>* Enter Interface portchannel mode. These commands allow you to configure port parameters for all port members in the selected trunk group (portchannel). **Command mode:** Global configuration
`dot1p` *<0-7>* Configures the port's 802.1p priority level. **Command mode:** Interface port/Interface portchannel
`description` *<1-64 characters>* Sets a description for the port. The assigned port description appears next to the port number on some information and statistics screens. The default is set to the port number. **Command mode:** Interface port/Interface portchannel
`[no] bpdu-guard` Enables or disables BPDU guard, to avoid Spanning-Tree loops on ports configured as `edge` ports. **Command mode:** Interface port/Interface portchannel
`[no] dscp-marking` Enables or disables DSCP re-marking on a port. **Command mode:** Interface port/Interface portchannel
`switchport mode private-vlan {host|promiscuous|trunk promiscuous|trunk secondary}` Configures port behavior when associated to a private VLAN. Private VLANs allow definition of VLAN sub-domains within a primary VLAN domain, usually for the purpose of enabling Layer 2 partitioning over a single Layer 3 subnet. – `host` ports are associated to a secondary VLAN within the private VLAN – `promiscuous` ports are associated to the primary VLAN within the private VLAN. – `trunk promiscuous` ports behave like promiscuous ports within the private VLAN domain, but can also belong to regular VLANs. – `trunk secondary` ports behave like secondary isolated ports within the private VLAN domain, but can also belong to regular VLANs. Default mode is `access`. **Command mode:** Interface port/Interface portchannel

Table 108. Port Configuration Options (continued)

Command Syntax and Usage
`switchport access vlan` *<1-4094>* Configures the associated VLAN used in access mode. If the VLAN does not exist, it will be created and enabled automatically. Default value is 1 for data ports and 4095 for the management port. **Command mode:** Interface port/Interface portchannel
`no switchport access vlan` Resets the access VLAN to its default value. **Command mode:** Interface port/Interface portchannel
`switchport trunk native vlan` *<1-4094>* Configures the Port VLAN ID (PVID) or Native-VLAN used to carry untagged traffic in trunk mode. If the VLAN does not exist, it will be created and enabled automatically. Default value is 1 for data ports and 4095 for the management port. **Command mode:** Interface port/Interface portchannel
`switchport trunk allowed vlan [add|remove]` *<VLAN ID range>* Updates the associated VLANs in trunk mode.If any VLAN in the range does not exist, it will be created and enabled automatically. – `add` enables the VLAN range in addition to the current configuration – `remove` eliminates the VLAN range from the current configuration **Command mode:** Interface port/Interface portchannel
`switchport trunk allowed vlan {all|none}` – `all` associates all existing and enabled VLANs to the port. This is an operational command applicable only to VLANs currently configured at the moment of execution. VLANs created afterward will not be associated automatically. Also, as an operational command, it will not be dumped into the configuration file. – `none` removes the port from all currently associated VLANS except the default VLAN **Command mode:** Interface port/Interface portchannel
`[no] switchport private-vlan mapping` *<primary VLAN>* Enables or disables private VLAN mapping on a port in promiscuous mode. **Command mode:** Interface port/Interface portchannel
`[no] switchport private-vlan association` *<primary VLAN> <secondary VLAN>* Enables or disables the private VLAN association on a secondary port. **Command mode:** Interface port/Interface portchannel

Table 108. Port Configuration Options (continued)

Command Syntax and Usage
`[no] vlan dot1q tag native` Disables or enables VLAN tag persistence. When disabled, the VLAN tag is removed at egress from packets whose VLAN tag matches the port PVID/Native-vlan. The default setting is `disabled`. **Note:** In global configuration mode, this is an operational command used to set the VLAN tag persistence on all ports currently tagged at the moment of execution. VLAN tag persistence will not be set automatically for ports tagged afterwords. Also, as an operational command, it will not be dumped into the configuration file. **Command mode:** Global configuration/Interface port/Interface portchannel
`[no] flood-blocking` Enables or disables port Flood Blocking. When enabled, unicast and multicast packets with unknown destination MAC addresses are blocked from the port. **Command mode:** Interface port/Interface portchannel
`[no] mac-address-table mac-notification` Enables or disables MAC Address Notification. With MAC Address Notification enabled, the switch generates a syslog message when a MAC address is added or removed from the MAC address table. **Command mode:** Interface port/Interface portchannel
`[no] learning` Enables or disables FDB learning on the port. **Command mode:** Interface port/Interface portchannel
`port-channel min-links` *<1-8>* Set the minimum number of links for this port. If the specified minimum number of ports are not available, the trunk is placed in the `down` state. **Command mode:** Interface port
`storm-control {broadcast|multicast|unicast} level pps` Limits the number of broadcast, multicast or unicast packets per second to the specified value. **Command mode:** Interface port/Interface portchannel
`no storm-control {broadcast|multicast|unicast}` Sets the port to forward all broadcast, multicast or unicast packets. **Command mode:** Interface port/Interface portchannel
`no shutdown` Enables the port. **Command mode:** Interface port/Interface portchannel
`shutdown` Disables the port. (To temporarily disable a port without changing its configuration attributes, refer to "Temporarily Disabling a Port" on page 174.) **Command mode:** Interface port/Interface portchannel

Table 108. Port Configuration Options (continued)

Command Syntax and Usage
`show interface port` <*port alias or number*> Displays current port parameters. **Command mode:** All

Port Error Disable and Recovery Configuration

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

Table 109. Port Error Disable Options

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

Port Link Flap Dampening Configuration

Table 110. Port Link Flap Dampening Configuration Options

Command Syntax and Usage
`errdisable link-flap enable` Enables Link Flap Dampening on the port. For more information, see "Link Flap Dampening Configuration" on page 134. **Command mode:** Interface port
`no errdisable link-flap enable` Disables Link Flap Dampening on the port. **Command mode:** Interface port
`show interface port errdisable` *<port alias or number>* `link-flap` Displays the current Link Flap Dampening parameters for the port. **Command mode:** All

Port Link Configuration

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

Table 111. Port Link Configuration Options

Command Syntax and Usage
`speed {10|100|1000|auto}` Sets the link speed. Some options are not valid on all ports. The choices include: – 10 Mbps – 100 Mbps – 1000 Mbps – any (auto negotiate port speed) **Command mode:** Interface port/Interface portchannel
`duplex {full|half|auto}` Sets the operating mode. The choices include: – “Auto negotiation (default) – Half-duplex – Full-duplex **Note**: Data ports are fixed at full duplex. **Command mode:** Interface port/Interface portchannel
`flowcontrol receive {on|off}` Enables or disables flow control receive. **Command mode:** Interface port/Interface portchannel
`flowcontrol send {on|off}` Enables or disables flow control transmit. **Command mode:** Interface port/Interface portchannel
`[no] auto` Turns auto-negotiation on or off. **Note**: Data ports are fixed at 10000 Mbps, and cannot be set to auto-negotiate, unless a 1 Gb SFP transceiver is used. **Command mode:** Interface port/Interface portchannel
`show interface port` *<port alias or number>* Displays current port parameters. **Command mode:** All

Temporarily Disabling a Port

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

```
RS G7028(config)# interface port <port alias or number> shutdown
```

Because this configuration sets a temporary state for the port, you do not need to use a save operation. The port state will revert to its original configuration when the G7028/G7052 is reset. See the "Operations Commands" on page 249 for other operations-level commands.

UniDirectional Link Detection Configuration

UDLD commands are described in the following table.

Table 112. Port UDLD Configuration Options

Command Syntax and Usage
`[no] udld` Enables or disables UDLD on the port. **Command mode:** Interface port
`[no] udld aggressive` Configures the UDLD mode for the selected port, as follows: – **Normal**: Detect unidirectional links that have mis-connected interfaces. The port is disabled if UDLD determines that the port is mis-connected. Use the "no" form to select normal operation. – **Aggressive**: In addition to the normal mode, the aggressive mode disables the port if the neighbor stops sending UDLD probes for 7 seconds. **Command mode:** Interface port
`show interface port <port number> udld` Displays current port UDLD parameters. **Command mode:** All

Port ACL Configuration

Table 113. ACL/QoS Configuration Options

Command Syntax and Usage
`access-control list` <*ACL number*> Adds the specified ACL to the port. You can add multiple ACLs to a port, but the total number of precedence levels allowed is two. **Command mode:** Interface port/Interface portchannel
`no access-control list` <*ACL number*> Removes the specified ACL list from the port. **Command mode:** Interface port/Interface portchannel
`access-control list6` <*ACL number*> Adds the specified IPv6 ACL to the port. You can add multiple ACLs to a port, but the total number of precedence levels allowed is two. **Command mode:** Interface port/Interface portchannel
`no access-control list6` <*ACL number*> Removes the specified IPv6 ACL list from the port. **Command mode:** Interface port/Interface portchannel
`access-control group` <*ACL group number*> Adds the specified ACL group to the port. You can add multiple ACL groups to a port, but the total number of precedence levels allowed is two. **Command mode:** Interface port/Interface portchannel
`no access-control group` <*ACL group number*> Removes the specified ACL group from the port. **Command mode:** Interface port/Interface portchannel
`show interface port` <*port alias or number*> `access-control` Displays current ACL QoS parameters. **Command mode:** All

Quality of Service Configuration

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

802.1p Configuration

This feature provides the G7028/G7052 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 114. 802.1p Configuration Options

Command Syntax and Usage
`qos transmit-queue mapping` *<priority (0-7)> <COSq number>* Maps the 802.1p priority of to the Class of Service queue (COSq) priority. Enter the 802.1p priority value (0-7), followed by the Class of Service queue that handles the matching traffic. **Command mode:** Global configuration
`qos transmit-queue weight-cos` *<COSq number> <weight (0-15)>* Configures the weight of the selected Class of Service queue (COSq). Enter the queue number (0-1), followed by the scheduling weight (0-15). **Command mode:** Global configuration
`qos transmit-queue number-cos {2|8}` Sets the number of Class of Service queues (COSq) for switch ports. Depending on the `numcos` setting, the valid COSq range for the `priq` and `qweight` commands is as follows: – If `numcos` is 2 (the default), the COSq range is 0-1. – If `numcos` is 8, the COSq range is 0-7. You must apply, save, and reset the switch to activate the new configuration. **Command mode:** Global configuration
`show qos transmit-queue` Displays the current 802.1p parameters. **Command mode:** All

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 115. DSCP Configuration Options

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

Control Plane Protection

These commands allow you to limit the number of selected protocol packets received by the control plane (CP) of the switch. These limits help protect the CP from receiving too many protocol packets in a given time period.

Table 116. Control Plane Protection Options

Command Syntax and Usage
`qos protocol-packet-control packet-queue-map` *<packet queue number (0-47)> <packet type>* Configures a packet type to associate with each packet queue number. Enter a queue number, followed by the packet type. You may map multiple packet types to a single queue. The following packet types are allowed: – **802.1x** (IEEE 802.1x packets) – **application-cri-packets** (critical packets of various applications, such as telnet,ssh) – **arp-bcast** (ARP broadcast packets) – **arp-ucast** (ARP unicast reply packets) – **bpdu** (Spanning Tree Protocol packets) – **cisco-bpdu** (Cisco STP packets) – **dest-unknown** (packets with destination not yet learned) – **dhcp** (DHCP packets) – **icmp** (ICMP packets) – **igmp** (IGMP packets) – **ipv4-miscellaneous** (IPv4 packets with IP options and TTL exception) – **ipv6-nd** (IPv6 Neighbor Discovery packets) – **lacp** (LACP/Link Aggregation protocol packets) – **lldp** (LLDP packets) – **system** (system protocols, such as tftp, ftp, telnet, ssh) – **udld** (UDLD packets) **Command mode:** Global configuration
`qos protocol-packet-control rate-limit-packet-queue` *<packet queue number (0-47)> <1-10000>* Configures the number of packets per second allowed for each packet queue. **Command mode:** Global configuration
`no qos protocol-packet-control packet-queue-map` *<packet type>* Clears the selected packet type from its associated packet queue. **Command mode:** Global configuration
`no qos protocol-packet-control rate-limit-packet-queue` *<packet queue number (0-47)>* Clears the packet rate configured for the selected packet queue. **Command mode:** Global configuration

Table 116. Control Plane Protection Options (continued)

Command Syntax and Usage
`show qos protocol-packet-control information protocol` Displays of mapping of protocol packet types to each packet queue number. The status indicates whether the protocol is running or not running. **Command mode:** All
`show qos protocol-packet-control information queue` Displays the packet rate configured for each packet queue. **Command mode:** All

Access Control Configuration

Use these commands to create Access Control Lists. ACLs define matching criteria used for IP filtering and Quality of Service functions.

For information about assigning ACLs to ports, see “Port ACL Configuration” on page 175.

Table 117. General ACL Configuration Options

Command Syntax and Usage
[no] access-control list <1-512> Configures an Access Control List. To view command options, see page 181. **Command mode:** Global configuration
[no] access-control list6 <1-47> Configures an Access Control List. To view command options, see page 186. **Command mode:** Global configuration
[no] access-control macl <1-128> Configures an Access Control List. To view command options, see page 181. **Command mode:** Global configuration
show access-control Displays the current ACL parameters. **Command mode:** All

Access Control List Configuration

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

Table 118. ACL Configuration Options

Command Syntax and Usage
`access-control list <1-512> action {permit|deny|set-priority <0-7>}` Configures a filter action for packets that match the ACL definitions. You can choose to permit (pass) or deny (drop) packets, or set the 802.1p priority level (0-7). **Command mode:** Global configuration
`[no] access-control list <1-512> statistics` Enables or disables the statistics collection for the Access Control List. **Command mode:** All except User EXEC
`[no] access-control list <1-512> log` Enables or disables logging for the Access Control List. **Note**: Enabling the LOG feature neutralizes ACL deny filter actions for Telnet and SSH traffic that is addressed to the switch's Layer 3 interfaces. **Command mode:** Global configuration
`default access-control list <1-512>` Resets the ACL parameters to their default values. **Command mode:** Global configuration
`show access-control list <1-512>` Displays the current ACL parameters. **Command mode:** All

ACL Mirroring Configuration

These commands allow you to define port mirroring for an ACL. Packets that match the ACL are mirrored to the destination interface.

Table 119. ACL Port Mirroring Options

Command Syntax and Usage
`[no] access-control list <1-512> mirror port <port alias or number>|none` Configures the destination to which packets that match this ACL are mirrored. **Command mode:** Global configuration
`show access-control list <1-512> mirror` Displays the current port mirroring parameters for the ACL. **Command mode:** All

Ethernet Filtering Configuration

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

Table 120. Ethernet Filtering Configuration Options

Command Syntax and Usage
[no] access-control list <*1-512*> ethernet source-mac-address <*MAC address*> <*MAC mask*> Defines the source MAC address for this ACL. **Command mode:** Global configuration
[no] access-control list <*1-512*> ethernet destination-mac-address <*MAC address*> <*MAC mask*> Defines the destination MAC address for this ACL. **Command mode:** Global configuration
[no] access-control list <*1-512*> ethernet vlan <*VLAN ID*> <*VLAN mask*> Defines a VLAN number and mask for this ACL. **Command mode:** Global configuration
[no] access-control list <*1-512*> ethernet ethernet-type {arp|ip|ipv6|mpls|rarp|any|<*other (0x600-0xFFFF)*>} Defines the Ethernet type for this ACL. **Command mode:** Global configuration
[no] access-control list <*1-512*> ethernet priority <*0-7*> Defines the Ethernet priority value for the ACL. **Command mode:** Global configuration
default access-control list <*1-512*> ethernet Resets Ethernet parameters for the ACL to their default values. **Command mode:** Global configuration
no access-control list <*1-512*> ethernet Removes Ethernet parameters for the ACL. **Command mode:** Global configuration
show access-control list <*1-512*> ethernet Displays the current Ethernet parameters for the ACL. **Command mode:** All

IPv4 Filtering Configuration

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

Table 121. IP version 4 Filtering Configuration Options

Command Syntax and Usage
[no] access-control list <*1-512*> ipv4 source-ip-address <*IP address*> <*IP mask*> Defines a source IP address for the ACL. If defined, traffic with this source IP address will match this ACL. Specify an IP address in dotted decimal notation. **Command mode:** Global configuration
[no] access-control list <*1-512*> ipv4 destination-ip-address <*IP address*> <*IP mask*> Defines a destination IP address for the ACL. If defined, traffic with this destination IP address will match this ACL. **Command mode:** Global configuration
[no] access-control list <*1-512*> ipv4 protocol <*0-255*> Defines an IP protocol for the ACL. If defined, traffic from the specified protocol matches this filter. Specify the protocol number. Listed below are some of the well-known protocols. **Number** **Name** 1 icmp 2 igmp 6 tcp 17 udp **Command mode:** Global configuration
[no] access-control list <*1-512*> ipv4 type-of-service <*0-255*> Defines a Type of Service (ToS) value for the ACL. For more information on ToS, refer to RFC 1340 and 1349. **Command mode:** Global configuration
default access-control list <*1-512*> ipv4 Resets the IPv4 parameters for the ACL to their default values. **Command mode:** Global configuration
show access-control list <*1-512*> ipv4 Displays the current IPv4 parameters. **Command mode:** All

TCP/UDP Filtering Configuration

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

Table 122. TCP/UDP Filtering Configuration Options

Command Syntax and Usage
[no] access-control list <*1-512*> tcp-udp source-port <*1-65535*> <*mask (0xFFFF)*> Defines a source port for the ACL. If defined, traffic with the specified TCP or UDP source port will match this ACL. Specify the port number. Listed here are some of the well-known ports: **Number** **Name** 20 ftp-data 21 ftp 22 ssh 23 telnet 25 smtp 37 time 42 name 43 whois 53 domain 69 tftp 70 gopher 79 finger 80 http **Command mode:** Global configuration
[no] access-control list <*1-512*> tcp-udp destination-port <*1-65535*> <*mask (0xFFFF)*> Defines a destination port for the ACL. If defined, traffic with the specified TCP or UDP destination port will match this ACL. Specify the port number, just as with source-port. **Command mode:** Global configuration
[no] access-control list <*1-512*> tcp-udp flags <*value (0x0-0x3f)*> <*mask (0x0-0x3f)*> Defines a TCP/UDP flag for the ACL. **Command mode:** Global configuration
default access-control list <*1-512*> tcp-udp Resets the TCP/UDP parameters for the ACL to their default values. **Command mode:** Global configuration
show access-control list <*1-512*> tcp-udp Displays the current TCP/UDP Filtering parameters. **Command mode:** All

ACL Metering Configuration

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

Table 123. ACL Metering Configuration Options

Command Syntax and Usage
`access-control list <1-512> meter committed-rate` Configures the committed rate, in per second. The committed rate must be a multiple of 64. **Command mode:** Global configuration
`access-control list <1-512> meter maximum-burst-size <32-4096>` Configures the maximum burst size, in kilobits. Enter one of the following values for `mbsize`: 32, 64, 128, 256, 512, 1024, 2048, 4096 **Command mode:** Global configuration
`[no] access-control list <1-512> meter enable` Enables or disables ACL Metering. **Command mode:** Global configuration
`default access-control list <1-512> meter` Sets the ACL meter configuration to its default values. **Command mode:** Global configuration
`no access-control list <1-512> meter` Deletes the selected ACL meter. **Command mode:** Global configuration
`show access-control list <1-512> meter` Displays current ACL Metering parameters. **Command mode:** All

ACL Re-Mark Configuration

You can choose to re-mark IP header data for the selected ACL. 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 124. ACL Re-Marking In-Profile Options

Command Syntax and Usage
`[no] access-control list <1-512> re-mark in-profile dot1p <0-7>` Re-marks the 802.1p value. The value is the priority bits information in the packet structure. **Command mode:** Global configuration
`[no] no access-control list <1-512> re-mark in-profile dscp <0-63>` Remarks the DSCP value for in-profile traffic. **Command mode:** Global configuration
`[no] no access-control list <1-512> re-mark use-tos-precedence` Enables or disables mapping of TOS (Type of Service) priority to 802.1p priority for in-profile packets. When enabled, the TOS value is used to set the 802.1p value. **Command mode:** Global configuration
`default access-control list <1-512> re-mark` Sets the ACL re-mark parameters to their default values. **Command mode:** Global configuration
`show access-control list <1-512> re-markS` Displays current re-mark parameters. **Command mode:** All

ACL IPv6 Configuration

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

Table 125. IPv6 ACL Options

Command Syntax and Usage
`access-control list6 <1-128> action {permit|deny|set-priority <0-7>}` Configures a filter action for packets that match the ACL definitions. You can choose to permit (pass) or deny (drop) packets, or set the 802.1p priority level (0-7). **Command mode:** Global configuration
`[no] access-control list6 <1-128> statistics` Enables or disables the statistics collection for the Access Control List. **Command mode:** Global configuration

Table 125. IPv6 ACL Options

Command Syntax and Usage
`[no] access-control list6 <1-128> log` Enables or disables Access Control List logging.
`default access-control list6 <1-128>` Resets the ACL parameters to their default values. **Command mode:** Global configuration
`show access-control list6 <1-128>` Displays the current ACL parameters. **Command mode:** All

IP version 6 Filtering Configuration

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

Table 126. IP version 6 Filtering Options

Command Syntax and Usage
[no] access-control list6 <*1-47*> ipv6 source-address <*IPv6 address*> <*prefix length (1-128)*> Defines a source IPv6 address for the ACL. If defined, traffic with this source address will match this ACL. **Command mode:** Global configuration
[no] access-control list6 <*1-47*> ipv6 destination-address <*IPv6 address*> <*prefix length (1-128)*> Defines a destination IPv6 address for the ACL. If defined, traffic with this destination address will match this ACL. **Command mode:** Global configuration
[no] access-control list6 <*1-47*> ipv6 next-header <*0-255*> Defines the next header value for the ACL. If defined, traffic with this next header value will match this ACL. **Command mode:** Global configuration
[no] access-control list6 <*1-47*> ipv6 flow-label <*0-1048575*> Defines the flow label for the ACL. If defined, traffic with this flow label will match this ACL. **Command mode:** Global configuration
[no] access-control list6 <*1-47*> ipv6 traffic-class <*0-255*> Defines the traffic class for the ACL. If defined, traffic with this traffic class will match this ACL. **Command mode:** Global configuration
default access-control list6 <*1-47*> ipv6 Resets the IPv6 parameters for the ACL to their default values. **Command mode:** Global configuration
show access-control list6 <*1-47*> ipv6 Displays the current IPv6 parameters. **Command mode:** All

IPv6 TCP/UDP Filtering Configuration

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

Table 127. IPv6 ACL TCP/UDP Filtering Options

Command Syntax and Usage
[no] access-control list6 <*1-47*> tcp-udp source-port <*1-65535*> <*mask (0xFFFF)*> Defines a source port for the ACL. If defined, traffic with the specified TCP or UDP source port will match this ACL. Specify the port number. Listed here are some of the well-known ports: **Number** **Name** 20 ftp-data 21 ftp 22 ssh 23 telnet 25 smtp 37 time 42 name 43 whois 53 domain 69 tftp 70 gopher 79 finger 80 http **Command mode:** Global configuration
[no] access-control list6 <*1-47*> tcp-udp destination-port <*1-65535*> <*mask (0xFFFF)*> Defines a destination port for the ACL. If defined, traffic with the specified TCP or UDP destination port will match this ACL. Specify the port number, just as with sport above. **Command mode:** Global configuration
[no] access-control list6 <*1-47*> tcp-udp flags <*value (0x0-0x3f)*> <*mask (0x0-0x3f)*> Defines a TCP/UDP flag for the ACL. **Command mode:** Global configuration
default access-control list6 <*1-47*> tcp-udp Resets the TCP/UDP parameters for the ACL to their default values. **Command mode:** Global configuration
show access-control list6 <*1-47*> tcp-udp Displays the current TCP/UDP Filtering parameters. **Command mode:** All

IPv6 Re-Mark Configuration

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

IPv6 Re-Marking In-Profile Configuration

Table 128. IPv6 Re-Marking In-Profile Options

Command Syntax and Usage
`[no] access-control list6 <1-47> re-mark dot1p <0-7>` Re-marks the 802.1p value. The value is the priority bits information in the packet structure. **Command mode:** Global configuration
`[no] access-control list6 <1-47> re-mark in-profile dscp <0-63>` Re-marks the DSCP value for in-profile traffic. **Command mode:** Global configuration
`default access-control list6 <1-47> re-mark` Sets the ACL re-mark parameters to their default values. **Command mode:** Global configuration
`show access-control list6 <1-47> re-mark` Displays current re-mark parameters. **Command mode:** All

ACL Log Configuration

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

Table 129. ACL Log Configuration Options

Command Syntax and Usage
`access-control list <1-512> log` Enables access control list logging. **Command mode:** Global configuration
`access-control log interval <seconds>` Sets the filter log displaying interval in seconds. **Command mode:** Global configuration
`access-control log rate-limit <seconds>` Sets the filter log queue rate limit in seconds. **Command mode:** Global configuration
`default access-control log [interval | rate-lmt]` Resets the specified filter log parameters to their default values. **Command mode:** Global configuration
`show access-control log` Displays the current ACL log parameters. **Command mode:** All

Port Mirroring

Port mirroring is disabled by default. For more information about port mirroring on the G7028/G7052, see “Appendix A: Troubleshooting” in the *IBM N/OS 7.6 Application Guide*.

Port Mirroring commands are used to configure, enable, and disable the monitor port. When enabled, network packets being sent and/or received on a target port are duplicated and sent to a monitor port. By attaching a network analyzer to the monitor port, you can collect detailed information about your network performance and usage.

Table 130. Port Mirroring Configuration Options

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

Port-Mirroring Configuration

Table 131. Port-Based Port-Mirroring Configuration Options

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

Layer 2 Configuration

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

Table 132. Layer 2 Configuration Commands

Command Syntax and Usage
`vlan <VLAN number>` Enter VLAN configuration mode. To view command options, see page 223. **Command mode:** Global configuration
`show layer2` Displays current Layer 2 parameters. **Command mode:** All

Spanning Tree Configuration

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

Table 133. Spanning Tree Configuration Options

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

Table 133. Spanning Tree Configuration Options (continued)

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

Table 133. Spanning Tree Configuration Options (continued)

Command Syntax and Usage
`show spanning-tree root` Displays the Spanning Tree configuration on the root bridge for each STP instance. For details, see page 55. **Command mode:** All
`show spanning-tree blockedports` Lists the ports blocked by each STP instance. **Command mode:** All
`show spanning-tree [vlan <VLAN ID>] bridge` Displays Spanning Tree bridge information. For details, see page 54. **Command mode:** All

MSTP Configuration

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

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

Table 134. Multiple Spanning Tree Configuration Options

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

Table 134. Multiple Spanning Tree Configuration Options (continued)

Command Syntax and Usage
`spanning-tree mst forward-time <4-30>` Configures the forward delay time in seconds. The forward delay parameter specifies the amount of time that a bridge port has to wait before it changes from the listening state to the learning state and from the learning state to the forwarding state. Default value is 15. **Command mode:** Global configuration
`spanning-tree mst max-age <6-40>` Configures the maximum age interval in seconds. The maximum age parameter specifies the maximum time the bridge waits without receiving a configuration bridge protocol data unit before it reconfigures the MSTP network. Default value is 20. **Command mode:** Global configuration
`default spanning-tree mst <0-32>` Restores the Spanning Tree instance to its default configuration. **Command mode:** Global configuration
`instance <0-32> vlan <VLAN numbers>` Map the specified VLANs to the Spanning Tree instance. If a VLAN does not exist, it will be created automatically, but it will not be enabled by default. **Command mode:** MST configuration
`no instance <0-32> vlan {<VLAN numbers>|all}` Remove the specified VLANs or all VLANs from the Spanning Tree instance. **Command mode:** MST configuration
`spanning-tree mst <0-32> priority <0-65535>` Configures the CIST bridge priority for the specified MSTP instance. The bridge priority parameter controls which bridge on the network is the MSTP root bridge. To make this switch the root bridge, configure the bridge priority lower than all other switches and bridges on your network. The lower the value, the higher the bridge priority. The range is 0 to 65535, in steps of 4096 (0, 4096, 8192...); the default value is `32768`. **Command mode:** Global configuration
`show spanning-tree mst <0-32> information` Displays current MST information for the specified instance. **Command mode:** All
`show spanning-tree mst configuration` Displays the current MSTP settings. **Command mode:** All

MSTP Port Configuration

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

Table 135. MSTP Port Configuration Options

Command Syntax and Usage
`spanning-tree mst <0-32> port-priority <0-240>` Configures the port priority for the specified MSTP instance. The port priority helps determine which bridge port becomes the designated port. In a network topology that has multiple bridge ports connected to a single segment, the port with the lowest port priority becomes the designated port for the segment. The range is 0 to 240, in steps of 16 (0, 16, 32...), and the default is 128. **Command mode:** Interface port/Interface portchannel
`spanning-tree mst <0-32> cost <0-200000000>` Configures the port path cost for the specified MSTP instance. The port path cost is used to help determine the designated port for a segment. Port path cost is based on the port speed, and is calculated as follows: – 1Gbps = 20000 – 10Gbps = 2000 The default value of 0 (zero) indicates that the default path cost will be computed for an auto negotiated link speed. **Command mode:** Interface port/Interface portchannel
`spanning-tree mst hello-time <1-10>` Configures the port Hello time.The Hello time specifies how often the root bridge transmits a configuration bridge protocol data unit (BPDU). Any bridge that is not the root bridge uses the root bridge Hello value. The range is 1 to 10 seconds, and the default is 2 seconds. **Command mode:** Interface port/Interface portchannel
`[no] spanning-tree pvst-protection` Configures PVST Protection on the selected port. If the port receives any PVST+/PVRST BPDUs, it error disabled. PVST Protection works only in MSTP mode. The default setting is `disabled`. **Command mode:** Interface port
`[no] spanning-tree mst <0-32> enable` Enables or disables the specified MSTP instance on the port. **Command mode:** Interface port/Interface portchannel
`show interface port <port alias or number> spanning-tree mstp cist` Displays the current CIST port configuration. **Command mode:** All

RSTP/PVRST Configuration

Table 136 describes the commands used to configure the Rapid Spanning Tree (RSTP) and Per VLAN Rapid Spanning Tree Protocol (PVRST) protocols.

Table 136. RSTP/PVRST Configuration Options

Command Syntax and Usage
`spanning-tree stp` <*STG number*> `vlan` <*VLAN number*> Associates a VLAN with a Spanning Tree Group and requires a VLAN ID as a parameter. If the VLAN does not exist, it will be created automatically, but it will not be enabled by default. **Command mode:** Global configuration
`no spanning-tree stp` <*STG number*> `vlan` <*VLAN number*> Breaks the association between a VLAN and a Spanning Tree Group and requires a VLAN ID as a parameter. **Command mode:** Global configuration
`no spanning-tree stp` <*STG number*> `vlan all` Removes all VLANs from a Spanning Tree Group. **Command mode:** Global configuration
`spanning-tree stp` <*STG number*> `enable` Globally enables Spanning Tree Protocol. STG is turned on by default. **Command mode:** Global configuration
`no spanning-tree stp` <*STG number*> `enable` Globally disables Spanning Tree Protocol. **Command mode:** Global configuration
`default spanning-tree` <*STG number*> Restores a Spanning Tree instance to its default configuration. **Command mode:** Global configuration
`show spanning-tree stp` <*STG number*> Displays current Spanning Tree Protocol parameters for the specified Spanning Tree Group. See page 53 for details about the `information` parameter. **Command mode:** All

Bridge RSTP/PVRST Configuration

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

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

Table 137. Bridge Spanning Tree Configuration Options

Command Syntax and Usage
`spanning-tree stp <STG number> bridge priority <0-65535>` Configures the bridge priority. The bridge priority parameter controls which bridge on the network is the STG root bridge. To make this switch the root bridge, configure the bridge priority lower than all other switches and bridges on your network. The lower the value, the higher the bridge priority. Enter the value in multiples of 4096. Non-multiples are automatically rounded up to the closest valid priority. The default value is 61440. **Command mode:** Global configuration
`spanning-tree stp <STG number> bridge hello-time <1-10>` Configures the bridge Hello time.The Hello time specifies how often the root bridge transmits a configuration bridge protocol data unit (BPDU). Any bridge that is not the root bridge uses the root bridge Hello value. The range is 1 to 10 seconds, and the default is 2 seconds. This command does not apply to MSTP. **Command mode:** Global configuration
`spanning-tree stp <STG number> bridge maximum-age <6-40>` Configures the bridge maximum age. The maximum age parameter specifies the maximum time the bridge waits without receiving a configuration bridge protocol data unit before it re configures the STG network. The range is 6 to 40 seconds, and the default is 20 seconds. This command does not apply to MSTP. **Command mode:** Global configuration
`spanning-tree stp <STG number> bridge forward-delay <4-30>` Configures the bridge forward delay parameter. The forward delay parameter specifies the amount of time that a bridge port has to wait before it changes from the listening state to the learning state and from the learning state to the forwarding state. The range is 4 to 30 seconds, and the default is 15 seconds. This command does not apply to MSTP **Command mode:** Global configuration
`show spanning-tree [vlan <VLAN ID>] bridge` Displays the current Spanning Tree parameters either globally or for a specific VLAN. See page 54 for sample output. **Command mode:** All

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

- 2*(*fwd*-1) ≥ *mxage*
- 2*(*hello*+1) ≤ *mxage*

RSTP/PVRST Port Configuration

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

- Port priority
- Port path cost

Table 138. Spanning Tree Port Options

Command Syntax and Usage
`spanning-tree stp` <*STG number*> `priority` <*0-240*> Configures the port priority. The port priority helps determine which bridge port becomes the designated port. In a network topology that has multiple bridge ports connected to a single segment, the port with the lowest port priority becomes the designated port for the segment. The default value is 128. **RSTP/MSTP**: The range is 0 to 240, in steps of 16 (0, 16, 32...) and the default is 128. **Command mode:** Interface port
`spanning-tree stp` <*STG number*> `path-cost` <*1-200000000, 0 for default)*> Configures the port path cost. The port path cost is used to help determine the designated port for a segment. Port path cost is based on the port speed, and is calculated as follows: – 1Gbps = 20000 – 10Gbps = 2000 The default value of 0 (zero) indicates that the default path cost will be computed for an auto negotiated link speed. **Command mode:** Interface port
`spanning-tree stp link-type {auto|p2p|shared}` Defines the type of link connected to the port, as follows: – `auto`: Configures the port to detect the link type, and automatically match its settings. – `p2p`: Configures the port for Point-To-Point protocol. – `shared`: Configures the port to connect to a shared medium (usually a hub). **Command mode:** Interface port
`spanning-tree stp` <*STG number*> `enable` Enables STG on the port. **Command mode:** Interface port

Table 138. Spanning Tree Port Options (continued)

Command Syntax and Usage
`no spanning-tree stp <STG number> enable` Disables STG on the port. **Command mode:** Interface port
`show interface port <port alias or number> spanning-tree stp <STG number>` Displays the current STG port parameters. **Command mode:** All

Forwarding Database Configuration

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

Table 139. FDB Configuration Options

Command Syntax and Usage
`mac-address-table aging <0-65535>` Configures the aging value for FDB entries, in seconds. The default value is 300. **Command mode**: Global configuration
`show mac-address-table` Display current FDB configuration. **Command mode**: All except User EXEC

Static Multicast MAC Configuration

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

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

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

Table 140. Static Multicast MAC Configuration Options

Command Syntax and Usage

`mac-address-table multicast` *<MAC address> <VLAN number>* `{port` *<port alias or number>*`}`
Adds a static multicast entry. You can list ports separated by a comma, or enter a range of ports separated by a hyphen (-). For example:
`mac-address-table multicast 01:00:00:23:3f:01 200 1-4`
Command mode: Global configuration

`no mac-address-table multicast {all|`*<MAC address> <VLAN number>*`}` Deletes a static multicast entry. **Command mode**: Global configuration
`show mac-address-table multicast` Display the current static multicast entries. **Command mode**: All

Static FDB Configuration

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

Table 141. FDB Configuration Options

Command Syntax and Usage
`mac-address-table static` <*MAC address*> `vlan` <*VLAN number*> `{port` <*port alias or number*>`|portchannel` <*trunk number*>`| adminkey` <*1-65535*>`}` Adds a permanent FDB entry. Enter the MAC address using the following format, `xx:xx:xx:xx:xx:xx` For example, `08:00:20:12:34:56` You can also enter the MAC address as follows: `xxxxxxxxxxxx` For example, `080020123456` **Command mode**: Global configuration
`no mac-address-table static [`<*MAC address*>`] [`<*VLAN number*>`]|all` Deletes permanent FDB entries. **Command mode**: Global configuration
`show mac-address-table` Display current FDB configuration. **Command mode**: All except User EXEC

LLDP Configuration

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

Table 142. LLDP Configuration Options

Command Syntax and Usage
`lldp refresh-interval <5-32768>` Configures the message transmission interval, in seconds. The default value is 30. **Command mode**: Global configuration
`lldp holdtime-multiplier <2-10>` Configures the message hold time multiplier. The hold time is configured as a multiple of the message transmission interval. The default value is 4. **Command mode**: Global configuration
`lldp trap-notification-interval <1-3600>` Configures the trap notification interval, in seconds. The default value is 5. **Command mode**: Global configuration
`lldp transmission-delay <1-8192>` Configures the transmission delay interval. The transmit delay timer represents the minimum time permitted between successive LLDP transmissions on a port. The default value is 2. **Command mode**: Global configuration
`lldp reinit-delay <1-10>` Configures the re-initialization delay interval, in seconds. The re-initialization delay allows the port LLDP information to stabilize before transmitting LLDP messages. The default value is 2. **Command mode**: Global configuration
`lldp enable` Globally turns LLDP on. The default setting is `on`. **Command mode**: Global configuration
`no lldp enable` Globally turns LLDP off. **Command mode**: Global configuration
`show lldp [port <port_number>]` Display current LLDP configuration. **Command mode**: All

LLDP Port Configuration

Use the following commands to configure LLDP port options.

Table 143. LLDP Port Options

Command Syntax and Usage
`lldp admin-status {tx_only|rx_only|tx_rx}` Configures the LLDP transmission type for the port, as follows: – Transmit only – Receive only – Transmit and receive – The default setting is `tx_rx`. **Command mode**: Interface port
`no lldp admin-status` Disables the LLDP transmission type. **Command mode**: Interface port
`[no] lldp trap-notification` Enables or disables SNMP trap notification for LLDP messages. **Command mode**: Interface port
`show interface port` <*port alias or number*> `lldp` Display current LLDP port configuration. **Command mode**: All

LLDP Optional TLV configuration

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

Table 144. Optional TLV Options

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

Table 144. Optional TLV Options (continued)

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

Trunk Configuration

Trunk groups can provide super-bandwidth connections between RackSwitch G7028/G7052s or other trunk capable devices. A *trunk* is a group of ports that act together, combining their bandwidth to create a single, larger port. Up to 16 static trunk groups can be configured on the G7028/G7052, with the following restrictions:

- Any physical switch port can belong to no more than one trunk group.
- Up to 8 ports can belong to the same trunk group.
- You must configure all ports in a trunk group with the same properties (speed, duplex, flow control, STG, VLAN, and so on).
- Trunking from non-IBM devices must comply with Cisco® EtherChannel® technology.

By default, each trunk group is empty and disabled.

Table 145. Trunk Configuration Options

Command Syntax and Usage
`portchannel <1-16> port <port alias or number>` Adds a physical port or ports to the current trunk group. You can add several ports, with each port separated by a comma (,) or a range of ports, separated by a dash (-). **Command mode:** Global configuration
`no portchannel <1-16> port <port alias or number>` Removes a physical port or ports from the current trunk group. **Command mode:** Global configuration
`[no] portchannel <1-16> enable` Enables or Disables the current trunk group. **Command mode:** Global configuration
`no portchannel <1-16>` Removes the current trunk group configuration. **Command mode:** Global configuration
`show portchannel <1-32>` Displays current trunk group parameters. **Command mode:** All

Trunk Hash Configuration

Use the following commands to configure trunk hash settings for the G7028/G7052. The trunk hash settings affect both static trunks and LACP trunks.

To achieve the most even traffic distribution, select options that exhibit a wide range of values for your particular network. You may use the configuration settings listed in Table 146 combined with the hash parameters listed in and .

Table 146. Trunk Hash Options

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

Layer 2 Trunk Hash

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

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

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

Table 147. Layer 2 Trunk Hash Options

Command Syntax and Usage
`portchannel thash l2hash l2-source-mac-address` Enables Layer 2 trunk hashing on the source MAC. **Command mode:** Global configuration
`portchannel thash l2hash l2-destination-mac-address` Enables Layer 2 trunk hashing on the destination MAC. **Command mode:** Global configuration

Table 147. Layer 2 Trunk Hash Options

Command Syntax and Usage
`portchannel thash l2hash l2-source-destination-mac` Enables Layer 2 trunk hashing on both the source and destination MAC. **Command mode:** Global configuration
`show portchannel hash` Displays the current trunk hash settings. **Command mode:** All

Layer 3 Trunk Hash

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

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

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

Table 148. Layer 3 Trunk Hash Options

Command Syntax and Usage
`portchannel thash l3thash l3-use-l2-hash` Enables use of Layer 2 hash parameters only. When enabled, Layer 3 hashing parameters are cleared. **Command mode:** Global configuration
`portchannel thash l3thash l3-source-ip-address` Enables Layer 3 trunk hashing on the source IP address. **Command mode:** Global configuration
`portchannel thash l3thash l3-destination-ip-address` Enables Layer 3 trunk hashing on the destination IP address. **Command mode:** Global configuration
`portchannel thash l3thash l3-source-destination-ip` Enables Layer 3 trunk hashing on both the source and the destination IP address. **Command mode:** Global configuration
`show portchannel hash` Displays the current trunk hash settings. **Command mode:** All

Virtual Link Aggregation Control Protocol Configuration

vLAG groups allow you to enhance redundancy and prevent implicit loops without using STP. The vLAG group acts as a single virtual entity for the purpose of establishing a multi-port trunk.

Table 149. vLAG Configuration Options

Command Syntax and Usage
`[no] vlag portchannel <trunk group number> enable` Enables or disables vLAG on the selected trunk group. **Command mode:** Global configuration
`[no] vlag adminkey <1-65535> enable` Enables or disables vLAG on the selected LACP *admin key*. LACP trunks formed with this *admin key* will be included in the vLAG configuration. **Command mode:** Global configuration
`vlag priority <0-65535>` Configures the vLAG priority for the switch, used for election of Primary and Secondary vLAG switches. The switch with lower priority is elected to the role of Primary vLAG switch. **Command mode:** Global configuration
`vlag auto-recovery <240-3600>` Sets the duration in seconds of the auto-recovery timer. This timer configures how log after boot-up configuration load, the switch can assume the Primary role from an unresponsive ISL peer and bring up the vLAG ports. The default value is `300`. **Command mode:** Global configuration
`no vlag auto-recovery` Sets the auto-recovery timer to the default 300 seconds duration. **Command mode:** Global configuration
`no vlag startup-delay` Sets the vLAG startup-delay timer to the default 120 seconds duration. **Command mode:** Global configuration
`show vlag` Displays current vLAG parameters. **Command mode:** All

vLAG Health Check Configuration

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

Table 150. vLAG Health Check Configuration Options

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

vLAG ISL Configuration

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

Table 151. vLAG ISL Configuration Options

Command Syntax and Usage
`[no] vlag isl portchannel <portchannel ID>` Enables or disables vLAG Inter-Switch Link (ISL) on the selected trunk group. **Command mode:** Global configuration
`[no] vlag isl adminkey <1-65535>` Enables or disables vLAG Inter-Switch Link (ISL) on the selected LACP *admin key*. LACP trunks formed with this *admin key* will be included in the ISL. **Command mode:** Global configuration
`show vlag` Displays current vLAG parameters. **Command mode:** All

Link Aggregation Control Protocol Configuration

Use the following commands to configure Link Aggregation Control Protocol (LACP) for the G7028/G7052.

Table 152. Link Aggregation Control Protocol Options

Command Syntax and Usage
`lacp system-priority` *<1-65535>* Defines the priority value for the G7028/G7052. Lower numbers provide higher priority. The default value is 32768. **Command mode:** Global configuration
`lacp timeout {short|long}` Defines the timeout period before invalidating LACP data from a remote partner. Choose `short` (3 seconds) or `long` (90 seconds). The default value is `long`. **Note:** To reduce LACPDU processing, use a timeout value of `long`. If the CPU use rate of your G7028/G7052 remains at 100% for periods of 90 seconds or more, consider using static trunks instead of LACP. **Command mode:** Global configuration
`no lacp` *<1-65535>* Deletes a selected LACP trunk, based on its *admin key*. This command is equivalent to disabling LACP on each of the ports configured with the same *admin key*. **Command mode:** Global configuration
`show lacp` Display current LACP configuration. **Command mode:** All

LACP Port Configuration

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

Table 153. LACP Port Options

Command Syntax and Usage
`lacp mode {off|active|passive}` Set the LACP mode for this port, as follows: – **off** Turn LACP off for this port. You can use this port to manually configure a static trunk. The default value is `off`. – **active** Turn LACP on and set this port to active. Active ports initiate LACPDUs. – **passive** Turn LACP on and set this port to passive. Passive ports do not initiate LACPDUs, but respond to LACPDUs from active ports. **Command mode:** Interface port
`lacp priority` *<1-65535>* Sets the priority value for the selected port. Lower numbers provide higher priority. The default value is 32768. **Command mode:** Interface port
`lacp key` *<1-65535>* Set the *admin key* for this port. Only ports with the same *admin key* and *oper key* (operational state generated internally) can form a LACP trunk group. **Command mode:** Interface port
`port-channel min-links` *<1-8>* Set the minimum number of links for this port. If the specified minimum number of ports are not available, the trunk is placed in the `down` state. **Command mode:** Interface port
`default lacp [key | mode | priority]` Restores the selected parameters to their default values. **Command mode:** Interface port
`default port-channel min-links` Restores the minimum number of links for this port to its default value. **Command mode:** Interface port
`show interface port` *<port alias or number>* `lacp` Displays the current LACP configuration for this port. **Command mode:** All

Layer 2 Failover Configuration

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

Table 154. Layer 2 Failover Configuration Options

Command Syntax and Usage
`failover enable` Globally turns Layer 2 Failover `on`. **Command mode:** Global configuration
`no failover enable` Globally turns Layer 2 Failover `off`. **Command mode:** Global configuration
`show failover trigger` Displays current Layer 2 Failover parameters. **Command mode:** All

Failover Trigger Configuration

Table 155. Failover Trigger Configuration Options

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

Failover Manual Monitor Port Configuration

Use these commands to define the port link(s) to monitor. The Manual Monitor Port configuration accepts any non-management port.

Table 156. Failover Manual Monitor Port Options

Command Syntax and Usage
`failover trigger <1-8> mmon monitor member <port alias or number>` Adds the selected port to the Manual Monitor Port configuration. **Command mode:** Global configuration
`no failover trigger <1-8> mmon monitor member <port alias or number>` Removes the selected port from the Manual Monitor Port configuration. **Command mode:** Global configuration
`failover trigger <1-8> mmon monitor portchannel <trunk number>` Adds the selected trunk group to the Manual Monitor Port configuration. **Command mode:** Global configuration
`no failover trigger <1-8> mmon monitor portchannel <trunk number>` Removes the selected trunk group from the Manual Monitor Port configuration. **Command mode:** Global configuration
`failover trigger <1-8> mmon monitor adminkey <1-65535>` Adds an LACP *admin key* to the Manual Monitor Port configuration. LACP trunks formed with this admin key will be included in the Manual Monitor Port configuration. **Command mode:** Global configuration
`no failover trigger <1-8> mmon monitor adminkey <1-65535>` Removes an LACP *admin key* from the Manual Monitor Port configuration. **Command mode:** Global configuration
`show failover trigger <1-8>` Displays the current Failover settings. **Command mode:** All

Failover Manual Monitor Control Configuration

Use these commands to define the port link(s) to control. The Manual Monitor Control configuration accepts any non-management port.

Table 157. Failover Manual Monitor Control Options

Command Syntax and Usage
`failover trigger <1-8> mmon control member <port alias or number>` Adds the selected port to the Manual Monitor Control configuration. **Command mode:** Global configuration
`no failover trigger <1-8> mmon control member <port alias or number>` Removes the selected port from the Manual Monitor Control configuration. **Command mode:** Global configuration
`failover trigger <1-8> mmon control portchannel <trunk number>` Adds the selected trunk group to the Manual Monitor Control configuration. **Command mode:** Global configuration
`no failover trigger <1-8> mmon control portchannel <trunk number>` Removes the selected trunk group from the Manual Monitor Control configuration. **Command mode:** Global configuration
`failover trigger <1-8> mmon control adminkey <1-65535>` Adds an LACP *admin key* to the Manual Monitor Control configuration. LACP trunks formed with this admin key will be included in the Manual Monitor Control configuration. **Command mode:** Global configuration
`no failover trigger <1-8> mmon control adminkey <1-65535>` Removes an LACP *admin key* from the Manual Monitor Control configuration. **Command mode:** Global configuration
`show failover trigger <1-8>` Displays the current Failover settings. **Command mode:** All

Hot Links Configuration

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

Table 158. Hot Links Configuration Options

Command Syntax and Usage
`[no] hotlinks bpdu` Enables or disables flooding of Spanning-Tree BPDUs on the active Hot Links interface when the interface belongs to a Spanning Tree group that is globally turned `off`. This feature can prevent unintentional loop scenarios (for example, if two uplinks come up at the same time). The default setting is `disabled`. **Command mode:** Global configuration
`[no] hotlinks fdb-update` Enables or disables FDB Update, which allows the switch to send FDB and MAC update packets over the active interface. The default value is `disabled`. **Command mode:** Global configuration
`hotlinks fdb-update-rate` *<10-200>* Configures the FDB Update rate in packets per second. **Command mode:** Global configuration
`hotlinks enable` Globally enables Hot Links. **Command mode:** Global configuration
`no hotlinks enable` Globally disables Hot Links. **Command mode:** Global configuration
`show hotlinks` Displays current Hot Links parameters. **Command mode:** All

Hot Links Trigger Configuration

Table 159. Hot Links Trigger Configuration Options

Command Syntax and Usage
`hotlinks trigger <1-25> forward-delay <0-3600>` Configures the Forward Delay interval, in seconds. The default value is `1`. **Command mode:** Global configuration
`[no] hotlinks trigger <1-25> name <1-32 characters>` Defines a name for the Hot Links trigger. **Command mode:** Global configuration
`[no] hotlinks trigger <1-25> preemption` Enables or disables pre-emption, which allows the Master interface to transition to the Active state whenever it becomes available. The default setting is `enabled`. **Command mode:** Global configuration
`[no] hotlinks trigger <1-25> enable` Enables or disables the Hot Links trigger. **Command mode:** Global configuration
`no hotlinks trigger <1-25>` Deletes the Hot Links trigger. **Command mode:** Global configuration
`show hotlinks trigger <1-25>` Displays the current Hot Links trigger settings. **Command mode:** All

Hot Links Master Configuration

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

Table 160. Hot Links Master Configuration Options

Command Syntax and Usage
[no] hotlinks trigger <*1-25*> master port <*port alias or number*> Adds or removes the selected port to the Hot Links Master interface. **Command mode:** Global configuration
[no] hotlinks trigger <*1-25*> master portchannel <*trunk group number*> Adds or removes the selected trunk group to the Master interface. **Command mode:** Global configuration
[no] hotlinks trigger <*1-25*> master adminkey <*1-65535*> Adds or removes an LACP *admin key* to the Master interface. LACP trunks formed with this *admin key* will be included in the Master interface. **Command mode:** Global configuration
show hotlinks trigger <*1-25*> Displays the current Hot Links trigger settings. **Command mode:** All

Hot Links Backup Configuration

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

Table 161. Hot Links Backup Configuration Options

Command Syntax and Usage
[no] hotlinks trigger <*1-25*> backup port <*port alias or number*> Adds or removes the selected port to the Hot Links Backup interface. **Command mode:** Global configuration
[no] hotlinks trigger <*1-25*> backup portchannel <*trunk group number*> Adds or removes the selected trunk group to the Backup interface. **Command mode:** Global configuration
[no] hotlinks trigger <*1-25*> backup adminkey <*1-65535*> Adds or removes an LACP *admin key* to the Backup interface. LACP trunks formed with this *admin key* will be included in the Backup interface. **Command mode:** Global configuration
show hotlinks trigger <*1-25*> Displays the current Hot Links trigger settings. **Command mode:** All

VLAN Configuration

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

By default, VLAN 1 is the only VLAN configured on the switch. All ports are members of VLAN 1 by default. Up to 4094 VLANs can be configured on the G7028/G7052.

VLANs can be assigned any number between 1 and 4094. VLAN 4095 is reserved for switch management.

Table 162. VLAN Configuration Options

Command Syntax and Usage
`vlan` <*VLAN number*> Enter VLAN configuration mode. **Command mode:** Global configuration
`name` <*1-32 characters*> Assigns a name to the VLAN or changes the existing name. The default VLAN name is the first one. **Command mode:** VLAN
`[no] shutdown` Disables or enables local traffic on the specified VLAN. Default setting is enabled (`no shutdown`) **Command mode:** VLAN
`stg` <*STG number*> Assigns a VLAN to a Spanning Tree Group. **Note**: For MST no VLAN assignation is required. VLANs are mapped from CIST. **Command mode:** VLAN
`[no] flood` Configures the switch to flood unregistered IP multicast traffic to all ports. The default setting is `enabled`. **Note:** If none of the IGMP hosts reside on the VLAN of the streaming server for a IPMC group, you must disable IGMP flooding to ensure that multicast data is forwarded across the VLANs for that IPMC group. **Command mode:** VLAN

Table 162. VLAN Configuration Options (continued)

Command Syntax and Usage
`[no] cpu` Configures the switch to forward unregistered IP multicast traffic to the MP, which adds an entry in the IPMC table, as follows: – If no Mrouter is present, drop subsequent packets with same IPMC. – If an Mrouter is present, forward subsequent packets to the Mrouter(s) on the ingress VLAN. The default setting is `enabled`. **Note**: If both `flood` and `cpu` are disabled, the switch drops all unregistered IPMC traffic. **Command mode:** VLAN
`[no] optflood` Enables or disables optimized flooding. When enabled, optimized flooding avoids packet loss during the learning period. The default setting is `disabled`. **Command mode:** VLAN
`no vlan` *<VLAN number>* Deletes this VLAN. **Command mode:** VLAN
`show vlan information` Displays the current VLAN configuration. **Command mode:** All

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

Private VLAN Configuration

Use the following commands to configure Private VLANs.

Table 163. Private VLAN Options

Command Syntax and Usage
`[no] private-vlan primary` Enables or disables the VLAN type as a Primary VLAN. A Private VLAN must have only one primary VLAN. The primary VLAN carries unidirectional traffic to ports on the isolated VLAN or to community VLAN. **Command mode:** VLAN
`[no] private-vlan community` Enables or disables the VLAN type as a community VLAN. Community VLANs carry upstream traffic from host ports. A Private VLAN may have multiple community VLANs. **Command mode:** VLAN
`[no] private-vlan isolated` Enables or disables the VLAN type as an isolated VLAN. The isolated VLAN carries unidirectional traffic from host ports. A Private VLAN may have only one isolated VLAN. **Command mode:** VLAN
`private-vlan association [add|remove]` *<secondary VLAN list>* Configures Private VLAN mapping between a primary VLAN and secondary VLANs. If no optional parameter is specified, the list of secondary VLANs, replaces the currently associated secondary VLANs. Otherwise: – `add` appends the secondary VLANs to the ones currently associated – `remove` excludes the secondary VLANs from the ones currently associated **Command mode:** VLAN
`private-vlan enable` Enables the private VLAN. **Command mode:** VLAN
`no private-vlan enable` Disables the Private VLAN. **Command mode:** VLAN
`show vlan private-vlan` – Displays current parameters for the selected Private VLAN(s). **Command mode:** VLAN

Layer 3 Configuration

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

Table 164. Layer 3 Configuration Commands

Command Syntax and Usage
`interface ip` <*interface number*> Configures the IP Interface. The G7028/G7052 supports up to 4 IP interfaces. However, IP interface 3 and 4 are reserved for switch management. To view command options, see page 227. **Command mode:** Global configuration
`show layer3` Displays the current IP configuration. **Command mode:** All

IP Interface Configuration

The G7028/G7052 supports up to 4 IP interfaces. Each IP interface represents the G7028/G7052 on an IP subnet on your network. The Interface option is disabled by default.

Table 165. IP Interface Configuration Options

Command Syntax and Usage
`interface ip` *<interface number>* Enter IP interface mode. **Command mode:** Global configuration
`ip address` *<IP address>* [*<IP netmask>*] Configures the IP address of the switch interface, using dotted decimal notation. **Command mode:** Interface IP
`ip netmask` *<IP netmask>* Configures the IP subnet address mask for the interface, using dotted decimal notation. **Command mode:** Interface IP
`ipv6 address` *<IP address (such as 3001:0:0:0:0:0:abcd:12)>* [`anycast`|`enable`] Configures the IPv6 address of the switch interface, using hexadecimal format with colons. **Command mode:** Interface IP
`vlan` *<VLAN number>* Configures the VLAN number for this interface. Each interface can belong to one VLAN. **IPv4**: Each VLAN can contain multiple IPv4 interfaces. **IPv6**: Each VLAN can contain only one IPv6 interface. **Command mode:** Interface IP
`[no] ipv6 unreachables` Enables or disables sending of ICMP Unreachable messages. The default setting is `enabled`. **Command mode:** Interface IP
`enable` Enables this IP interface. **Command mode:** Interface IP
`no enable` Disables this IP interface. **Command mode:** Interface IP

Table 165. IP Interface Configuration Options (continued)

Command Syntax and Usage
`no interface ip` <*interface number*> Removes this IP interface. **Command mode:** Interface IP
`show interface ip` <*interface number*> Displays the current interface settings. **Command mode:** All

Default Gateway Configuration

The switch can be configured

This option is disabled by default.

Table 166. IPv4 Default Gateway Options

Command Syntax and Usage
`ip gateway <1,4> address <IP address>` Configures the IP address of the default IP gateway using dotted decimal notation. **Command mode:** Global configuration
`ip gateway <1,4> interval <0-60>` The switch pings the default gateway to verify that it's up. This command sets the time between health checks. The range is from 0 to 60 seconds. The default is 2 seconds. **Command mode:** Global configuration
`ip gateway <1,4> retry <1-120>` Sets the number of failed health check attempts required before declaring this default gateway inoperative. The range is from 1 to 120 attempts. The default is 8 attempts. **Command mode:** Global configuration
`[no] ip gateway <1,4> arp-health-check` Enables or disables Address Resolution Protocol (ARP) health checks. The default setting is `disabled`. The `arp` option does not apply to management gateways. **Command mode:** Global configuration
`ip gateway <1,4> enable` Enables the gateway for use. **Command mode:** Global configuration
`no ip gateway <1,4> enable` Disables the gateway. **Command mode:** Global configuration
`no ip gateway <1,4>` Deletes the gateway from the configuration. **Command mode:** Global configuration
`show ip gateway <1,4>` Displays the current gateway settings. **Command mode:** All

Network Filter Configuration

Table 167. IP Network Filter Configuration Options

Command Syntax and Usage
`ip match-address <1-256> <IP address> <IP netmask>` Sets the starting IP address and IP Netmask for this filter to define the range of IP addresses that will be accepted by the peer when the filter is enabled. The default address is `0.0.0.0 0.0.0.0` **Command mode:** Global configuration.
`ip match-address <1-256> enable` Enables the Network Filter configuration. **Command mode:** Global configuration
`no ip match-address <1-256> enable` Disables the Network Filter configuration. **Command mode:** Global configuration
`no ip match-address <1-256>` Deletes the Network Filter configuration. **Command mode:** Global configuration
`show ip match-address [<1-256>]` Displays the current the Network Filter configuration. **Command mode:** All except User EXEC

IGMP Configuration

Table 168 describes the commands used to configure basic IGMP parameters.

Table 168. IGMP Configuration Options

Command Syntax and Usage
`ip igmp enable` Globally turns IGMP on. **Command mode:** Global configuration
`no ip igmp enable` Globally turns IGMP off. **Command mode:** Global configuration
`show ip igmp` Displays the current IGMP configuration parameters. **Command mode:** All

The following sections describe the IGMP configuration options.

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 169 describes the commands used to configure IGMP Snooping.

Table 169. IGMP Snooping Configuration Options

Command Syntax and Usage
`ip igmp snoop mrouter-timeout` *<1-600>* Configures the timeout value for IGMP Membership Queries (mrouter). Once the timeout value is reached, the switch removes the multicast router from its IGMP table, if the proper conditions are met. The range is from 1 to 600 seconds. The default is 255 seconds. **Command mode:** Global configuration
`[no] ip igmp aggregate` Enables or disables IGMP Membership Report aggregation. **Command mode:** Global configuration
`ip igmp snoop source-ip` *<IP address>* Configures the source IP address used as a proxy for IGMP Group Specific Queries. **Command mode:** Global configuration
`ip igmp snoop vlan` *<VLAN number>* Adds the selected VLAN(s) to IGMP Snooping. **Command mode:** Global configuration
`no ip igmp snoop vlan` *<VLAN number>* Removes the selected VLAN(s) from IGMP Snooping. **Command mode:** Global configuration
`no ip igmp snoop vlan all` Removes all VLANs from IGMP Snooping. **Command mode:** Global configuration
`ip igmp snoop enable` Enables IGMP Snooping. **Command mode:** Global configuration

Table 169. IGMP Snooping Configuration Options (continued)

Command Syntax and Usage
`no ip igmp snoop enable` Disables IGMP Snooping. **Command mode:** Global configuration
`default ip igmp snoop` Resets IGMP Snooping parameters to their default values. **Command mode:** Global configuration
`show ip igmp snoop` Displays the current IGMP Snooping parameters. **Command mode:** All

IGMPv3 Configuration

Table 170 describes the commands used to configure IGMP version 3.

Table 170. IGMP Version 3 Configuration Options

Command Syntax and Usage
`ip igmp snoop igmpv3 sources` *<1-64>* Configures the maximum number of IGMP multicast sources to snoop from within the group record. Use this command to limit the number of IGMP sources to provide more refined control. The default value is 8. **Command mode:** Global configuration
`[no] ip igmp snoop igmpv3 v1v2` Enables or disables snooping on IGMP version 1 and version 2 reports. When disabled, the switch drops IGMPv1 and IGMPv2 reports. The default value is `enabled`. **Command mode:** Global configuration
`[no] ip igmp snoop igmpv3 exclude` Enables or disables snooping on IGMPv3 Exclude Reports. When disabled, the switch ignores Exclude Reports. The default value is `enabled`. **Command mode:** Global configuration
`ip igmp snoop igmpv3 enable` Enables IGMP version 3. The default value is `disabled`. **Command mode:** Global configuration
`no ip igmp snoop igmpv3 enable` Disables IGMP version 3. **Command mode:** Global configuration
`show ip igmp snoop igmpv3` Displays the current IGMP v3 Snooping configuration. **Command mode:** All except User EXEC

IGMP Static Multicast Router Configuration

Table 171 describes the commands used to configure a static multicast router.

Note: When static Mrouters are used, the switch continues learning dynamic Mrouters via IGMP snooping. However, dynamic Mrouters may not replace static Mrouters. If a dynamic Mrouter has the same port and VLAN combination as a static Mrouter, the dynamic Mrouter is not learned.

Table 171. IGMP Static Multicast Router Configuration Options

Command Syntax and Usage
`ip igmp mrouter` *<port alias or number> <VLAN number> <version (1-3)>* Selects a port/VLAN combination on which the static multicast router is connected, and configures the IGMP version of the multicast router. **Command mode:** Global configuration
`no ip igmp mrouter` *<port alias or number> <VLAN number> <version (1-3)>* Removes a static multicast router from the selected port/VLAN combination. **Command mode:** Global configuration
`no ip igmp mrouter all` Removes all static multicast routers. **Command mode:** Global configuration
`clear ip igmp mrouter` Clears the multicast router port table. **Command mode:** Global configuration
`show ip igmp mrouter` Displays the current IGMP Static Multicast Router parameters. **Command mode:** All except User EXEC

IGMP Filtering Configuration

Table 172 describes the commands used to configure an IGMP filter.

Table 172. IGMP Filtering Configuration Options

Command Syntax and Usage
`ip igmp profile` *<1-16>* Configures the IGMP filter. **Command mode:** Global configuration To view command options, see page 234.
`ip igmp filtering` Enables IGMP filtering globally. **Command mode:** Global configuration
`no ip igmp filtering` Disables IGMP filtering globally. **Command mode:** Global configuration
`show ip igmp filtering` Displays the current IGMP Filtering parameters. **Command mode:** All

IGMP Filter Definition

Table 173 describes the commands used to define an IGMP filter.

Table 173. IGMP Filter Definition Options

Command Syntax and Usage
`ip igmp profile` *<1-16>* `range` *<IP address 1>* *<IP address 2>* Configures the range of IP multicast addresses for this filter. **Command mode:** Global configuration
`ip igmp profile` *<1-16>* `action {allow|deny}` Allows or denies multicast traffic for the IP multicast addresses specified. The default action is `deny`. **Command mode:** Global configuration
`ip igmp profile` *<1-16>* `enable` Enables this IGMP filter. **Command mode:** Global configuration
`no ip igmp profile` *<1-16>* `enable` Disables this IGMP filter. **Command mode:** Global configuration

Table 173. IGMP Filter Definition Options (continued)

Command Syntax and Usage
`no ip igmp profile <1-16>` Deletes this filter's parameter definitions. **Command mode:** Global configuration
`show ip igmp profile <1-16>` Displays the current IGMP filter. **Command mode:** All

IGMP Filtering Port Configuration

Table 174 describes the commands used to configure a port for IGMP filtering.

Table 174. IGMP Filter Port Configuration Options

Command Syntax and Usage
`[no] ip igmp filtering` Enables or disables IGMP filtering on this port. **Command mode:** Interface port
`ip igmp profile <1-16>` Adds an IGMP filter to this port. **Command mode:** Interface port
`no ip igmp profile <1-16>` Removes an IGMP filter from this port. **Command mode:** Interface port
`show interface port <port alias or number> igmp-filtering` Displays the current IGMP filter parameters for this port. **Command mode:** All except User EXEC

IGMP Querier Configuration

Table 175 describes the commands used to configure IGMP Querier.

Table 175. IGMP Querier Configuration Options

Command Syntax and Usage
`[no] ip igmp querier vlan <VLAN number or range> enable` Enables or disables IGMP Querier for the selected VLANs. **Command mode:** Global configuration
`ip igmp querier vlan <VLAN number> source-ip <IP address>` Configures the IGMP source IP address for the selected VLAN. **Command mode:** Global configuration

Table 175. IGMP Querier Configuration Options (continued)

Command Syntax and Usage
`ip igmp querier vlan <VLAN number> max-response <1-256>` Configures the maximum time, in tenths of a second, allowed before responding to a Membership Query message. The default value is 100. By varying the Query Response Interval, an administrator may tune the burstiness of IGMP messages on the subnet; larger values make the traffic less bursty, as host responses are spread out over a larger interval. **Command mode:** Global configuration
`ip igmp querier vlan <VLAN number> query-interval <1-608>` Configures the interval between IGMP Query broadcasts. The default value is 125 seconds. **Command mode:** Global configuration
`ip igmp querier vlan <VLAN number> robustness <1-10>` Configures the IGMP Robustness variable, which is the number of times that the switch sends each IGMP message. The default value is 2. **Command mode:** Global configuration
`ip igmp querier vlan <VLAN number> election-type [ipv4|mac]` Sets the IGMP Querier election criteria as IP address or Mac address. The default setting is IPv4. **Command mode:** Global configuration
`ip igmp querier vlan <VLAN number> startup-interval <1-608>` Configures the Startup Query Interval, which is the interval between General Queries sent out at startup. **Command mode:** Global configuration
`ip igmp querier vlan <VLAN number> startup-count <1-10>` Configures the Startup Query Count, which is the number of IGMP Queries sent out at startup. Each Query is separated by the Startup Query Interval. The default value is 2. **Command mode:** Global configuration
`ip igmp querier vlan <VLAN number> version [v1|v2|v3]` Configures the IGMP version. The default version is `v3`. **Command mode:** Global configuration
`[no] ip igmp querier enable` Enables or disables IGMP Querier. **Command mode:** Global configuration

Table 175. IGMP Querier Configuration Options (continued)

Command Syntax and Usage
`show ip igmp querier vlan <VLAN number>` Displays IGMP Querier information for the selected VLAN. **Command mode:** Global configuration
`show ip igmp querier` Displays the current IGMP Querier parameters. **Command mode:** All

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 176. Domain Name Service Options

Command Syntax and Usage
`[no] ip dns primary-server` *<IP address>* You are prompted to set the IPv4 address for your primary DNS server, using dotted decimal notation. **Command mode:** Global configuration
`[no] ip dns secondary-server` *<IP address>* You are prompted to set the IPv4 address for your secondary DNS server, using dotted decimal notation. If the primary DNS server fails, the configured secondary will be used instead. **Command mode:** Global configuration
`[no] ip dns ipv6 primary-server` *<IP address>* You are prompted to set the IPv6 address for your primary DNS server, using hexadecimal format with colons. **Command mode:** Global configuration
`[no] ip dns ipv6 secondary-server` *<IP address>* You are prompted to set the IPv6 address for your secondary DNS server, using hexadecimal format with colons. If the primary DNS server fails, the configured secondary will be used instead. **Command mode:** Global configuration
`ip dns ipv6 request-version {ipv4|ipv6}` Sets the protocol used for the first request to the DNS server, as follows: – IPv4 – IPv6 **Command mode:** Global configuration
`[no] ip dns domain-name` *<string>* Sets the default domain name used by the switch. For example: `mycompany.com` **Command mode:** Global configuration
`show ip dns` Displays the current Domain Name System settings. **Command mode:** All except User EXEC

IPv6 Default Gateway Configuration

The switch supports IPv6 default gateways

Table 177 describes the IPv6 Default Gateway Configuration commands.

Table 177. IPv6 Default Gateway Configuration Options

Command Syntax and Usage
`ip gateway6 {1|4} address` *<IPv6 address>* Configures the IPv6 address of the default gateway, in hexadecimal format with colons (such as 3001:0:0:0:0:0:abcd:12). **Command mode**: Global configuration
`[no] ip gateway6 {1|4} enable` Enables or disables the default gateway. **Command mode**: Global configuration
`no ip gateway6 {1|4}` Deletes the default gateway. **Command mode**: Global configuration
`show ipv6 gateway6 {1|4}` Displays the current IPv6 default gateway configuration. **Command mode**: All

Remote Monitoring Configuration

Remote Monitoring (RMON) allows you to monitor traffic flowing through the switch. The RMON MIB is described in RFC 1757.

The following sections describe the Remote Monitoring (RMON) configuration options.

- "RMON History Configuration" on page 240
- "RMON Event Configuration" on page 241
- "RMON Alarm Configuration" on page 242

RMON History Configuration

Table 178 describes the RMON History commands.

Table 178. RMON History Configuration Options

Command Syntax and Usage
`rmon history` *<1-65535>* `interface-oid` *<1-127 characters>* Configures the interface MIB Object Identifier. The IFOID must correspond to the standard interface OID, as follows: 1.3.6.1.2.1.2.2.1.1.x where x is the `ifIndex` **Command mode**: Global configuration
`rmon history` *<1-65535>* `requested-buckets` *<1-65535>* Configures the requested number of buckets, which is the number of discrete time intervals over which data is to be saved. The default value is 30. The maximum number of buckets that can be granted is 50. **Command mode**: Global configuration
`rmon history` *<1-65535>* `polling-interval` *<1-3600>* Configures the time interval over which the data is sampled for each bucket. The default value is 1800. **Command mode**: Global configuration
`rmon history` *<1-65535>* `owner` *<1-127 characters>* Enter a text string that identifies the person or entity that uses this History index. **Command mode**: Global configuration
`no rmon history` *<1-65535>* Deletes the selected History index. **Command mode**: Global configuration
`show rmon history` Displays the current RMON History parameters. **Command mode**: All

RMON Event Configuration

Table 179 describes the RMON Event commands.

Table 179. RMON Event Configuration Options

Command Syntax and Usage
`rmon event <1-65535> description <1-127 characters>` Enter a text string to describe the event. **Command mode**: Global configuration
`[no] rmon event <1-65535> type log|trap|both` Selects the type of notification provided for this event. For log events, an entry is made in the log table and sent to the configured syslog host. For trap events, an SNMP trap is sent to the management station. **Command mode**: Global configuration
`rmon event <1-65535> owner <1-127 characters>` Enter a text string that identifies the person or entity that uses this event index. **Command mode**: Global configuration
`no rmon event <1-65535>` Deletes the selected RMON Event index. **Command mode**: Global configuration
`show rmon event` Displays the current RMON Event parameters. **Command mode**: All

RMON Alarm Configuration

The alarm RMON group can track rising or falling values for a MIB object. The MIB object must be a counter, gauge, integer, or time interval. Each alarm index must correspond to an event index that triggers once the alarm threshold is crossed.

Table 180 describes the RMON alarm commands.

Table 180. RMON Alarm Configuration Options

Command Syntax and Usage
`rmon alarm <1-65535> oid <1-127 characters>` Configures an alarm MIB Object Identifier. **Command mode**: Global configuration
`rmon alarm <1-65535> interval <1-65535>` Configures the time interval over which data is sampled and compared with the rising and falling thresholds. The default value is 1800. **Command mode**: Global configuration
`rmon alarm <1-65535> sample abs|delta` Configures the method of sampling the selected variable and calculating the value to be compared against the thresholds, as follows: – `abs`–absolute value, the value of the selected variable is compared directly with the thresholds at the end of the sampling interval. – `delta`–delta value, the value of the selected variable at the last sample is subtracted from the current value, and the difference compared with the thresholds. **Command mode**: Global configuration
`rmon alarm <1-65535> alarm-type rising|falling|either` Configures the alarm type as rising, falling, or either (rising or falling). **Command mode**: Global configuration
`rmon alarm <1-65535> rising-limit <-2147483647 - 2147483647>` Configures the rising threshold for the sampled statistic. When the current sampled value is greater than or equal to this threshold, and the value at the last sampling interval was less than this threshold, a single event is generated. **Command mode**: Global configuration
`rmon alarm <1-65535> falling-limit <-2147483647 - 214748364)` Configures the falling threshold for the sampled statistic. When the current sampled value is less than or equal to this threshold, and the value at the last sampling interval was greater than this threshold, a single event is generated. **Command mode**: Global configuration
`rmon alarm <1-65535> rising-crossing-index <0-65535>` Configures the rising alarm event index that is triggered when a rising threshold is crossed. **Command mode**: Global configuration
`rmon alarm <1-65535> falling-crossing-index <0-65535>` Configures the falling alarm event index that is triggered when a falling threshold is crossed. **Command mode**: Global configuration

Table 180. RMON Alarm Configuration Options (continued)

Command Syntax and Usage
`rmon alarm <1-65535> owner <1-127 characters>` Enter a text string that identifies the person or entity that uses this alarm index. **Command mode**: Global configuration
`no rmon alarm <1-65535>` Deletes the selected RMON Alarm index. **Command mode**: Global configuration
`show rmon alarm` Displays the current RMON Alarm parameters. **Command mode**: All

Configuration Dump

The dump program writes the current switch configuration to the terminal screen. To start the dump program, at the prompt, enter:

```
RS G7028(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 247.

Saving the Active Switch Configuration

When the `copy running-config {ftp|tftp}` command is used, the switch's active configuration commands (as displayed using `show running-config`) will be uploaded to the specified script configuration file on the FTP/TFTP server. To start the switch configuration upload, at the prompt, enter:

```
RS G7028(config)# copy running-config ftp
    or
RS G7028(config)# copy running-config tftp
```

The switch prompts you for the server address and filename.

Note: The output file is formatted with line-breaks but no carriage returns—the file cannot be viewed with editors that require carriage returns (such as Microsoft Notepad).

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

Restoring the Active Switch Configuration

When the `copy {ftp|tftp} running-config` command is used, the active configuration will be replaced with the commands found in the specified configuration file. The file can contain a full switch configuration or a partial switch configuration.

To start the switch configuration download, at the prompt, enter:

```
RS G7028(config)# copy ftp running-config
    or
RS G7028(config)# copy tftp running-config
```

The switch prompts you for the server address and filename.

USB Copy

If a USB drive is inserted into the USB port, you can copy files from the switch to the USB drive, or from the USB drive to the switch. You also can boot the switch using software or configuration files found on the USB drive (see "USB Boot Configuration" on page 254).

Copy to USB

Use the following command to copy a file from the switch to the USB drive:

```
usbcopy tousb <filename> {active|boot|crashdump|image1|image2|syslog|}
```

Command mode: Privileged EXEC

In this example, the active configuration file is copied to a directory on the USB drive:

```
RS G7028(config)# usbcopy tousb a_folder/myconfig.cfg active
```

Copy from USB

Use the following command to copy a file from the USB drive to the switch:

```
usbcopy fromusb <filename> {active|boot|image1|image2}
```

Command mode: Privileged EXEC

In this example, the active configuration file is copied from a directory on the USB drive:

```
RS G7028(config)# usbcopy fromusb a_folder/myconfig.cfg active
```

The new file replaces the current file.

Note: Do not use two consecutive dot characters (..). Do not use a slash character (/) to begin a filename.

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 181. General Operations Commands

Command Syntax and Usage
`password` Allows the user to change the password. You must enter the current password in use for validation. The switch prompts for a new password between 1-128 characters. **Command Mode**: Privileged EXEC
`access tnetsshc` Closes all open Telnet and SSH connections. **Command Mode**: Global configuration
`console-log` Enables or disables session console logging. **Command Mode**: Privileged EXEC
`clear logging` Clears all Syslog messages. **Command Mode**: Privileged EXEC
`ntp send` Allows the user to send requests to the NTP server. **Command Mode**: Privileged EXEC

Operations-Level Port Commands

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

Table 182. Port Operations

Command Syntax and Usage
`interface port <port number or alias> dot1x init` Reinitializes 802.1x access control on the port. **Command Mode**: Privileged EXEC
`interface port <port number or alias> dot1x re-authenticate` Immediately starts reauthentication on the port. **Command Mode**: Privileged EXEC
`[no] interface port <port number or alias> rmon` Temporarily enables or disables remote monitoring of the port. The port will be returned to its configured operation mode when the switch is reset. **Command Mode**: Privileged EXEC
`no interface port <port number or alias> shutdown` Temporarily enables the port. The port will be returned to its configured operation mode when the switch is reset. **Command Mode**: Privileged EXEC
`interface port <port number or alias> shutdown` Temporarily disables the port. The port will be returned to its configured operation mode when the switch is reset. **Command Mode**: Privileged EXEC
`show interface port <port number or alias> operation` Displays the port interface operational state. **Command Mode**: Privileged EXEC

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.

Table 183. Scheduled Reboot Options

Command Syntax and Usage

`boot schedule` *<day> <time (hh:mm)>*
Configures the switch reset time. The following options are valid for the `day` value:
`monday`
`tuesday`
`wednesday`
`thursday`
`friday`
`saturday`
`sunday`
Command Mode: Global configuration

`no boot schedule` Cancels the switch reset time. **Command Mode**: Global configuration
`show boot` Displays the current switch reboot schedule. **Command Mode**: All except User EXEC

Netboot Configuration

Netboot allows the switch to automatically download its configuration file over the network during switch reboot, and apply the new configuration. Upon reboot, the switch includes the following options in its DHCP requests:

- Option 66 (TFTP server address)
- Option 67 (file path)

If the DHCP server returns the information, the switch initiates a TFTP file transfer, and loads the configuration file into the active configuration block. As the switch boots up, it applies the new configuration file. Note that the option 66 TFTP server address must be specified in IP-address format (host name is not supported).

Table 184. Netboot Options

Command Syntax and Usage
`boot netboot enable` Enables Netboot. When enabled, the switch boots into factory-default configuration, and attempts to download a new configuration file. **Command Mode**: Global configuration
`no boot netboot enable` Disables Netboot. **Command Mode**: Global configuration
`[no] boot netboot tftp` *<IP address>* Configures the IP address of the TFTP server used for manual configuration. **Command Mode**: Global configuration
`[no] boot netboot cfgfile` *<1-31 characters>* Defines the file path for the configuration file on the TFTP server. For example: `/directory/sub/config.cfg` **Command Mode**: Global configuration
`show boot` Displays the current Netboot parameters. **Command Mode**: All

USB Boot Configuration

USB Boot allows you to boot the switch with a software image file, boot file, or configuration file that resides on a USB drive inserted into the USB port. Use the following command to enable or disable USB Boot:

```
[no] boot usbboot enable
```

Command mode: Global configuration

When enabled, the switch checks the USB port when it is reset. If a USB drive is inserted into the port, the switch checks the drive for software and image files. If a valid file is present on the USB drive, the switch loads the file and boots using the file.

The following list describes the valid file names, and describes the switch behavior when it recognizes them. The file names must be exactly as shown, or the switch will not recognize them.

- `RSG7028_Boot.img (for G7028)`
  `RSG7052_Boot.img (for G7052)`
  The switch replaces the current boot image with the new image, and boots with the new image.
- `RSG7028_OS.img (for G7028)`
  `RSG7052_OS.img (for G7052)`
  The switch boots with the new software image. The existing images are not affected.
- `RSG7028_replace1_OS.img (for G7028)`
  `RSG7052_replace1_OS.img (for G7052)`
  The switch replaces the current software image1 with the new image, and boots with the new image.
- `RSG7028_replace2_OS.img (for G7028)`
  `RSG7052_replace2_OS.img (for G7052)`
  The switch replaces the current software image2 with the new image, and boots with the new image.
- `RSG7028.cfg (for G7028)`
  `RSG7052.cfg (for G7052)`
  The switch boots with the new configuration file. The existing configuration files (active and backup) are not affected.
- `RSG7028_replace.cfg (for G7028)`
  `RSG7052_replace.cfg (for G7052)`
  The switch replaces the active configuration file with the new file, and boots with the new file. This file takes precedence over any other configuration files that may be present on the USB drive.

If more than one valid file is present, the switch loads all valid files and boots with them. For example, you may simultaneously load a new boot file, image file, and configuration file from the USB drive.

The switch ignores any files that do not match the valid file names or that have the wrong format.

You also can copy files to and from the USB drive. See “USB Copy” on page 248.

Updating the Switch Software Image

The switch software image is the executable code running on the G7028/G7052. A version of the image ships with the switch, and comes pre-installed on the device. As new versions of the image are released, you can upgrade the software running on your switch.

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

Upgrading the software image on your switch requires the following:

- Loading the new image onto a FTP or TFTP server on your network
- Transferring the new image from the FTP or TFTP server to your switch
- Selecting the new software image to be loaded into switch memory the next time the switch is reset

Loading New Software to Your Switch

The switch can store up to two different software images, called `image1` and `image2`, as well as boot software, called `boot`. When you load new software, you must specify where it should be placed: either into `image1`, `image2`, or `boot`.

For example, if your active image is currently loaded into `image1`, you would probably load the new image software into `image2`. This lets you test the new software and reload the original active image (stored in `image1`), if needed.

To load a new software image to your switch, you need the following:

- The image or boot software loaded on a FTP/TFTP server on your network
- The hostname or IP address of the FTP/TFTP server
- The name of the new software image or boot file

Note: The DNS parameters must be configured if specifying hostnames.

When the above requirements are met, use the following procedure to download the new software to your switch.

1. In Privileged EXEC mode, enter the following command:

```
RS G7028# copy {ftp|tftp} {image1|image2|boot-image}
```

2. Select a port to use for downloading the image

```
Port type [DATA|MGT]:
```

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

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

4. Enter the name of the new software file on the server.

```
Source file name: <filename>
```

   The exact form of the name will vary by server. However, the file location is normally relative to the FTP or TFTP directory (usually `tftpboot`).

5. Enter your username and password for the server, if applicable.

```
User name: {<username>|<Enter>}
```

6. The system prompts you to confirm your request.

Next, select a software image to run, as described in the following section.

Selecting a Software Image to Run

You can select which software image (`image1` or `image2`) you want to run in switch memory for the next reboot.

1. In Global Configuration mode, enter:

```
RS G7028(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:

```
RS G7028# copy {image1|image2|boot-image} {ftp|tftp}
```

2. Select a port type to use for uploading the image.

```
Port type [DATA|MGT]:
```

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

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

4. Enter the name of the file into which the image will be uploaded on the FTP or TFTP server:

```
Destination file name: <filename>
```

5. Enter your username and password for the server, if applicable.

```
User name: {<username> | <Enter>}
```

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

```
image2 currently contains Software Version 6.6.0
 that was downloaded at  0:23:39 Thu Jan  3, 2011.
Upload will transfer image2 (2788535 bytes) to file "image1"
 on FTP/TFTP server 1.90.90.95.
Confirm upload operation (y/n) ? y
```

Selecting a Configuration Block

When you make configuration changes to the G7028/G7052, 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 G7028/G7052 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 G7028/G7052 is moved to a network environment where it will be re-configured for a different purpose.

In Global Configuration mode, use the following command to set which configuration block you want the switch to load the next time it is reset:

```
RS G7028(config)# boot configuration-block {active|backup|factory}
```

Setting an Entitlement Serial Number

To improve customer technical support, your customer support representative can assign your switch an Entitlement Serial Number (ESN) at the time you request support. The ESN can be conveniently stored on the switch using the following command:

```
RS G7028(config)# boot esn <Entitlement Serial Number>
```

The ESN helps to locate your switch's identifying information when you call technical support for help in future.

Resetting the Switch

You can reset the switch to make your software image file and configuration block changes occur.

Note: Resetting the switch causes the Spanning Tree Group to restart. This process can be lengthy, depending on the topology of your network.

Enter the following command to reset (reload) the switch:

```
>> RS G7028# 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) ?
```

Using the Boot Management Menu

The Boot Management menu allows you to switch the software image, reset the switch to factory defaults, or to recover from a failed software download.

You can interrupt the boot process and enter the Boot Management menu from the serial console port. When the system displays Memory Test, press **<Shift B>**. The Boot Management menu appears.

```
Resetting the System ...
Memory Test .............................

Boot Management Menu
1 - Change booting image
2 - Change configuration block
3 - Boot in recovery mode
4 - Xmodem download (for boot image only - use recovery mode for
application images)
5 - Reboot
6 - Exit

Please choose your menu option: 1
Current boot image is 1. Enter image to boot: 1 or 2: 2
Booting from image 2
```

The Boot Management menu allows you to perform the following actions:

- To change the booting image, press 1 and follow the screen prompts.
- To change the configuration block, press 2, and follow the screen prompts.
- To boot in recovery mode and to restore the application image, press 3 and follow the screen prompts.
- To download the boot image via xmodem, press 4 and follow the screen prompts.
- To reboot the system, press 5 and follow the screen prompts.
- To exit the Boot Management menu, press 6. The booting process continues.

Recovering from a Failed Upgrade

Use the following procedure to recover from a failed software upgrade.

1. Connect a PC to the serial port of the switch.
2. Open a terminal emulator program that supports XModem Download (for example, HyperTerminal, CRT, PuTTY) and select the following serial port characteristics:
   - Speed: 9600 bps
   - Data Bits: 8
   - Stop Bits: 1
   - Parity: None
   - Flow Control: None
3. Boot the switch and access the Boot Management menu by pressing **<Shift B>** while the Memory Test is in progress and the dots are being displayed.
4. Select **3** for **Xmodem download**. When you see the following message, change the Serial Port characteristics to 115200 bps:

```
## Switch baudrate to 115200 bps and press ENTER ...
```

5. Press <**Enter>** to set the system into download accept mode. When the readiness meter displays (a series of “C” characters), start XModem on your terminal emulator.
6. Select the Boot Image to download. The XModem initiates the file transfer. When the download is complete, a message similar to the following is displayed:

```
yzModem - CRC mode, 62494(SOH)/0(STX)/0(CAN) packets, 6 retries

Extracting images ... Do *NOT* power cycle the switch.

**** VMLINUX ****

Un-Protected 10 sectors

Erasing Flash.............. done

Writing to Flash.............done

Protected 10 sectors

**** RAMDISK ****

Un-Protected 44 sectors

Erasing Flash.............................................. done

Writing to Flash.............................................done

Protected 44 sectors

**** BOOT CODE ****

Un-Protected 8 sectors

Erasing Flash........... done

Writing to Flash...........done

Protected 8 sectors
```

7. When you see the following message, change the Serial Port characteristics to 9600 bps:

```
## Switch baudrate to 9600 bps and press ESC ...
```

8. Press the Escape key (<**Esc>**) to re-display the Boot Management menu.
9. Select **3** to start a new **XModem Download**. When you see the following message, change the Serial Port characteristics to 115200 bps:

```
## Switch baudrate to 115200 bps and press ENTER ...
```

10. Press <**Enter>** to continue the download.

11. Select the OS Image to download. The XModem initiates the file transfer. When the download is complete, a message similar to the following is displayed:

```
yzModem - CRC mode, 27186(SOH)/0(STX)/0(CAN) packets, 6 retries

Extracting images ... Do *NOT* power cycle the switch.

**** Switch OS ****


Please choose the Switch OS Image to upgrade [1|2|n] :
```

12. Select the image number to load the new image (1 or 2). It is recommended that you select 1. A message similar to the following is displayed:

```
Switch OS Image 1 ...

Un-Protected 27 sectors

Erasing Flash.............................. done

Writing to Flash.............................done

Protected 27 sectors
```

13. When you see the following message, change the Serial Port characteristics to 9600 bps:

```
## Switch baudrate to 9600 bps and press ESC ...
```

14. Press the Escape key (<**Esc>**) to re-display the Boot Management menu. Select **4** to exit and boot the new image.

Chapter 7. Maintenance Commands

The maintenance commands are used to manage dump information and forward database information. They include debugging commands to help with troubleshooting.

Dump information contains internal switch state data that is written to flash memory on the G7028/G7052 after any one of the following occurs:

- The watchdog timer forces a switch reset. The purpose of the watchdog timer is to reboot the switch if the switch software freezes.
- The switch detects a hardware or software problem that requires a reboot.

To use the maintenance commands, you must be logged in to the switch as the administrator.

Table 185. General Maintenance Commands

Command Syntax and Usage
`show flash-dump-uuencode` Displays dump information in uuencoded format. For details, see page 274. **Command mode:** All
`copy flash-dump {tftp|ftp} {data-port|mgt-port}` Saves the system dump information via TFTP, FTP. For details, see page 275. **Command mode:** Privileged EXEC
`copy` *<switch filename>* `tftp address` *<TFTP server address>* `filename` *<filename on TFTP server>* Saves a file via TFTP. **Command mode:** Privileged EXEC
`clear flash-dump` Clears dump information from flash memory. **Command mode:** Privileged EXEC
`copy log tftp {data|mgt}` Saves the system log file (SYSLOG) via TFTP. **Command mode:** Privileged EXEC
`clear log` Clears the system log file (SYSLOG). **Command mode:** Privileged EXEC

Table 185. General Maintenance Commands (continued)

Command Syntax and Usage
`show tech-support [l2|l3|link|port]` Dumps all G7028/G7052 information, statistics, and configuration. You can log the output (`tsdmp`) into a file. To filter the information, use the following options: – `l2` displays only Layer 2-related information – `l3` displays only Layer 3-related information – `link` displays only link status-related information – `port` displays only port-related information **Command mode:** All except User EXEC
`copy tech-support tftp {data|mgt}` Redirects the technical support dump (tsdmp) to an external TFTP server. **Command mode:** Privileged EXEC
`copy tech-support ftp {data|mgt}` Redirects the technical support dump (tsdmp) to an external FTP server. **Command mode:** Privileged 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 186. FDB Manipulation Options

Command Syntax and Usage
`show mac-address-table address` <*MAC address*> Displays a single database entry by its MAC address. Enter the MAC address using one of the following formats: – `xx:xx:xx:xx:xx:xx` (such as `08:00:20:12:34:56`) – `xxxxxxxxxxxx` (such as `080020123456`) **Command mode:** All
`show mac-address-table interface port` <*port number or alias*> Displays all FDB entries for a particular port. **Command mode:** All
`show mac-address-table vlan` <*VLAN number*> Displays all FDB entries on a single VLAN. **Command mode:** All
`show mac-address-table multicast` Displays all Multicast MAC entries in the FDB. **Command mode:** All
`show mac-address-table static` Displays static entries in the FBD. **Command mode:** All except User EXEC
`no mac-address-table {static|multicast} {all|`<*MAC address*> <*VLAN number*>`}` Removes static FDB entries. **Command mode:** Global configuration
`clear mac-address-table` Clears the entire Forwarding Database from switch memory. **Command mode:** Privileged EXEC

Debugging Commands

The Miscellaneous Debug Commands display trace buffer information about events that can be helpful in understanding switch operation. You can view the following information using the debug commands:

- Events traced by the Management Processor (MP)
- Events traced to a buffer area when a reset occurs

If the switch resets for any reason, the MP trace buffer is saved into the snap trace buffer area. The output from these commands can be interpreted by Technical Support personnel.

Table 187. Miscellaneous Debug Options

Command Syntax and Usage
`debug debug-flags` This command sets the flags that are used for debugging purposes. **Command mode:** Privileged EXEC

`debug mp-trace`
Displays the Management Processor trace buffer. Header information similar to the following is shown:
`MP trace buffer at 13:28:15 Fri May 25, 2001; mask: 0x2ffdf748`
The buffer information is displayed after the header.
Command mode: Privileged EXEC

`debug dumpbt` Displays the backtrace log. **Command mode:** Privileged 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:** Privileged EXEC
`clear flash-config` Deletes all flash configuration blocks. **Command mode:** Privileged EXEC
`[no] debug lacp packet [receive|transmit|both] [port` *<port numbers>*`]` Enables/disables debugging for Link Aggregation Control Protocol (LACP) packets on all ports running LACP. The following parameters are available: – `receive` filters only LACP packets received – `transmit` filters only LACP packets sent – `both` filters LACP packets either sent or received – `port` filters LACP packets sent/received on specific ports By default, LACP debugging is disabled. **Command mode:** Privileged EXEC

Table 187. Miscellaneous Debug Options

Command Syntax and Usage
`[no] debug spanning-tree bpdu [receive|transmit]` Enables/disables debugging for Spanning Tree Protocol (STP) Bridge Protocol Data Unit (BPDU) frames sent or received. The following parameters are available: – `receive` filters only BPDU frames received – `transmit` filters only BPDU frames sent By default, STP BPDU debugging is disabled. **Command mode**: Privileged EXEC

LLDP Cache Manipulation

Table 188 describes the LLDP cache manipulation commands.

Table 188. LLDP Cache Manipulation Options

Command Syntax and Usage
`show lldp receive` Displays information about the LLDP receive state machine. **Command mode:** All
`show lldp transmit` Displays information about the LLDP transmit state machine. **Command mode:** All
`show lldp remote-device [`*<1-256>*`|detail]` Displays information received from LLDP -capable devices. For more information, see page 48. **Command mode:** All
`show lldp` Displays all LLDP information. **Command mode:** All
`clear lldp` Clears the LLDP cache. **Command mode:** Privileged EXEC

IGMP Snooping Maintenance

Table 189 describes the IGMP Snooping maintenance commands.

Table 189. IGMP Multicast Group Maintenance Options

Command Syntax and Usage
`show ip igmp groups address` *<IP address>* Displays a single IGMP multicast group by its IP address. **Command mode:** All
`show ip igmp groups vlan` *<VLAN number>* Displays all IGMP multicast groups on a single VLAN. **Command mode:** All
`show ip igmp groups interface port` *<port number or alias>* Displays all IGMP multicast groups on selected ports. **Command mode:** All
`show ip igmp groups portchannel` *<trunk number>* Displays all IGMP multicast groups on a single trunk group. **Command mode:** All
`show ip igmp groups detail` *<IP address>* Displays detailed information about a single IGMP multicast group. **Command mode:** All
`show ip igmp groups` Displays information for all multicast groups. **Command mode:** All
`clear ip igmp groups` Clears the IGMP group table. **Command mode:** Privileged EXEC

IGMP Multicast Routers Maintenance

Table 190 describes the maintenance commands for IGMP multicast routers (Mrouters).

Table 190. IGMP Multicast Router Maintenance Commands

Command Syntax and Usage
`show ip igmp mrouter vlan` *<VLAN number>* Displays IGMP Mrouter information for a single VLAN. **Command mode:** All
`show ip igmp mrouter` Displays information for all Mrouters. **Command mode:** All
`show ip igmp mrouter information` Displays IGMP snooping information for all Mrouters. **Command mode:** All
`show ip igmp snoop igmpv3` Displays IGMPv3 snooping information. **Command mode:** All
`show ip igmp querier vlan` *<VLAN number>* Displays IGMP querier information for a single VLAN. **Command mode:** All
`clear ip igmp mrouter` Clears the IGMP Mrouter port table. **Command mode:** Privileged EXEC

LACP Maintenance

Table 191 describes the maintenance commands for LACP.

Table 191. LACP Maintenance Commands

Command Syntax and Usage
`qos protocol-packet-control packet-queue-map <`*packet queue number*`> lacp` Send an LACP Marker packet (for debugging only). **Command mode:** All

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 276.

To access dump information, enter:

```
RS G7028# 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 tftp`), 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:

```
RS G7028# copy flash-dump tftp <server filename>
```

You are prompted for the TFTP server IP address or hostname, and the *filename* of the target dump file.

To save dump information via FTP, enter:

```
RS G7028# copy flash-dump ftp  <server filename>
```

You are prompted for the FTP server IPv4 address or hostname, your *username* and *password*, and the *filename* of the target dump file.

Clearing Dump Information

To clear dump information from flash memory, enter:

```
RS G7028# clear flash-dump
```

The switch clears the dump region of flash memory and displays the following message:

```
FLASH dump region cleared.
```

If the flash dump region is already clear, the switch displays the following message:

```
FLASH dump region is already clear.
```

Unscheduled System Dumps

If there is an unscheduled system dump to flash memory, the following message is displayed when you log on to the switch:

```
Note: A system dump exists in FLASH. The dump was saved
      at 13:43:22 Wednesday January 30, 2011. Use show flash-dump
      uuencode to
      extract the dump for analysis and clear flash-dump to
      clear the FLASH region. The region must be cleared
      before another dump can be saved.
```

Appendix A. IBM N/OS System Log Messages

The G7028/G7052 uses the following syntax when outputting system log (syslog) messages:

<*Time stamp*><*IP/Hostname*><*Log Label*>IBMOS<*Thread ID*>: <*Message*>

The following parameters are used:

- <*Timestamp*>

  The time of the message event is displayed in the following format:

  <*month (3 characters)*> <*day*> <*hour (1-24)*>:<*minute*>:<*second*>

  For example: Aug 19 14:20:30

- <*IP/Hostname*>

  The hostname is displayed when configured.

  For example: 1.1.1.1

- <*Log Label*>

  The following types of log messages are recorded: LOG_CRIT, LOG_WARNING, LOG_ALERT, LOG_ERR, LOG_NOTICE, and LOG_INFO

- <*Thread ID*>

  This is the software thread that reports the log message. For example: stg, ip, console, telnet, system, web server, ssh

- <*Message*>: The log message

Following is a list of potential syslog messages. To keep this list as short as possible, only the <*Thread ID*> and <*Message*> are shown. The messages are sorted by <*Log Label*>.

Where the <*Thread ID*> is listed as mgmt, one of the following may be shown: console, telnet, web server, or ssh.

LOG_ALERT

Thread	LOG_ALERT Message
	Possible buffer overrun attack detected!
HOTLINKS	LACP trunk *<trunk ID>* and *<trunk ID>* formed with admin key *<key>*
IP	cannot contact default gateway *<IP address>*
IP	Route table full
MGMT	Maximum number of login failures (*<threshold>*) has been exceeded.
STP	CIST new root bridge
STP	CIST topology change detected
STP	STG *<STG>*, new root bridge
STP	STG *<STG>*, topology change detected
SYSTEM	LACP trunk *<trunk ID>* and *<trunk ID>* formed with admin key <key>

LOG_CRIT

Thread	LOG_CRIT Message
SSH	can't allocate memory in load_MP_INT()
SSH	currently not enough resource for loading RSA {private | public key}
SYSTEM	System memory is at <*n*> percent

LOG_ERR

Thread	LOG_ERR Message
CFG	Configuration file is EMPTY
CFG	Configuration is too large
CFG	Default VLAN cannot be a private-VLAN.
CFG	Error writing active config to FLASH! Configuration is too large
CFG	Error writing active config to FLASH! Unknown error
CFG	TFTP {Copy|cfgRcv} attempting to redirect a previously redirected output
MGMT	Apply is issued by another user. Try later
MGMT	Critical Error. Failed to add Interface <*interface*>
MGMT	Diff is issued by another user. Try later
MGMT	Dump is issued by another user. Try later
MGMT	Error: Apply not done
MGMT	Error: Save not done.
MGMT	Firmware download failed (insufficient memory
MGMT	Revert Apply is issued by another user. Try later
MGMT	Revert is issued by another user. Try later.
MGMT	Save is issued by another user. Try later
NTP	unable to listen to NTP port
PFC	PFC can be enabled on 2 priorities only - priority 3 and one other priority.
STP	Cannot set "{Hello Time | Max Age | Forward Delay | Aging}" (Switch is in MSTP mode)
SYSTEM	I2C device <*ID*> <*description*> set to access state <*state*> [from CLI]
SYSTEM	Not enough memory!

LOG_INFO

Thread	LOG_INFO Message
	System log cleared by user <*username*>.
	System log cleared via SNMP.
HOTLINKS	"Error" is set to "{Active | Standby}"
HOTLINKS	"Learning" is set to "{Active | Standby}"
HOTLINKS	"None" is set to "{Active | Standby}"
HOTLINKS	"Side Max" is set to "{Active | Standby}"
HOTLINKS	has no "{Side Max | None | Learning | Error}" interface
MGMT	/* Config changes at <time> by <*username*> */ <*config diff*> /* Done */
MGMT	<*username*> ejected from BBI
MGMT	<*username*>(<*user type*>) {logout | ejected | idle timeout | connection closed} from {Console | Telnet/SSH}
MGMT	<*username*>(<*user type*>) login {on Console | from host <*IP address*>}
MGMT	boot kernel download completed. Now writing to flash.
MGMT	boot kernel downloaded {from host <*hostname*> | via browser}, filename too long to be displayed, software version <*version*>
MGMT	boot kernel downloaded from host <*hostname*>, file'<*filename*>', software version <*version*>
MGMT	Can't downgrade to image with only single flash support
MGMT	Could not revert unsaved changes
MGMT	Download already currently in progress. Try again later via {Browser | BBI}
MGMT	Error in setting the new config
MGMT	Failed to allocate buffer for diff track.
MGMT	Firmware download failed to {invalid image | image1 | image2 | boot kernel | undefined | SP boot kernel}
MGMT	Firmware downloaded to {invalid image | image1 | image2 | boot kernel | undefined | SP boot kernel}.
MGMT	Flash dump successfully tftp'd to <*hostname*>:<*filename*>
MGMT	FLASH ERROR - invalid address used
MGMT	Flash Read Error. Failed to read flash into holding structure. Quitting

Thread	LOG_INFO Message (continued)
MGMT	Flash Write Error
MGMT	Flash Write Error. Failed to allocate buffer. Quitting
MGMT	Flash Write Error. Trying again
MGMT	image1 | 2 download completed. Now writing to flash.
MGMT	image1 | 2 downloaded {from host <*hostname*> | via browser}, filename too long to be displayed, software version <*version*>
MGMT	image1 | 2 downloaded from host <*hostname*>, file'<*filename*>', software version <*version*>
MGMT	Incorrect image being loaded
MGMT	Invalid diff track address. Continuing with apply()
MGMT	Invalid image being loaded for this switch type
MGMT	invalid image download completed. Now writing to flash.
MGMT	invalid image downloaded {from host <*hostname*> | via browser}, filename too long to be displayed, software version <*version*>
MGMT	invalid image downloaded from host <*hostname*>, file '<*filename*>', software version <*version*>
MGMT	New config set
MGMT	new configuration applied [from BBI | EM | SCP | SNMP]
MGMT	new configuration saved from {BBI | ISCLI | SNMP}
MGMT	scp<*username*>(<*user type*>) {logout | ejected | idle timeout | connection closed} from {Console | Telnet/SSH}
MGMT	scp<*username*>(<*user type*>) login {on Console | from host <*IP address*>}
MGMT	SP boot kernel download completed. Now writing to flash.
MGMT	SP boot kernel downloaded {from host <*hostname*> | via browser}, filename too long to be displayed, software version <*version*>
MGMT	SP boot kernel downloaded from host <*hostname*>, file '<*filename*>', software version <*version*>
MGMT	Starting Firmware download for {invalid image | image1 | image2 | boot kernel | undefined | SP boot kernel}.
MGMT	Static FDB entry on disabled VLAN
MGMT	Tech support dump failed
MGMT	Tech support dump successfully tftp'd to <*hostname*>:<*filename*>
MGMT	Two Phase Apply Failed in Creating Backup Config Block.
MGMT	undefined download completed. Now writing to flash.

Thread	LOG_INFO Message (continued)
MGMT	undefined downloaded {from host <*hostname*> | via browser}, filename too long to be displayed, software version <*version*>
MGMT	undefined downloaded from host <*hostname*>, file '<*filename*>', software version <*version*>
MGMT	unsaved changes reverted [from BBI | from SNMP]
MGMT	Unsupported GBIC {accepted | refused}
MGMT	user {SNMP user | <*username*>} ejected from BBI
MGMT	Watchdog has been {enabled | disabled}
MGMT	Watchdog timeout interval is now <*seconds*> seconds)
MGMT	Wrong config file type
SSH	<*username*>(<*user type*>) {logout | ejected | idle timeout | connection closed} from {Console | Telnet/SSH}
SSH	<*username*>(<*user type*>) login {on Console | from host <*IP address*>}
SSH	Error in setting the new config
SSH	New config set
SSH	scp<*username*>(<*user type*>) {logout | ejected | idle timeout | connection closed} from {Console | Telnet/SSH}
SSH	scp<*username*>(<*user type*>) login {on Console | from host <*IP address*>}
SSH	server key autogen {starts | completes}
SSH	Wrong config file type
SYSTEM	booted version <*version*> from Flash image <*image*>, {active | backup | factory} config block

LOG_NOTICE

Thread	LOG_NOTICE Message
	ARP table is full.
	Current config successfully tftp'd <*filename*> from <*hostname*>
	Current config successfully tftp'd to <*hostname*>: <*filename*>
	Port <*port*> mode is changed to full duplex for 1000 Mbps operation.
CONSOLE	RADIUS: authentication timeout. Retrying...
CONSOLE	RADIUS: failed to contact primary | secondary server
CONSOLE	RADIUS: No configured RADIUS server
CONSOLE	RADIUS: trying alternate server...
HOTLINKS	"Error" is set to "Standby | Active"
HOTLINKS	"Learning" is set to "Standby | Active"
HOTLINKS	"None" is set to "Standby | Active"
HOTLINKS	"Side Max" is set to "Standby | Active"
HOTLINKS	has no "{Side Max | None | Learning | Error}" interface
MGMT	<*username*> automatically logged out from BBI because changing of authentication type
MGMT	<*username*>(<*user type*>) {logout | ejected | idle timeout | connection closed} from {BBI | Console | Telnet/SSH}
MGMT	<*username*>(<*user type*>) login {on Console | from host <*IP address*> | from BBI}
MGMT	Authentication failed for backdoor.
MGMT	Authentication failed for backdoor. Password incorrect!
MGMT	Authentication failed for backdoor. Telnet disabled!
MGMT	boot config block changed
MGMT	boot image changed
MGMT	boot mode changed
MGMT	enable password changed
MGMT	Error in setting the new config
MGMT	Failed login attempt via {BBI | TELNET} from host <*IP address*>.
MGMT	Failed login attempt via the CONSOLE
MGMT	FLASH Dump cleared from BBI

Thread	LOG_NOTICE Message (continued)
MGMT	New config set
MGMT	packet-buffer statistics cleared
MGMT	PANIC command from CLI
MGMT	PASSWORD FIX-UP MODE IN USE
MGMT	Password for {oper | operator} changed by {SNMP user | <*username*>}, notifying admin to save.
MGMT	QSFP: Port <*port*> changed to {10G|40G}, from {BBI|SNMP|CLI}.
MGMT	RADIUS server timeouts
MGMT	RADIUS: authentication timeout. Retrying...
MGMT	RADIUS: failed to contact {primary|secondary} server
MGMT	RADIUS: No configured RADIUS server
MGMT	RADIUS: trying alternate server...
MGMT	scp<*username*>(<*user type*>) {logout | ejected | idle timeout | connection closed} from {Console | Telnet/SSH}
MGMT	scp<*username*>(<*user type*>) login {on Console | from host <*IP address*>}
MGMT	second syslog host changed to {this host | <*IP address*>}
MGMT	selectable [boot] mode changed
MGMT	STP BPDU statistics cleared
MGMT	switch reset from CLI
MGMT	syslog host changed to {this host | <*IP address*>}
MGMT	System clock set to <time>.
MGMT	System date set to <date>.
MGMT	Terminating BBI connection from host <*IP address*>
MGMT	User <*username*> deleted by {SNMP user | <*username*>}.
MGMT	User <*username*> is {deleted | disabled} and will be ejected by {SNMP user | <*username*>}
MGMT	User {oper | operator} is disabled and will be ejected by {SNMP user | <*username*>}.
MGMT	Wrong config file type
NTP	System clock updated
SERVER	link {down | up} on port <*port*>
SSH	(remote disconnect msg)

Thread	LOG_NOTICE Message (continued)
SSH	<*username*>(<*user type*>) {logout | ejected | idle timeout | connection closed} from {Console | Telnet/SSH}
SSH	<*username*>(<*user type*>) login {on Console | from host <*IP address*>}
SSH	Error in setting the new config
SSH	Failed login attempt via SSH
SSH	New config set
SSH	scp<*username*>(<*user type*>) {logout | ejected | idle timeout | connection closed} from {Console | Telnet/SSH}
SSH	scp<*username*>(<*user type*>) login {on Console | from host <*IP address*>}
SSH	Wrong config file type
SYSTEM	Change fibre GIG port <*port*> mode to full duplex
SYSTEM	Change fibre GIG port <*port*> speed to 1000
SYSTEM	Changed ARP entry for IP <*IP address*> to: MAC <MAC address>, Port <*port*>, VLAN <*VLAN*>
SYSTEM	Enable auto negotiation for copper GIG port: <*port*>
SYSTEM	I2C device <ID> <description> set to access state <state> [from CLI]
SYSTEM	Port <*port*> disabled
SYSTEM	Port <*port*> disabled due to reason code <*reason code*>
SYSTEM	rebooted (<*reason*>)[, administrator logged in] Reason: • Boot watchdog reset • console PANIC command • console RESET KEY • hard reset by SNMP • hard reset by WEB-UI • hard reset from console • hard reset from Telnet • low memory • MM Cycled Power Domain • power cycle • Reset Button was pushed • reset by SNMP • reset by WEB-UI • reset from console • reset from EM • reset from Telnet/SSH • scheduled reboot • SMS-64 found an over-voltage • SMS-64 found an under-voltage • software ASSERT • software PANIC • software VERIFY • Telnet PANIC command • unknown reason • watchdog timer
SYSTEM	Watchdog threshold changed from <old value> to <new value> seconds

Thread	LOG_NOTICE Message (continued)
SYSTEM	Watchdog timer has been enabled
TEAMING	error, action is undefined
TEAMING	is down, but teardown is blocked
TEAMING	is down, control ports are auto disabled
TEAMING	is up, control ports are auto controlled
VLAN	Default VLAN can not be deleted
WEB	<*username*> ejected from BBI
WEB	RSA host key is being saved to Flash ROM, please don't reboot the box immediately.

LOG_WARNING

Thread	LOG_WARNING Message
CFG	Authentication should be disabled to run RIPv2 in RIPv1 compatibility mode on interface <*interface*>.
CFG	Multicast should be disabled to run RIPv2 in RIPv1 compatibility mode on interface <*interface*>.
ETS	ETS prohibits a PG comprising of PFC and non-PFC traffic. Mixing in the same PG different PFC settings may affect the switch functionality.
HOTLINKS	"Error" is set to "Standby | Active"
HOTLINKS	"Learning" is set to "Standby | Active"
HOTLINKS	"None" is set to "Standby | Active"
HOTLINKS	"Side Max" is set to "Standby | Active"
HOTLINKS	has no "{Side Max | None | Learning | Error}" interface
NTP	cannot contact [primary | secondary] NTP server <*IP address*>
SYSTEM	I2C device <*ID*> <*description*> set to access state <*state*> [from CLI]
TEAMING	error, action is undefined
TEAMING	is down, but teardown is blocked
TEAMING	is down, control ports are auto disabled
TEAMING	is up, control ports are auto controlled

Appendix B. Getting help and technical assistance

If you need help, service, or technical assistance or just want more information about IBM products, you will find a wide variety of sources available from IBM to assist you. This section contains information about where to go for additional information about IBM and IBM products, what to do if you experience a problem with your system, and whom to call for service, if it is necessary.

Before you call

Before you call, make sure that you have taken these steps to try to solve the problem yourself:

- Check all cables to make sure that they are connected.
- Check the power switches to make sure that the system and any optional devices are turned on.
- Use the troubleshooting information in your system documentation, and use the diagnostic tools that come with your system. Information about diagnostic tools is in the *Problem Determination and Service Guide* on the IBM *Documentation* CD that comes with your system.
- Go to the IBM support website at http://www.ibm.com/systems/support/ to check for technical information, hints, tips, and new device drivers or to submit a request for information.

You can solve many problems without outside assistance by following the troubleshooting procedures that IBM provides in the online help or in the documentation that is provided with your IBM product. The documentation that comes with IBM systems also describes the diagnostic tests that you can perform. Most systems, operating systems, and programs come with documentation that contains troubleshooting procedures and explanations of error messages and error codes. If you suspect a software problem, see the documentation for the operating system or program.

Using the documentation

Information about your IBM system and pre-installed software, if any, or optional device is available in the documentation that comes with the product. That documentation can include printed documents, online documents, ReadMe files, and Help files. See the troubleshooting information in your system documentation for instructions for using the diagnostic programs. The troubleshooting information or the diagnostic programs might tell you that you need additional or updated device drivers or other software. IBM maintains pages on the World Wide Web where you can get the latest technical information and download device drivers and updates. To access these pages, go to http://www.ibm.com/systems/support/ and follow the instructions. Also, some documents are available through the IBM Publications Center at http://www.ibm.com/shop/publications/order/.

Getting help and information on the World Wide Web

On the World Wide Web, the IBM website has up-to-date information about IBM systems, optional devices, services, and support. The address for IBM System x® and xSeries® information is http://www.ibm.com/systems/x/. The address for IBM BladeCenter information is http://www.ibm.com/systems/bladecenter/. The address for IBM IntelliStation® information is http://www.ibm.com/intellistation/.

You can find service information for IBM systems and optional devices at http://www.ibm.com/systems/support/.t Line, you can get telephone assistance, for a fee, with usage, configuration, and software problems with System x and x Series servers, BladeCenter products, IntelliStation workstations, and appliances. For information about which products are supported by Support Line in your country or region, see http://www.ibm.com/services/sl/products/.

For more information about Support Line and other IBM services, see http://www.ibm.com/services/, or see http://www.ibm.com/planetwide/ for support telephone numbers. In the U.S. and Canada, call 1-800-IBM-SERV (1-800-426-7378).

Hardware service and support

You can receive hardware service through your IBM reseller or IBM Services. To locate a reseller authorized by IBM to provide warranty service, go to http://www.ibm.com/partnerworld/ and click **Find Business Partners** on the right side of the page. For IBM support telephone numbers, see http://www.ibm.com/planetwide/. In the U.S. and Canada, call 1-800-IBM-SERV (1-800-426-7378).

In the U.S. and Canada, hardware service and support is available 24 hours a day, 7 days a week. In the U.K., these services are available Monday through Friday, from 9 a.m. to 6 p.m.

IBM Taiwan product service

台灣 IBM 產品服務聯絡方式：
台灣國際商業機器股份有限公司
台北市松仁路 7 號 3 樓
電話：0800-016-888

IBM Taiwan product service contact information:

IBM Taiwan Corporation
3F, No 7, Song Ren Rd.
Taipei, Taiwan
Telephone: 0800-016-888

Index

Numerics

A

B

C

D

E

F

G

H

I

L

M

N

O

P

R

S

T

U

V

W