IBM

eserver

BladeCenter T 4-Port Gb Ethernet Switch Module

CLI Reference Guide

IBM

eserver

BladeCenter T 4-Port Gb
Ethernet Switch Module

CLI Reference Guide

First Edition (July 2004)

Contents

Chapter 1. Command-line interface management

The IBM® *@server* BladeCenter™ T 4-Port Gb Ethernet Switch Module supports a command-line interface (CLI) to set up and control a device over the network using TCP/IP Telnet. You can use the Telnet interface to perform the same network-management functions that you can perform using the Web Interface. You can also use the Telnet interface to configure the switch module for management using an SNMP-based network management system. This chapter describes how to use the CLI to access the Ethernet switch module, change its settings, and monitor its operation.

Important: Before configuring the Ethernet switch module, make sure that the management module in the BladeCenter T unit is configured correctly. To access and manage your switch module from an external environment, you might have to enable external ports or external management over all ports. See the management module *Installation Guide* and *User's Guide* on the IBM *BladeCenter T Documentation* CD for more information.

Command-line interface (CLI) conventions

The CLI syntax, conventions, and terminology are described in this section. Each CLI command in this document uses the following structure.

Syntax

Some commands, such as **show inventory,** do not require parameters. Other commands, such as **config lag deleteport**, have parameters for which you must supply values. Parameters are positional; you must type the values in the correct order. Optional parameters follow required parameters. For example:

```
config vlan mcaststorm vlan enable/disable [packets_per_second]
```

where

vlan is a variable that requires a value for the command.

enable/disable indicates that a choice of the listed values is required for the command.

[*packets_per_second*] is an optional variable for the command.

```
config lag deleteport logical_port port/listofports/all
```

where

logical_port is a required value for the command.

***port*/*listofports*/all** indicates a choice of the listed values must be entered as a required value for the command.

Parameters

The following conventions apply to the parameters:

- Parameters are order dependent.
- Variables, which must be replaced by values or text strings, are displayed in italic font.
- To use spaces as part of a name parameter, enclose the parameter in double quotation marks, for example, ″System Name with Space″.
- A parameter can be required or optional and might have a list of choices.
  - – ***variable*** Italics indicate that the parameter is required and you must enter a value in place of the text.
  - – **[*parameter*]** The square brackets indicate that the parameter is optional and you might choose to enter a value in place of the brackets and text.
  - – **choice1/choice2** Enter one and only one of the listed parameters.
  - – ***variable1/variable2*** Use one and only one of the listed variables.

Values

Some variables are used frequently. Use the following formats when providing values for them:

ipaddr Enter a valid IP address made up of four decimal digits ranging from 0 through 255. The default for all IP addresses consists of zeros (that is, 0.0.0.0). The interface IP address of 0.0.0.0 is invalid. In some cases, you can also enter the IP address as a 32-bit number.

macaddr The MAC address format is six hexadecimal numbers separated by hyphens, for example 00-06-29-32-81-40.

port This variable is used to identify a physical interface, in the form of bay.*port* for an I/O-module bay and ext.*port* for an external port. Enter a name and number separated by a period, for example:

bay.1 identifies I/O-module bay 1

ext.4 identifies external port 4

listofports This is a comma-separated list of valid ports, in one of the following forms:bay.*port*,bay.*port* ext.*port*,ext.*port*
Port lists must *not* contain spaces, and each interface must have its prefix specified (for example: bay.10,ext.2,bay.1).

logical_port This variable is used to identify a logical interface: a link aggregation group (LAG) or a VLAN. Enter a name and number separated by a period, for example:

lag.3 identifies LAG 3

vlan.2 identifies VLAN 2

character strings
Use double quotation marks to identify character strings, for example, ″System Name with Spaces″. An empty string (″″) is not valid.

Comments

When you are writing a test or configuration script, you can add comments by using the comment character “#” to flag the beginning of a comment. The comment character can appear anywhere on the command line, and all input following this character will be ignored. Any command line that begins with the character “#” is recognized as a comment line and is ignored by the parser.

For example:

#Script file for displaying the ip interface

#Display information about interfaces

show ip interface ext.1 #Displays information about the first external interface

#Display information about the next interface

show ip interface ext.2

#End of the script file

Special characters

Certain special key combinations speed up use of the CLI. They are listed in this section. Also, you can type `help` to display help.

Delete or Backspace
delete the previous character

Ctrl+A go to the beginning of line

Ctrl+E go to the end of line

Ctrl+F go forward one character

Ctrl+B go backward one character

Ctrl+D delete the current character

Ctrl+H display the command history or retrieve a command

Ctrl+U or Ctrl+X
delete to the beginning of the line

Ctrl+K delete to the end of the line

Ctrl+W delete the previous word

Ctrl+T transpose the previous character

Ctrl+P go to the previous line in the history buffer

Ctrl+N go to the next line in the history buffer

Ctrl+Z return to the root command prompt

Tab or Spacebar
Complete the command on the command line. After you have typed enough letters of a command name to uniquely identify the command, if you press the Spacebar or Tab key, the system will complete the command name. The prompt will change to the command name and you can type any required or optional parameters to complete the command.

Exit go to the next lower command prompt

!! execute the most recent command

!-n	execute the nth most recent command
!n	execute the nth command in the history buffer
!str	execute the most recent command that starts with the string “str”
!*str	execute the most recent command that contains the string “str”
?	list choices

Remotely managing the Ethernet switch module

The Ethernet switch module supports two remote-access modes for management over Ethernet connections. The switch module contains four external Ethernet ports and an internal Ethernet path to the management module.

The default mode uses the internal path to the management module only, and the remote-access link to the management console must be attached to the 100 Mbps Ethernet port on the management module. Use this mode to:

- Manually assign the IP addresses and SNMP parameters of the Ethernet switch modules through the management-module Web interface.
- Provide a secure LAN for management of the platform subsystems separately from the data network.

Note: In the default mode, the Ethernet switch module does not respond to remote management commands from the four external Ethernet ports on the switch module.

See the *Installation and User’s Guide* document on the IBM *BladeCenter T Documentation* CD for additional information.

You can choose to enable remote management of the Ethernet switch module through the four external Ethernet ports on the switch module, instead of or in addition to access through the management module. This mode can be enabled only through the management-module configuration interface. When this mode is enabled, the external Ethernet ports will support both management traffic and data traffic. Also, the Ethernet switch module will be able to transmit DHCP request frames through the external Ethernet ports.

This mode enables the switch module IP addresses to be on a different subnet than the management modules. This is useful when the switch modules are to be managed and controlled as part of the overall network infrastructure, while maintaining secure management of other chassis subsystems through the management module. However, management access to the Ethernet switch module link will be lost if the switch-module IP address is not on the same subnet as the management module. This chapter contains additional instructions for configuring the switch module for this mode of operation.

These two modes are applicable only to the Ethernet switch module. The management module can be remotely accessed only through the 100 Mbps Ethernet port on the management module.

Connecting to the Ethernet switch module

When you know the IP address for your switch module and have an existing network connection, you can use the Telnet program (in VT-100 compatible terminal mode) to access and control the switch module. If you have to obtain the IP address for your switch module or establish a network connection, consult your system or network administrator. Be sure to use the correct IP address in the required command, as specified in this section.

The Ethernet switch module supports user-based security that you can use to prevent unauthorized users from accessing the switch module or changing its settings. This section provides instructions for logging on to the switch module for the first time.

To connect to the switch module through the Telnet interface, type the following command from a DOS prompt command line:

```
telnet x.x.x.x
```

where *x.x.x.x* is the IP address of your switch module

When you first connect to the switch module, you will be prompted to enter a user ID followed by a password. Enter `USERID` in response to the prompt for a user ID and enter `PASSW0RD` in response to the prompt for a password (notice the use of the zero and not the “O”). This will give you read/write access to the switch module. By default, the switch module has one read-only account named ″guest″. The password for the read-only guest account is left blank, press Enter. For security, change these default passwords after you log on to the system for the first time.

Note: All user IDs and passwords are case sensitive.

A user with read/write privileges can add new user accounts, make changes to existing user accounts, and update firmware and configuration files.

Changing configuration settings

The Ethernet switch module has two levels of memory: normal random-access memory (RAM) and nonvolatile RAM (NVRAM). When a configuration change is entered, the new settings are immediately applied to the switching software in RAM. The new settings remain in effect until the switch is restarted or another change is made. To make the changes permanent you must enter the **save config** command to store the current configuration in NVRAM. After the switch-configuration settings are saved to NVRAM, they become the default settings for the switch. These settings are used every time the switch module is restarted.

Note: Some settings require you to restart the switch before they will take effect. Make sure that you save the new configuration to NVRAM first.

There are two ways to change the configuration that is stored in NVRAM:

- Save a new configuration by entering the **save config** command.
- Reset all configuration values to the initial settings that are listed in Appendix A, “Run-time switching software default settings,” on page 167 by entering the **clear config** command. This restores the configuration settings that were entered at the factory and causes the switch module to restart. If you load the factory-default configuration, all user accounts and configuration settings that you entered are erased and the switch module is returned to its original state.

Managing user accounts

Access to the Ethernet switch module is controlled through an authorized user ID and password. The switch supports a maximum of six user accounts, only one of which can have read/write privileges. The interface does not allow deletion of the currently logged-in user, to prevent accidental deletion of all the users with root privileges.

To log in after you have created a registered user, type `login` at a command-line prompt.

1. At the prompt, type your user ID and press Enter.
2. At the password prompt, type your password and press Enter.

Note: The passwords that are used to access the switch module are case sensitive.

Only the user with read/write privileges can add new user accounts or make changes to existing user accounts. Before you can update a user account, you must also enter the password (if any) for that user account.

Complete the following steps to update a user account:

1. Type
   ```
   config users passwd account password
   ```
   where *account* is the name of the account and *password* is the new account password.
2. Enter the old password when prompted. For an account without a password, press Enter.

To delete a user account, type

```
config users delete account
```

where *account* is the name of the account.

Initial configuration

You must enter some settings to enable the Ethernet switch module to be managed from an SNMP-based Network Management System or to access the switch module using the Telnet protocol. The switch module will assign an IP address to the switch, enabling it to be identified on the network using the DHCP protocol.

Dynamic Host Configuration Protocol (DHCP)

The Ethernet switch module sends out a Dynamic Host Configuration Protocol (DHCP) broadcast request when it is turned on. The DHCP protocol enables IP addresses, network masks, and default gateways to be assigned by a DHCP server.

Chapter 2. Ethernet switch-module system commands

This section describes the following commands that you use to configure and manage the switch:

- System information and statistics commands
- System configuration commands
- System description commands
- System utility commands
- Trap management commands

System information and statistics commands

These commands display and configure system information and statistics.

show arp switch

Use this command to display information about the connectivity between the switch and other devices. The Address Resolution Protocol (ARP) cache identifies the MAC addresses of the IP stations that communicate with the switch.

Syntax:

```
show arp switch
```

Return values:

MAC address
A unicast MAC address of a device on a subnet that is attached to one of the switch routing interfaces for which the switch has forwarding or filtering information. The format is six two-digit hexadecimal numbers separated by hyphens, for example 01-23-45-67-89-AB.

IP address
The IP address that is associated with the MAC address.

Port The identification of the port being used for the connection.

config forwardingdb agetime

Use this command to configure the forwarding database address aging timeout in seconds.

Syntax:

```
config forwardingdb agetime timeout
```

where the value for *timeout* is a positive integer ranging from 10 through 1000000 that indicates the address aging timeout, in seconds.

Default:
300

show forwardingdb agetime

Use this command to display information about the address aging timeout for the forwarding database.

Syntax:

```
show forwardingdb agetime
```

Return values:

Agetime The address aging timeout for the forwarding database in seconds.

show forwardingdb learned

Use this command to display information about forwarding database entries for learned addresses.

Syntax:

```
show forwardingdb learned
```

Return values:

MAC address A unicast MAC address for which the switch has forwarding or filtering information. The format is a two-byte hexadecimal VLAN ID number followed by a six-byte MAC address where each byte is separated by hyphens; for example, 00-01-00-23-45-67-89-AB.

Port The physical interface on which the MAC address was learned.

ifIndex The ifIndex of the MIB interface table entry associated with the port.

Status The status of the entry. The possible values are:

Static The value of the corresponding instance was added by the system or a user and cannot be relearned.

Learned
The entry was learned by observing the source MAC addresses of incoming traffic, and is currently in use.

Management
The system MAC address, identified with Bay.1.

Self The MAC address of one of the switch physical interfaces.

show forwardingdb table

Use this command to display information about the forwarding database entries. If the command is entered without a parameter or with the optional `all` parameter, the entire table is displayed. Enter a MAC address to display information about the table entry for that address and all entries following it.

Syntax:

```
show forwardingdb table
```

Return values:

MAC address A unicast MAC address for which the switch has forwarding or filtering information. The format is a two-byte hexadecimal VLAN ID number followed by a six-byte MAC address where each byte is separated by hyphens; for example, 00-01-00-23-45-67-89-AB.

Port The physical interface on which the MAC address was learned.

ifIndex The ifIndex of the MIB interface table entry associated with the port.

Status The status of the entry. The possible values are:

Static The value of the corresponding instance was added by the system or a user and cannot be relearned.

Learned
The entry was learned by observing the source MAC addresses of incoming traffic, and is currently in use.

Management
The system MAC address, identified with Bay.1.

Self The MAC address of one of the switch physical interfaces.

show inventory

Use this command to display information about inventory information for the switch.

Syntax:

```
show inventory
```

Return values:

Switch Description
The product name of this switch.

Machine Type The machine type of this switch.

Machine Model
The model within the machine type.

Serial Number
The unique box serial number for this switch.

FRU Number The field-replaceable unit number.

Part Number The manufacturing part number.

Maintenance Level
The identification of the hardware change level.

Manufacturer The two-octet code that identifies the manufacturer.

Burnedin MAC address
The burned-in universally administered MAC address of this switch.

Software Version
The release.version.maintenance number of the code currently running on the switch.

Operating System
The operating system currently running on the switch.

Network Processing Element
Identifies the network processor hardware.

Additional Packages
The list of optional software packages installed on the switch, if any. For example, Quality of Service.

show eventlog

Use this command to display information about the event log, which is used to hold error messages for catastrophic events. After the event is logged and the updated log is saved in FLASH memory, the switch will be reset. The log can hold at least 2,000 entries (the actual number depends on the platform and operating system), and is erased when an attempt is made to add an entry after it is full.

Note: Event log information is retained across a switch module reset.

Syntax:
```
show eventlog
```

Return values:

File The source code filename identifying the code that detected the event.

Line The line number within the source file of the code that detected the event.

Task Id The OS-assigned ID of the task reporting the event.

Code The event code passed to the event log handler by the code reporting the event.

Time The time the event occurred, measured from the previous reset.

show msglog

Use this command to display information about the message log.The message log contains system trace information that records non-critical problems.

Note: Message log information is not retained across a switch module reset and wraps after 512 entries.

Syntax:
```
show msglog
```

Return values:

Time The time the event occurred, calculated from the time the switch was last reset.

File The source code filename identifying the code that detected the event.

Line The line number within the source file of the code that detected the event.

Description An explanation of the problem being reported.

config port adminmode

Use this command to enable or disable one or more ports. The port will only be active in the network when it is enabled.

Syntax:
config port adminmode *port*/*listofports*/all enable/disable

Default:
```
enable
```

config port autoneg

Use this command to enable or disable automatic negotiation on one or more ports.

Syntax:
config port autoneg *port*/*listofports*/all enable/disable

Default:

```
enable
```

config port flowcontrol

Use this command to enable or disable IEEE 802.3x flow control for one or more ports.

Syntax:

```
config port flowcontrol port/listofports/all enable/disable
```

Default:

```
disable
```

config port lacpmode

Use this command to enable or disable the Link Aggregation Control Protocol (LACP) on one or more ports.

Syntax:

```
config port lacpmode port/listofports/all enable/disable
```

Default:

```
disable
```

config port linktrap

Use this command to enable or disable link status traps for one or more ports.

Note: This command is valid only when the Link Up/Down Flag is enabled (see “config trapflags linkmode” on page 36).

Syntax:

```
config port linktrap port/listofports/all enable/disable
```

config port physicalmode

Use this command to configure the speed and duplex mode for one or more ports. For this configuration to take effect, auto negotiation must be disabled.

Syntax:

```
config port physicalmode port/listofports/all duplexmode
```

where *duplexmode* has one of the following values:

1000f	1000BASE-T full duplex
100f	100BASE-T full duplex
100h	100BASE-T half-duplex
10f	10BASE-T full duplex
10h	10BASE-T half duplex

show port

Use this command to display information about a port.

Syntax:

```
show port port/listofports/all
```

Return values:

Port The interface number of the physical port or LAG whose information is displayed on the line.

Type If not blank, this field indicates that this port is a special type of port. The possible values are:

Mon Monitoring port, participating in Port Mirroring.

Probe Probe port, participating in Port Mirroring.

LAG Member of a LAG.

Admin Mode Displays information about the administration mode of the port. The port must be enabled in order for it to be allowed into the network. The factory default is enabled.

Physical Mode Displays information about the port speed and duplex mode. If auto-negotiation is specified for the port, then the duplex mode and speed will be set by the auto-negotiation process. Note that the port’s maximum capability (full duplex -100M) will be advertised. The factory default is auto.

Physical Status Indicates the port speed and duplex mode.

Link Status Indicates whether the link is up or down.

Link Trap Indicates whether or not a trap will be sent when link status changes. The factory default is enabled.

LACP Mode Displays information about whether Link Aggregation Control Protocol is enabled or disabled on this port.

FlowControl Mode Displays information about whether flow control is enabled or disabled on this port.

config mirroring create

Use this command to configure a probe port and a mirrored port for port mirroring. The first port is the probe port and the second port is the mirrored port. If this command is executed while port mirroring is enabled, it will change the probe and mirrored port values. The probe port will be removed from all VLANs.

Syntax:

```
config mirroring create port port
```

config mirroring delete

Use this command to remove the port mirroring designation from both the probe port and the mirrored port. The probe port must be manually added to any selected VLANs.

Syntax:

```
config mirroring delete
```

config mirroring mode

Use this command to enable or disable the port mirroring mode. The probe and mirrored ports must be configured before port mirroring can be enabled. If the port mirroring mode is enabled, the probe port will mirror all traffic received and transmitted on the physical mirrored port. It is not necessary to disable port mirroring before modifying the probe and mirrored ports.

Syntax:
```
config mirroring mode enable/disable
```

Default:
disable

show mirroring

Use this command to display the port mirroring information for the switch module.

Syntax:
```
show mirroring
```

Return values:

Port mirroring mode
Indicates whether the port mirroring feature is enabled or disabled.

Probe port The port that is configured as the probe port. If this value has not been configured, ‘Not Configured’ will be displayed.

Mirrored port The port that is configured as the mirrored port. If this value has not been configured, ‘Not Configured’ will be displayed.

config snmpcommunity accessmode

Use this command to configure SNMP access to switch information for a specific community name. The access mode can be Read-only (also called public) or Read/write (also called private).

Syntax:
```
config snmpcommunity accessmode readonly/readwrite name
```

config snmpcommunity create

Use this command to add and name a new SNMP community. A community name associates the switch with a set of SNMP managers and a specified privilege level. The name can be up to 16 alphanumeric (case-sensitive) characters long. Community names in the SNMP community table must be unique. In the case that there are multiple entries using the same community name, the first entry is kept and processed and all duplicate entries are ignored.

Syntax:
```
config snmpcommunity create name
```

Default:
There are two default community names: Public (with read-only access) and Private (with read/write access). You can replace these default community names with unique identifiers for each community. The default values for the remaining four community names are blank.

config snmpcommunity delete

Use this command to remove a name from the SNMP community table.

Syntax:

```
config snmpcommunity delete name
```

config snmpcommunity ipaddr

Use this command to specify the IP address (or portion thereof) from which this device will accept SNMP packets with the associated community name. The requesting entity's IP address is ANDed with the IP mask before being compared to this IP address. Note that if the IP mask is set to 0.0.0.0, an IP address of 0.0.0.0 matches all IP addresses. The default value is "0.0.0.0". The parameter *name* is the applicable community name, and may be up to 16 alphanumeric characters.

Syntax:

```
config snmpcommunity ipaddr ipaddr name
```

Default:

0.0.0.0

config snmpcommunity ipmask

Specify the mask to be ANDed with the requesting entity's IP address before comparison with the SNMP community IP address that is associated with the same community name. If the result matches the SNMP community IP address; then, the address is an authenticated IP address. For example, if the IP address = 9.47.128.0 and the corresponding IP mask = 255.255.255.0, a range of incoming IP addresses will match. For example, the incoming IP address could equal 9.47.128.0 - 9.47.128.255. The default value is "0.0.0.0". The parameter *name* is the applicable community name, and may be up to 16 alphanumeric characters.

Syntax:

```
config snmpcommunity ipmask ipmask name
```

Default:

0.0.0.0

config snmpcommunity mode

Use this command to activate or deactivate an SNMP community. If a community is enabled, an SNMP manager associated with this community is allowed to access the switch. If the community is disabled, no SNMP requests using this community name are accepted. In this case the SNMP manager associated with this community cannot manage the switch until the status is changed back to Enable.

Syntax:

```
config snmpcommunity mode enable/disable name
```

Default:

The default private and public communities are enabled by default. The four undefined communities are disabled by default.

show snmpcommunity

Use this command to display SNMP community information.

Up to six communities are supported. You can add, change, or delete communities. The switch does not have to be reset for changes to take effect.

The SNMP agent of the switch complies with SNMP Version 1. See the SNMP RFCs for more information about this SNMP specification. The SNMP agent sends traps through TCP/IP to an external SNMP manager based on the SNMP configuration (the trap receiver and other SNMP community parameters).

Syntax:

```
show snmpcommunity
```

Return values:

SNMP Community Name
The community name of this row of the table.

Client IP address
An IP address (or portion thereof) from which this device will accept SNMP packets with the associated community name. The requesting entity’s IP address is ANDed with the Client IP mask before being compared to the Client IP address. Note that if the Client IP mask is set to 0.0.0.0, an IP address of 0.0.0.0 matches all IP addresses. The default value is 0.0.0.0.

Client IP Mask
The mask that will be ANDed with the requesting entity’s IP address before comparison with the Client IP address. If the result matches the Client IP address then the address is an authenticated IP address. For example, if the IP address = 9.47.128.0 and the corresponding Client IP mask = 255.255.255.0, a range of incoming IP addresses would match, for example, the incoming IP address could equal 9.47.128.0 - 9.47.128.255. The default value is 0.0.0.0.

Access Mode The access level for this community. Either Read/write or Read-only.

Status The status of this community. Either enable or disable.

config snmptrap create

Use this command to add an SNMP trap receiver community name and associated IP address. The maximum length of name is 16 case-sensitive alphanumeric characters.

Syntax:

```
config snmptrap create name ipaddr
```

config snmptrap delete

Use this command to delete a trap receiver from a community.

Syntax:

```
config snmptrap delete name ipaddr
```

config snmptrap ipaddr

Use this command to assign a new IP address to a specified trap receiver community. The maximum length of name is 16 case-sensitive alphanumeric characters.

IP addresses in the SNMP trap receiver table must be unique. If you make multiple entries using the same IP address, the first entry is retained and processed. All duplicate entries are ignored.

Syntax:

```
config snmptrap ipaddr ipaddrold name ipaddrnew
```

config snmptrap mode

Use this command to enable or disable an SNMP trap receiver identified by trap receiver community name and IP address. Enabled trap receivers are active (able to receive traps). Disabled trap receivers are inactive (not able to receive traps).

Syntax:

```
config snmptrap mode enable/disable name ipaddr
```

show snmptrap

Use this command to display information about SNMP trap receivers. Trap messages are sent across the network to an SNMP Network Manager. These messages alert the manager to events occurring within the switch or on the network. Up to six trap receivers are supported at the same time.

Syntax:

```
show snmptrap
```

Return values:

SNMP Trap Name
The community string of the SNMP trap packet sent to the trap manager. Note that trap receiver communities and SNMP communities are separate and distinct.

IP address
The IP address that receives SNMP traps from the switch for this trap receiver community.

Status
Indicates whether traps are currently enabled for this community.

Enable -
traps will be sent.

Disable -
traps will not be sent.

System configuration commands

config loginsession close

Use this command to close a specified Telnet session.

Syntax:

```
config loginsession close sessionid/all
```

The sessionid can be obtained as a return value from the show loginsession commend (see the following information).

show loginsession

Use this command to display currently active Telnet and serial port connections to the switch.

Syntax:

```
show loginsession
```

Return values:

ID Login Session ID

User Name The account name used to login via the serial port or Telnet.

Connection From The IP address of the Telnet client machine or EIA-232 for the serial port connection.

Idle Time Time this session has been idle.

Session Time Total time this session has been connected.

config network javamode

Use this command to enable or disable the java applet that displays a picture of the switch module at the top right of the screen when you are using the Web interface. If you run the applet you will be able to click on the picture of the switch to select configuration screens instead of using the navigation tree at the left side of the screen. The factory default is disabled.

Syntax:

```
config network javamode enable/disable
```

Default:
disable

config network webmode

Use this command to enable or disable access to the switch module via the Web interface. When access is enabled a user can login to the switch from a web browser through TCP port 80. Disabling access takes effect immediately on all interfaces.

Syntax:

```
config network webmode enable/disable
```

Default:
enable

show network

Use this command to display network configuration settings that are necessary for in-band connectivity.

Syntax:

```
show network
```

Return values:

IP address The IP address of the interface. The factory default value is 0.0.0.0.

Subnet Mask The IP subnet mask for this interface. The factory default value is 0.0.0.0.

Default Gateway
The default IP gateway address for this interface. The factory default value is 0.0.0.0.

Burned In MAC address
The burned-in MAC address used for in-band connectivity if you choose not to configure a locally administered address.

Network Configuration Protocol Current
Indicates that the switch will transmit a DHCP request following power-up.

Web Mode
Indicates whether the switch may be accessed from a web browser. If web mode is enabled you can manage the switch from a web browser. The factory default is enabled.

Java Mode
Indicates whether the java applet that displays a picture of the switch at the top right of the screen is enabled or disabled. If the applet is enabled you will be able to click on the picture of the switch to select configuration screens instead of using the navigation tree at the left side of the screen. The factory default is disabled.

config telnet maxsessions

Use this command to configure the number of simultaneous Telnet and Secure Shell (SSH) sessions that can be established.

Syntax:

```
config telnet maxsessions sessions
```

where the value for *sessions* is a positive integer ranging from 0 through 5 that indicates the number of simultaneous Telnet sessions. A value of 0 indicates that no Telnet session can be established.

Default:
5

config telnet mode

Use this command to allow or disallow new Telnet sessions. If sessions are allowed, new Telnet sessions can be established until there are no more sessions available. If sessions are disabled, no new Telnet sessions are established but an established session will remain active until the session is terminated or an abnormal network error ends it.

Syntax:

```
config telnet mode enable/disable
```

Default:
enable

config telnet timeout

Use this command to specify the number of minutes of inactivity that will occur on a Telnet or SSH session before the switch logs off.

Changing the timeout value does not affect an active session until the session is reaccessed. Any keystroke will also activate the new timeout duration.

Syntax:

```
config telnet timeout minutes
```

where the value for *minutes* is a integer value ranging from 0 through 160 representing the timeout period in minutes. A value of 0 indicates there will be no timeout and the session will remain active indefinitely.

Default:
5

show telnet

Use this command to display Telnet settings.

Syntax:

```
show telnet
```

Return values:

Telnet Login Timeout (minutes)
The number of minutes of inactivity that will occur on a Telnet or SSH session before the switch logs off. A value of zero means there will be no timeout.

Maximum Number of Telnet Sessions
The number of simultaneous Telnet and SSH sessions allowed.

Allow New Telnet Sessions
Indicates whether new Telnet and SSH sessions are allowed.

config users add

Use this command to add a new user account if the maximum number of users has not been reached.

Syntax:

```
config users add name
```

where *name* is a text string representing a new user account name that is up to eight alphanumeric characters and is case-sensitive. A maximum of six user accounts can be defined.

config users delete

Use this command to remove a user account.

Note: The admin user account cannot be deleted.

Syntax:

```
config users delete name
```

where *name* is a text string representing an existing user account name.

config users passwd

Use this command to change the password of an existing user. The password is up to eight alphanumeric characters and is case-sensitive.

After you enter this command you will be prompted for the user password. If none, press enter.

Syntax:

```
config users passwd user
```

Default:

Blank (indicating no password) for users with Read-only access. For those with Read/write access the factory standard password is “PASSW0RD.” Please note the use of zero instead of the letter O.

config users snmpv3 accessmode

Use this command to specify the SNMPv3 access privileges for the specified user account. The valid accessmode values are `readonly` or `readwrite`. The *`user`* is the login user name for which the specified access mode will apply.

Syntax:

```
config users snmpv3 accessmode user readonly/readwrite
```

Default:

Readwrite for admin user; readonly for all other users

config users snmpv3 authentication

Use this command to specify the protocol to be used to authenticate a user account. The valid authentication protocols are none, md5 or sha. If md5 or sha are specified, the user login password will be used as the SNMPv3 authentication password. The *`user`* is the user account for which the specified authentication protocol will be used.

Syntax:

```
config users snmpv3 authentication user none/md5/sha
```

Default:

no authentication

config users snmpv3 encryption

Use this command to specify the encryption protocol and key to be used to authenticate a user account. The valid encryption protocols are none or DES. The DES protocol requires a key, which can be specified on the command line. The key may be up to 16 characters long. If the DES protocol is specified but a key is not provided, you will be prompted for the key. If none is specified as the protocol, you may not enter a key. The *`user`* is the user account for which the specified encryption protocol will be used.

Syntax:

```
config users snmpv3 encryption user none/des [key]
```

Default:

no encryption

show users info

Use this command to display the configured user names and their settings. This command is only available for the user with Read/write privileges.

Syntax:

```
show users info
```

Return values:

User Name The name the user will use to login using the serial port, Telnet or Web.

User Access Mode
Shows whether the user is able to change parameters on the switch (read/write) or is only able to view them (read-only). As a factory default, admin has Read/write access and guest has read-only access. There can only be one read/write user and up to five read-only users.

SNMPv3 Access Mode
Displays information about the SNMPv3 Access Mode. If the value is set to read/write, the SNMPv3 user will be able to set and retrieve parameters on the system. If the value is set to read-only, the SNMPv3 user will only be able to retrieve parameter information. The SNMPv3 access mode does not have to be the same as the CLI and Web access modes.

SNMPv3 Authentication
The protocol (if any) that will be used to authenticate the user.

SNMPv3 Encryption
The encryption protocol (if any) that will be used for the authentication process.

System description commands

config prompt

Use this command to change the prompt that is displayed when you use the CLI. You may enter up to 64 alphanumeric characters (which include the letters a through z, the numbers 0 through 9, and the underscore and dash characters).

Syntax:

```
config prompt system_prompt
```

config syscontact

Use this command to configure the name of the person or organization responsible for the switch. The range for contact is from 1 through 31 alphanumeric characters.

Syntax:

```
config syscontact contact
```

config syslocation

Use this command to configure the physical location assigned to the switch. The range for name is from 1 through 31 alphanumeric characters.

Syntax:

```
config syslocation location
```

config sysname

Use this command to configure the name assigned to the switch. The range for name is from 1 through 31 alphanumeric characters.

Syntax:

```
config sysname name
```

Display commands

show stats port detailed

Use this command to display detailed statistics for a specified port.

Syntax:

```
show stats port detailed port
```

Return values:

Packets Received

Octets Received
The total number of octets of data (including those in bad packets) received on the network (excluding framing bits but including FCS octets). This object can be used as a reasonable estimate of Ethernet utilization. If greater precision is desired, the etherStatsPkts and etherStatsOctets objects should be sampled before and after a common interval.

Packets Received 64 Octets
The total number of packets (including bad packets) received that were 64 octets in length (excluding framing bits but including FCS octets).

Packets Received 65-127 Octets
The total number of packets (including bad packets) received that were from 65 through 127 octets in length (excluding framing bits but including FCS octets).

Packets Received 128-255 Octets
The total number of packets (including bad packets) received that were from 128 through 255 octets in length (excluding framing bits but including FCS octets).

Packets Received 256-511 Octets
The total number of packets (including bad packets) received that were from 256 through 511 octets in length (excluding framing bits but including FCS octets).

Packets Received 512-1023 Octets
The total number of packets (including bad packets) received that were from 512 through 1023 octets in length (excluding framing bits but including FCS octets).

Packets Received 1024-1518 Octets
The total number of packets (including bad packets) received that were from 1024 through 1518 octets in length (excluding framing bits but including FCS octets).

Packets Received 1519-1522 Octets
The total number of packets (including bad packets) received that were from 1519 through 1522 octets in length (excluding framing bits but including FCS octets).

Packets Received >1522 Octets
The total number of packets (including bad packets) received that were >1522 octets in length (excluding framing bits but including FCS octets).

Packets Received Successfully

Total Packets Received Without Error
The total number of packets received that were without error.

Unicast Packets Received
The number of subnetwork-unicast packets delivered to a higher-layer protocol.

Multicast Packets Received
The number of packets received that were directed to a multicast address. Note that this number does not include packets directed to the broadcast address.

Broadcast Packets Received
The number of packets received that were directed to a broadcast address. Note that this number does not include packets directed to the multicast address.

Packets Received with MAC Errors

Total Packets Received with MAC Errors
The total number of inbound packets that contained errors that prevented them from being delivered to a higher-layer protocol.

Jabbers Received
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). Note that this definition of jabber is different than the definition in IEEE-802.3 section 8.2.1.5 (10BASE5) and section 10.3.1.4 (10BASE2). These documents define jabber as the condition where any packet exceeds 20 ms. The allowed range to detect jabber is 20 ms through 150 ms.

Fragments/Undersized Received
The total number of packets received that were less than 64 octets in length (excluding framing bits but including FCS octets).

Alignment Errors
The total number of packets received that had a length (excluding framing bits but including FCS octets) of 64 through 1518 octets, inclusive, but had a bad Frame Check Sequence (FCS) with a non-integral number of octets.

Rx FCS Errors
The total number of packets received that had a length (excluding framing bits but including FCS octets) of 64 through 1518 octets, inclusive, but had a bad Frame Check Sequence (FCS) with an integral number of octets.

Received Packets Not Forwarded

802.3x Pause Frames Received
A count of MAC Control frames received on this interface with an opcode indicating the PAUSE operation. This counter does not increment when the interface is operating in half-duplex mode.

Packets Transmitted

Total Packets Transmitted (Octets)
The total number of octets of data (including those in bad packets) transmitted on the network (excluding framing bits but including FCS octets). This object can be used as a reasonable estimate of Ethernet utilization. If greater precision is desired, the etherStatsPkts and etherStatsOctets objects should be sampled before and after a common interval.

Packets Transmitted 64 Octets
The total number of packets (including bad packets) transmitted that were 64 octets in length (excluding framing bits but including FCS octets).

Packets Transmitted 65-127 Octets
The total number of packets (including bad packets) transmitted that were from 65 through 127 octets in length (excluding framing bits but including FCS octets).

Packets Transmitted 128-255 Octets
The total number of packets (including bad packets) transmitted that were from 128 through 255 octets in length (excluding framing bits but including FCS octets).

Packets Transmitted 256-511 Octets
The total number of packets (including bad packets) transmitted that were from 256 through 511 octets in length (excluding framing bits but including FCS octets).

Packets Transmitted 512-1023 Octets
The total number of packets (including bad packets) transmitted that were from 512 through 1023 octets in length (excluding framing bits but including FCS octets).

Packets Transmitted 1024-1518 Octets
The total number of packets (including bad packets) transmitted that were from 1024 through 1518 octets in length (excluding framing bits but including FCS octets).

Packets Transmitted 1519-1522 Octets
The total number of packets (including bad packets) transmitted that were from 1519 through 1522 octets in length (excluding framing bits but including FCS octets).

Max Info The maximum size of the Info (non-MAC) field that this port will receive or transmit.

Packets Transmitted Successfully

Total Packets Transmitted Successfully
The total number of packets that have been transmitted by this port to its segment.

Unicast Packets Transmitted
The total number of packets that higher-level protocols requested be transmitted to a subnetwork-unicast address, including those that were discarded or not sent.

Multicast Packets Transmitted
The total number of packets that higher-level protocols requested be transmitted to a multicast address, including those that were discarded or not sent.

Broadcast Packets Transmitted
The total number of packets that higher-level protocols requested be transmitted to a broadcast address, including those that were discarded or not sent.

Transmit Errors

Total Transmit Errors
The sum of Single, Multiple and Excessive Collisions.

Tx FCS Errors
The total number of packets transmitted that had a length (excluding framing bits but including FCS octets) from 64 through 1518 octets, inclusive, but had a bad Frame Check Sequence (FCS) with an integral number of octets.

Tx Oversized The total number of packets that exceeded the maximum permitted frame size. This counter has a maximum increment rate of 815 counts per second at 10 Mbps.

Underrun Errors
The total number of packets discarded because the transmit FIFO buffer became empty during frame transmission.

Transmit Discards

Total Transmit Packet Discarded
The sum of single collision frames discarded, multiple collision frames discarded, and excessive collision frames discarded.

Single Collision Frames
The number of successfully transmitted packets which encountered exactly one collision.

Multiple Collision Frames
The number of successfully transmitted packets which encountered more than one collision.

Excessive Collision Frames
The number of packets which were not successfully transmitted because of excessive collisions.

Protocol Statistics

BPDUs Received
The number of BPDUs (Bridge Protocol Data Units) received by the spanning tree layer.

BPDUs Transmitted
The number of BPDUs (Bridge Protocol Data Units) transmitted from the spanning tree layer.

802.3x Pause Frames Transmitted
The number of MAC Control frames received on this interface with an opcode indicating the PAUSE operation. This counter does not increment when the interface is operating in half-duplex mode.

GVRP PDUs Received
The number of GARP VLAN Registration Protocol (GVRP) PDUs received by the Generic Attributes Registration Protocol (GARP) layer.

GVRP PDUs Transmitted
The number of GVRP PDUs transmitted by the GARP layer.

GVRP PDUs Failed Registrations
The number of times attempted GVRP registrations could not be completed.

GMRP PDUs Received
The number of GMRP PDUs received.

GMRP PDUs Transmitted
The number of GMRP PDUs transmitted.

GMRP PDUs Failed Registrations
The number of times attempted GMRP registrations could not be completed.

Time Since Counters Last Cleared
The elapsed time in days, hours, minutes and seconds since the statistics for this port were last cleared.

show stats port summary

Use this command to display a summary of the statistics for a specified port.

Syntax:

```
show stats port summary port
```

Return values:

Packets Received Without Error
The total number of packets (including multicast and broadcast packets) received on this port.

Packets Received With Error
The number of inbound packets that contained errors that prevented them being delivered to a higher-layer protocol.

Broadcast Packets Received
The total number of packets received that were directed to the broadcast address. Note that this does not include multicast packets.

Packets Transmitted Without Error
The total number of packets transmitted from the interface.

Transmit Packet Errors
The number of outbound packets that could not be transmitted because of errors.

Collision frames
The best estimate of the total number of collisions on this Ethernet segment.

Time Since Counters Last Cleared
The elapsed time in days, hours, minutes and seconds since the statistics for this port were last cleared.

show stats switch detailed

Use this command to display detailed statistics for all CPU traffic.

Syntax:

```
show stats switch detailed
```

Return values:

Received

Octets Received
The total number of octets of data received by the processor (excluding framing bits but including FCS octets).

Packets Received Without Errors
Total number of packets received on the network.

Unicast Packets Received
The number of subnetwork-unicast packets delivered to a higher-layer protocol.

Multicast Packets Received
The number of packets received that were directed to a multicast address. Note that this number does not include packets directed to the broadcast address.

Broadcast Packets Received
The number of packets received that were directed to a broadcast address. Note that this number does not include packets directed to the multicast address.

Receive Packets Discarded
The number of inbound packets that were chosen to be discarded even though no errors had been detected that would prevent their being deliverable to a higher-layer protocol. One possible reason for discarding a packet could be to free up buffer space.

Transmitted

Octets Transmitted
The total number of octets of data transmitted on the network including framing bits.

Packets Transmitted Without Errors
The total number of packets that have been transmitted on the network.

Unicast Packets Transmitted
The total number of packets that higher-level protocols requested be transmitted to a subnetwork-unicast address, including those that were discarded or not sent.

Multicast Packets Transmitted
The total number of packets that higher-level protocols requested be transmitted to a multicast address, including those that were discarded or not sent.

Broadcast Packets Transmitted
The total number of packets that higher-level protocols requested be transmitted to a broadcast address, including those that were discarded or not sent.

Transmit Packets Discarded
The number of outbound packets that were chosen to be discarded even though no errors had been detected. One possible reason for discarding a packet could be to free up buffer space.

Table Entries

Most Address Entries Ever Used
The highest number of Forwarding Database Address Table entries used by this switch module since the last reboot.

Address Entries In Use
The number of learned and static Forwarding Database Address Table entries currently in use by this switch module.

VLAN Entries

Maximum VLAN Entries
The maximum number of VLANs enabled on the switch module.

Most VLAN Entries Ever Used
The highest number of VLANs that have been active on this switch module since the last reboot.

Static VLAN Entries
The number of VLANs currently active on this switch module that were created statically.

Dynamic VLAN Entries
The number of VLANs currently active on this switch module that were created by GVRP registration.

VLAN Deletes The number of VLANs that have been created and then deleted on this switch module since the last reboot.

Time Since Counters Last Cleared
The elapsed time in days, hours, minutes and seconds since the statistics for this port were last cleared.

show stats switch summary

Use this command to display a summary of the statistics for all switch traffic.

Syntax:

```
show stats switch summary
```

Return values:

Packets Received Without Error
The total number of packets (including multicast and broadcast packets) received by the processor.

Broadcast Packets Received
The total number of packets received that were directed to the broadcast address. Note that this does not include multicast packets.

Packets Received With Error
The number of inbound packets that contained errors that prevented them being delivered to a higher-layer protocol.

Packets Transmitted Without Errors
The total number of packets transmitted from the switch module.

Broadcast Packets Transmitted
The total number of packets that higher-layer protocols requested to be transmitted to the broadcast address, including those that were discarded or not sent.

Transmit Packet Errors
The number of outbound packets that could not be transmitted because of errors.

Address Entries Currently In Use
The number of learned and static Forwarding Database Address Table entries currently in use by this switch module.

VLAN Entries Currently In Use
The number of VLANs currently in the VLAN table on this switch module.

Time Since Counters Last Cleared
The elapsed time in days, hours, minutes and seconds since the statistics for the switch were last cleared.

show sysinfo

Use this command to display switch information.

Syntax:
```
show sysinfo
```

Return values:

Switch Description
The product name of the switch.

System Name
The name used to identify the switch.

System Location
Text used to identify the location of the switch. May be up to 31 alphanumeric characters. The factory default is blank.

System Contact
Text used to identify a contact person for the switch. May be up to 31 alphanumeric characters. The factory default is blank.

System ObjectID
The base object ID for the switch enterprise MIB.

System Up Time
The time in days, hours and minutes since the last reboot.

MIBs Supported
The list of MIBs supported by the management agent running on the switch.

System utility commands

The commands in this section allow you to fine tune your systems performance and functionality.

clear config

Use this command to reset the configuration of the switch module to the factory defaults. The switch is automatically reset when this command is processed. All configuration changes that you have made, including those saved to NVRAM, will be lost. You will be prompted to confirm that the reset should proceed.

Syntax:
```
clear config
```

clear igmpsnooping

Use this command to clear the tables managed by the Internet Group Management Protocol (IGMP) Snooping function. The switch will attempt to delete these entries from the Multicast Forwarding Database (MFDB). You will be prompted to confirm that you want to issue this command.

Syntax:
```
clear igmpsnooping
```

clear lag

Use this command to clear all LAGs. You will be prompted to confirm that you want to issue this command.

Syntax:

```
clear lag
```

clear pass

Use this command to reset all user passwords to the factory defaults. You will be prompted to confirm that the password reset should proceed.

Syntax:

```
clear pass
```

clear stats port

Use this command to clear the statistics for a specified port. You will be prompted to confirm that you want to issue this command.

Syntax:

```
clear stats port port/listofports/all
```

clear stats switch

Use this command to clear the statistics for the switch. You will be prompted to confirm that you want to issue this command.

Syntax:

```
clear stats switch
```

clear transfer

Use this command to reset the file transfer parameters to the factory defaults. You will be prompted to confirm that you want to issue this command.

Syntax:

```
clear transfer
```

clear traplog

Use this command to clear the trap log. You will be prompted to confirm that you want to issue this command.

Syntax:

```
clear traplog
```

clear vlan

Use this command to reset the VLAN configuration parameters to the factory defaults. You will be prompted to confirm that you want to issue this command.

Syntax:

```
clear vlan
```

logout

Use this command to close the current Telnet connection or reset the current serial connection. If you have any saved configuration changes, you will be prompted to save them. If you logout without issuing a **save config** command any configuration changes you have made will be lost.

Syntax:

```
logout
```

ping

Use this command to have the switch transmit a Ping request to a specified IP address. This checks whether the switch can communicate with a particular IP device. The switch will send three Ping requests and display the results. The switch can be pinged from any IP workstation with which it is connected through the default VLAN (VLAN 1), as long as there is a physical path between the switch and the workstation.

Syntax:

```
ping ipaddr
```

reset system

Use this command to reset the switch without powering it off. Reset means that all network connections are terminated and the boot code executes. The switch uses the stored configuration to initialize the switch. You will be prompted to confirm that the reset should proceed. A successful reset is indicated by the LEDs on the switch.

Syntax:

```
reset system
```

save config

Use this command to permanently save configuration changes made since the previous save or reboot to Non-Volatile Random Access Memory (NVRAM). You are prompted to verify your choice.

Syntax:

```
save config
```

show history

Use this command to show the contents of the command history buffer. The output will display the oldest command in the history buffer first and the **show history** command (the newest command) last.

Syntax:

```
show history
```

transfer download datatype

Use this command to configure the type of file to be downloaded to the switch.

Syntax:

```
transfer download datatype config/code/sshkey-rsa1/sshkey-rsa2/sshkey-
dsa/sslpem-root/sslpem-server/sslpem-dhweak/sslpem-dhstrong
```

where datatype type is one of the following:

config	Configuration file
code	Code file
sshkey-rsa1	SSH RSA1 Key file
sshkey-rsa2	SSH RSA2 Key file
sshkey-dsa	SSH DSA Key file
sslpem-root	Secure Root PEM file
sslpem-server	Secure Server PEM file
sslpem-dhweak	Secure DH Weak PEM file
sslpem-dhstrong	Secure DH Strong PEM file

Default:
code

transfer download filename

Use this command to specify the name of the file that is to be downloaded to the switch. The switch will remember the last file name used.

You may specify the file path as part of the file name if the string is less than 31 characters. Otherwise, use the transfer download path command.

This command is valid only when the Transfer Mode is TFTP. See transfer download mode.

Syntax:
```
transfer download filename name
```

transfer download path

Use this command to specify the directory path on the TFTP server where the file to be downloaded to the switch is located. The switch will remember the last file path used.

This command is valid only when the Transfer Mode is TFTP. See **transfer download mode**. Details of the TFTP path are explained under the command **transfer upload path**.

Syntax:
```
transfer download path path
```

transfer download serverip

Use this command to configure the IP address of the server on which a file to be downloaded is located. This command is valid only when the transfer mode is TFTP. See **transfer download mode**.

Syntax:
```
transfer download serverip ipaddr
```

Default:
0.0.0.0

transfer download start

Use this command to start a download transfer. After the current settings are displayed you will be prompted to confirm your decision. This command will close your connection to the host.

Syntax:
```
transfer download start
```

The following information fields are displayed:

TFTP Server IP
The IP address of the server where the file is to be downloaded.

TFTP Path The directory path specification for the file to be downloaded.

TFTP Filename
The name of the file to be downloaded.

Where datatype is one of the following:

config Configuration file

code Code file

sshkey-rsa1 SSH RSA1 Key file

sshkey-rsa2 SSH RSA2 Key file

sshkey-dsa SSH DSA Key file

sslpem-root Secure Root PEM file

sslpem-server
Secure Server PEM file

sslpem-dhweak
Secure DH Weak PEM file

sslpem-dhstrong
Secure DH Strong PEM file

TFTP upload example

This example shows three ways to specify the same TFTP client-to-server file transfer. Each scenario involves uploading the config.bin file from the switch to the location c:\tftp\ on the server. The different scenarios are shown below:

Table 1. TFTP Upload Scenarios

TFTP Server path	TFTP Client path
c:\tftp\	blank
c:\	tftp\
c:	\tftp\

The directory path statement can be cleared by issuing the **clear config** command.

transfer upload datatype

Use this command to specify the type of file to be uploaded from the switch.

Syntax:

```
transfer upload datatype config/errorlog/msglog/traplog
```

Where datatype type is one of the following:

config	Configuration file
errlog	Error log file
msglog	Message log file
traplog	Trap log file

transfer upload filename

Use this command to specify the name of the file to be uploaded from the switch. The switch will remember the last file name used.

You may specify the file path as part of the file name if the string is less than 31 characters. Otherwise, use the **transfer upload path** command to specify the directory path.

This command is valid only when the Transfer Mode is TFTP. See **transfer upload mode**.

Syntax:

```
transfer upload filename name
```

transfer upload path

Use this command to specify the directory path on the TFTP server where you want to save a file uploaded from the switch. The switch will remember the last file path used.

Note: This command is valid only when the transfer mode is TFTP. See the command, **transfer upload mode**.

The Ethernet switch module software supports the use of a TFTP client. The TFTP client path statement requirement is server dependent. A path statement is generally required to setup the TFTP client; however, the client path may remain blank.

Syntax:

```
transfer upload path path
```

transfer upload serverip

Use this command to configure the IP address of the server on which a file to be uploaded is to be located. It is valid only when the transfer mode is TFTP. See **transfer upload mode**.

Syntax:

```
transfer upload serverip ipaddr
```

Default:
0.0.0.0

transfer upload start

Use this command to start an upload transfer. After the current settings are displayed you will be prompted to confirm your decision. Note that issuing this command will close your connection to the host.

Syntax:

```
transfer upload start
```

The following information fields are displayed:

TFTP Server IP address
The Internet Protocol (IP) address of the server where the file is to be uploaded.

TFTP File Path
The directory path specification for the file to be uploaded.

TFTP File Name
The name to be given to the file after it has been uploaded.

File Type
The type of file to be uploaded: config, error log, message log or trap log.

Trap management

config trapflags authentication

Use this command to enable or disable the Authentication Flag, which determines whether a trap message is sent when the switch detects an authentication failure.

Syntax:

```
config trapflags authentication enable/disable
```

Default:
enable

config trapflags dvmrp

Use this command to enable or disable sending DVMRP traps.

Syntax:

```
config trapflags dvmrp enable/disable
```

Default:
enable

config trapflags linkmode

Use this command to enable or disable Link Up/Down traps for the entire switch. When enabled, link trap messages are sent only if the Link Trap flag associated with the affected port is also set to enabled.

Syntax:

```
config trapflags linkmode enable/disable
```

Default:
enable

config trapflags multiusers

Use this command to enable or disable Multiple User traps. When enabled, a multiple user trap message is sent when a user logs in to the terminal interface (EIA 232 or Telnet) and there is an existing terminal interface session for the same user account.

Syntax:

```
config trapflags multiusers enable/disable
```

Default:
enable

config trapflags ospf

This command enables or disables OSPF traps.

Syntax:

```
config trapflags ospf enable/disable
```

Default:
enable

config trapflags pim

Use this command to enable or disable sending PIM traps.

Syntax:

```
config trapflags pim enable/disable
```

Default:
enable

config trapflags stpmode

Use this command to enable or disable STP traps. When enabled, topology change notification trap messages will be sent.

Syntax:

```
config trapflags stpmode enable/disable
```

Default:
enable

show trapflags

Use this command to display trap conditions. When the condition identified by an active trap is encountered by the switch a trap message will be sent to any enabled SNMP Trap Receivers, and a message will be written to the trap log. Cold and warm start traps are always enabled.

Syntax:

```
show trapflags
```

Return values:

Authentication Flag
Indicates whether authentication failure traps will be sent (enable) or not (disable).

Link Up/Down Flag
Indicates whether a trap will be sent when the link status changes from up to down or vice versa.

Multiple Users Flag
Indicates whether a trap will be sent when the same user ID is logged into the switch more than once at the same time (either via Telnet or serial port).

Spanning Tree Flag
Indicates whether spanning tree traps will be sent.

show traplog

Use this command to display the trap log.

Note: Trap log information is not retained across a switch module reset.

Syntax:

```
show traplog
```

Return values:

Number of Traps Since Last Reset
The number of traps that have occurred since the last time the switch was reset.

Number of Traps Since Log Last Viewed
The number of traps that have occurred since the traps were last displayed. Displaying the traps by any method (terminal interface display, Web display, upload file from switch, and so on.) will cause this counter to be cleared to 0.

Log The sequence number of this trap.

System Up Time
The time at which this trap occurred, expressed in days, hours, minutes and seconds since the last reboot of the switch.

Trap Information identifying the trap.

Chapter 3. Switching configuration commands

This section describes the commands you use to manage the switch and to show the current management settings.

This section also provides detailed explanations of the switching commands. The commands are divided into nine groups:

- Generic Attributes Registration Protocol (GARP) commands
- IGMP snooping commands
- Link Aggregation (LAG) commands
- MAC filter commands
- Multicast Forwarding Database (MFDB) commands
- Protocol-based VLAN commands
- Spanning tree commands
- Virtual Local Area Network (VLAN) commands

Generic Attribute Registration Protocol (GARP) commands

config garp gmrp adminmode

Use this command to enable or disable the GARP Multicast Registration Protocol (GMRP) on the switch module.

Syntax:

```
config garp gmrp adminmode enable/disable
```

Default:
disable

config garp gmrp interfacemode

Use this command to enable or disable the GMRP on one, some, or all interfaces. If an interface which has GARP enabled is enabled for routing or is made a member of a LAG, GARP functionality will be disabled on that interface. GARP functionality will subsequently be re-enabled if routing is disabled or LAG membership is removed from an interface that previously had GARP enabled.

Syntax:

```
config garp grmp interfacemode port/listofports/all enable/disable
```

Default:
disable

config garp gvrp adminmode

Use this command to enable or disable GVRP on the switch module.

Syntax:

```
config garp gvrp adminmode enable/disable
```

Default:
disable

config garp gvrp interfacemode

Use this command to enable or disable GVRP for one, some, or all interfaces. If GVRP is disabled, Join Time, Leave Time, and LeaveAll Time have no effect.

Syntax:

```
config garp gvrp interfacemode port/listofports/all enable/disable
```

Default:
disable

config garp jointimer

Use this command to configure the GARP join time for the specified ports. Join time is the interval between the transmission of GARP Protocol Data Units (PDUs) registering (or re-registering) membership for a VLAN or multicast group.

This command has an effect only when GVRP is enabled.

Syntax:

```
config garp jointimer port/listofports/all join_time
```

where *join_time* is an integer value ranging from 10 through 100 representing the GARP join time in centiseconds.

Default:
20 centiseconds (0.2 seconds)

config garp leavealltimer

Use this command to configure how frequently LeaveAll PDUs are generated for the specified ports. A LeaveAll PDU indicates that all registrations will be unregistered. Participants would need to rejoin in order to maintain registration. The value applies per port and per GARP participation.

This command has an effect only when GVRP is enabled.

Syntax:

```
config garp leavealltimer port/listofports/all time
```

where *time* is an integer value ranging from 200 through 6000 in centiseconds.

Default:
1000 centiseconds (10 seconds)

config garp leavetimer

Use this command to configure the GARP leave time for the specified ports. Leave time is the time to wait after receiving an unregistered request for a VLAN or a multicast group before deleting the VLAN entry or group. This allows time for another station to assert registration for the same attribute in order to maintain uninterrupted service.

This command has an effect only when GVRP is enabled.

Syntax:

```
config garp leavetimer port/listofports/all leave_time
```

where *leave_time* is an integer value ranging from 20 through 600 representing the GARP leave time in centiseconds.

Default:
60 centiseconds (0.6 seconds)

show garp info

Use this command to display GARP information for the Ethernet switch module.

Syntax:
```
show garp info
```

Return values:

GMRP Admin Mode
This displays information about the administrative mode of GMRP for the switch module. The default is disable.

GVRP Admin Mode
This displays information about the administrative mode of GVRP for the Ethernet switch module. The default is disable.

show garp interface

Use this command to display GARP information for one, some or all interfaces.

Syntax:
`show garp interface` *`port`*`/`*`listofports`*`/all`

Return values:

Port This displays information about the identification of the interface that this row in the table describes.

Join Timer Displays the interval between the transmission of GARP PDUs registering (or re-registering) membership for an attribute. Current attributes are a VLAN or a multicast group. There is an instance of this timer on a per-port, per-GARP participant basis. Permissible values are 10 through 100 centiseconds (0.1 through 1.0 seconds) in increments of 1 centisecond (0.01 seconds). The factory default is 20 centiseconds (0.2 seconds).

Leave Timer Displays the period of time to wait after receiving an unregistered request for an attribute before deleting the attribute. Current attributes are a VLAN or a multicast group. This allows time for another station to assert registration for the same attribute in order to maintain uninterrupted service. There is an instance of this timer on a per-port, per-GARP participant basis. Permissible values are 20 through 600 centiseconds (0.2 through 6.0 seconds) in increments of 1 centisecond (0.01 seconds). The factory default is 60 centiseconds (0.6 seconds).

LeaveAll Timer
Shows how frequently LeaveAll PDUs are generated. A LeaveAll PDU indicates that all registrations will shortly be deregistered. Participants will need to rejoin in order to maintain registration. There is an instance of this timer on a per-port, per-GARP participant basis. The LeaveAll Period Time is set to a random value in the range of LeaveAll Time to (1.5*LeaveAll Time). This

value is chosen randomly to avoid network loading if all participants use the same timer values. Permissible values are 200 through 6000 centiseconds (2 through 60 seconds) in increments of 1 centisecond (0.01 seconds). The factory default is 1000 centiseconds (10 seconds).

Port GMRP Mode
Indicates the GMRP administrative mode for the port. It may be enabled or disabled. If this parameter is disabled, Join Time, Leave Time, and LeaveAll Time have no effect. The factory default is disabled.

Port GVRP Mode
Indicates the GVRP administrative mode for the port. It may be enabled or disabled. If this parameter is disabled, Join Time, Leave Time, and LeaveAll Time have no effect. The factory default is disabled.

IGMP snooping commands

config igmpsnooping adminmode

Use this command to enable or disable IGMP Snooping on the switch module.

Syntax:

```
config igmpsnooping adminmode enable/disable
```

Default:
disable

config igmpsnooping groupmembershipinterval

Use this command to configure the IGMP Group Membership Interval time on the Ethernet switch module. The group membership interval time is the amount of time in seconds that a switch will wait for a report from a particular group on a particular interface before deleting the interface from the entry. This value must be greater than the IGMP maximum response time value.

Syntax:

```
config igmpsnooping groupmembershipinterval seconds
```

where *seconds* is an integer value ranging from 2 through 3600 representing the group membership interval time in seconds.

Default:
260 seconds

config igmpsnooping interfacemode

Use this command to enable or disable IGMP Snooping on a selected interface. The `port/listofports/all` parameter identifies the interfaces on which to enable or disable IGMP Snooping. If an interface which has IGMP Snooping enabled is enabled for routing or becomes a member of a LAG, IGMP Snooping functionality will be disabled on that interface. IGMP Snooping functionality will subsequently be re-enabled if routing is disabled, or the interface is deleted from the LAG.

Syntax:

```
config igmpsnooping interfacemode port/listofports/all enable/disable
```

Default:
disable

config igmpsnooping maxresponse

Use this command to configure the IGMP Maximum Response time on the Ethernet switch module. The maximum response time is the amount of time in seconds that a switch will wait after sending a query on an interface because it did not receive a report for a particular group in that interface. This value must be less than the IGMP query interval time value.

Syntax:

```
    config igmpsnooping maxresponse seconds
```

where *seconds* is 1 through 3599. A value of 0 indicates an infinite timeout and the time will not expire.

Default:
10 seconds

config igmpsnooping mcrtrexpiretime

Use this command to configure the Multicast Router Present Expiration time on the switch module. This is the amount of time in seconds that a switch will wait for a query to be received on an interface before the interface is removed from the list of interfaces with multicast routers attached.

Syntax:

```
config igmpsnooping mcrtrexpiretime seconds
```

where *seconds* is an integer value ranging from 0 through 3600 representing the expiration time in seconds. A value of 0 indicates an infinite timeout and the time will not expire.

Default:
0

show igmpsnooping

Use this command to display IGMP Snooping information for the Ethernet switch module. Configuration information is displayed whether or not IGMP Snooping is enabled. Status information is only displayed when IGMP Snooping is enabled.

Syntax:

```
    show igmpsnooping
```

Return values:

Admin Mode This indicates whether or not IGMP Snooping is enabled on the switch.

Group Membership Interval (secs)
This displays the IGMP Query Interval Time. This is the amount of time the switch will wait for a report for a particular group on a particular interface before it sends a query on that interface.

Max Response Time (secs)
This displays the amount of time the switch will wait after sending a query on an interface because it did not receive a report for a particular group on that interface.

Multicast Router Present Expiration Time (secs)
If a query is not received on an interface within this amount of time, the interface is removed from the list of interfaces with multicast routers attached.

Interfaces Enabled for IGMP Snooping
This is the list of interfaces on which IGMP Snooping is enabled.

The following status value is only displayed when IGMP Snooping is enabled.

Multicast Control Frame Count
This displays the number of multicast control packets that have been processed by the CPU.

Link Aggregation (LAG) commands

config lag addport

Use this command to add a physical port to a LAG. The first interface parameter designation is of a configured LAG and the second identifies the port to be added. There can be a maximum of 8 member ports.

Syntax:

```
config lag addport logical_port port
```

config lag adminmode

Use this command to enable or disable the specified LAg or LAGs. The option `all` sets all of the configured LAGs to the same administrative mode setting.

Syntax:

```
config lag adminmode logical_port/listofports/all enable/disable
```

config lag create

Use this command to configure a new LAG, assign a name to it, and generate a logical port number for it. To display the assigned logical port number use the **show lag** command. The *name* parameter is a string of up to 15 alphanumeric characters.

Syntax:

```
config lag create name
```

config lag deletelag

Use this command to delete the specified LAGs. The `all` option removes all configured LAGs.

Syntax:

```
config lag deletelag logical_port/listofports/all
```

config lag deleteport

Use this command to delete one or more ports from a LAG. The first interface parameter designates a configured LAG. The second interface number designates a port that is a member of the LAG. Use `all` to delete all ports in the specified LAG.

Syntax:
```
config lag deleteport logical_port port/listofports/all
```

config lag linktrap

Use this command to enable or disable link trap notifications for the specified LAG. The option `all` sets every configured LAG to the same administrative mode setting.

Syntax:
```
config lag linktrap logical_port/listofports/all enable/disable
```

Default:
enable

config lag name

Use this command to define or modify a name for the specified LAG. Name is an alphanumeric string up to 15 characters.

Syntax:
```
config lag name logical_port_name
```

show lag

Use this command to display an overview of all link aggregation groups (LAGs) on the switch.

Syntax:
```
show lag logical_port/listofports/all
```

Return values:

Logical Port The logical port identifying the LAG, in the format lag.port.

LAG Name The name of this LAG.

Link State Indicates whether the link is up or down.

Admin Mode The administrative mode. The factory default is enabled.

Link Trap Mode
Indicates whether or not a trap will be sent when link status changes. The factory default is enabled.

STP Mode The Spanning Tree Protocol Administrative Mode associated with the LAG. The possible values are:

Disable -
Spanning tree is disabled for this LAG.

Enable -
Spanning tree is enabled for this LAG.

Mbr Ports A listing of the ports that are members of this LAG, in port notation. There can be a maximum of 8 ports assigned to a given LAG.

Port Speed The speed of the LAG. A LAG is always full-duplex.

MAC filter commands

config macfilter adddest

Use this command to add the *port* to the destination filter set for the MAC filter with the MAC address of *macaddr* and VLAN of *vlan*. The *macaddr* parameter must be specified as a 6-byte hexadecimal number in the format of 00-12-34-56-78-90. The *vlan* parameter must identify a valid VLAN.

The *port* parameter identifies the destination ports to be added to the destination port filter set for the MAC filter. If `all` is selected, all ports will be added to the destination port filter set. Packets for the specified MAC address and VLAN ID will only be transmitted out of ports that are in the filter set.

Syntax:

```
config macfilter adddest macaddr vlan port/listofports/all
```

config macfilter create

Use this command to add a static MAC filter entry for a MAC address and VLAN pair. The *macaddr* parameter must be specified as a 6-byte hexadecimal number in the format of 00-12-34-56-78-90.

Filters may not be defined for MAC addresses:

- 00-00-00-00-00-00
- 01-80-C2-00-00-00 to 01-80-C2-00-00-0F
- 01-80-C2-00-00-20 to 01-80-C2-00-00-21
- FF-FF-FF-FF-FF-FF

The *vlan* parameter must identify a valid VLAN.

Up to 100 static MAC filters may be created.

Syntax:

```
config macfilter create macaddr vlan
```

config macfilter deldest

Use this command to remove one or more ports from the destination filter set for the MAC filter with the MAC address of *macaddr* and VLAN of *vlan*. The *macaddr* parameter must be specified as a 6-byte hexadecimal number in the format of 00-12-34-56-78-90. The *vlan* parameter must identify a valid VLAN.

The *port* parameter identifies the destination ports to be removed from the destination port filter set for the MAC filter. If `all` is selected, all ports will be removed from the destination port filter set.

Syntax:

```
config macfilter deldest macaddr vlan port/listofports/all
```

config macfilter remove

Use this command to remove the static MAC filter entry for the given MAC address on the VLAN. The *macaddr* parameter must be specified as a 6-byte hexadecimal number in the format of 00-12-34-56-78-90. The *vlan* parameter must identify a valid VLAN.

Syntax:

```
config macfilter remove macaddr vlan
```

show macfilter

Use this command to display the Static MAC Filtering information. If `all` is selected as the first parameter, all the Static MAC Filters in the switch module are displayed. If a *macaddr* is entered, a VLAN ID must also be entered and the Static MAC Filter information will be displayed only for that MAC address and VLAN ID pair.

Syntax:

```
show macfilter all/macaddr all/vlan
```

Return values:

MAC address The MAC address of the static MAC filter entry.

VLAN ID The VLAN ID of the static MAC filter entry.

Destination Ports
The ports in the destination filter. Packets with the associated MAC address and VLAN ID will only be transmitted out of ports in the list.

Multicast Forwarding Database (MFDB) commands

show mfdb gmrp

Use this command to display the GMRP entries in the Multicast Forwarding Database (MFDB) table.

Syntax:

```
    show mfdb gmrp
```

Return values:

Mac Address A MAC address and VLAN pair for which the switch has forwarding or filtering information. The format is two, two-digit hexadecimal numbers, representing the VLAN and six, two-digit hexadecimal numbers, representing the MAC address, separated by hyphens; for example, 00-01-00-23-45-67-89-AB.

Type Displays the type of the entry. Static entries are those that are configured by the end user. Dynamic entries are added to the table as a result of a learning process or protocol.

Description The text description of this multicast table entry.

Interfaces The list of interfaces that are designated for forwarding (Fwd:) and filtering (Flt:).

show mfdb igmpsnooping

Use this command to display the IGMP Snooping entries in the MFDB.

Syntax:

```
show mfdb igmpsnooping
```

Return values:

Mac Address A MAC address and VLAN pair for which the switch has forwarding or filtering information. The format is two, two-digit hexadecimal numbers, representing the VLAN and six, two-digit hexadecimal numbers, representing the MAC address, separated by hyphens; for example, 00-01-00-23-45-67-89-AB.

Type Displays the type of the entry. Static entries are those that are configured by the end user. Dynamic entries are added to the table as a result of a learning process or protocol.

Description The text description of this multicast table entry.

Interfaces The list of interfaces that are designated for forwarding (Fwd:) and filtering (Flt:).

show mfdb staticfiltering

Use this command to display the Static Filtering entries in the MFDB.

Syntax:

```
show mfdb staticfiltering
```

Return values:

Mac Address A MAC address and a VLAN pair for which the switch has forwarding or filtering information. The format is two, two-digit hexadecimal numbers, representing the VLAN; and, six, two-digit hexadecimal numbers, representing the MAC address, separated by hyphens. For example, 00-01-00-23-45-67-89-AB.

Type Displays the type of the entry. Static entries are those that are configured by the end user. Dynamic entries are added to the table as a result of a learning process or protocol.

Description The text description of this multicast table entry.

Interfaces The list of interfaces that are designated for forwarding (Fwd:) and filtering (Flt:).

show mfdb stats

Use this command to display the MFDB statistics.

Syntax:

```
    show mfdb stats
```

Return values:

Max MFDB Table Entries
Displays the total number of entries possible in the MFDB table.

Most MFDB Entries Since Last Reset
Displays the largest number of entries that have been present in the MFDB table since the switch was reset. This value is also known as the MFDB high-water mark.

Current Entries
Displays the current number of entries in the MFDB table.

show mfdb table

Use this command to display the MFDB information. If the command is entered without a parameter or with the optional `all` parameter, the entire table is displayed. The user can display the table entry for one MAC address by specifying the MAC address as an optional parameter.

Syntax:

```
show mfdb table [macaddr/all]
```

Return values:

Mac Address A MAC address and a VLAN pair for which the switch has forwarding or filtering information. The format is two, two-digit hexadecimal numbers, representing the VLAN and six, two-digit hexadecimal numbers, representing the MAC address, separated by hyphens; for example, 00-01-00-23-45-67-89-AB.

Type This displays the type of the entry. Static entries are those that are configured by the end user. Dynamic entries are added to the table as a result of a learning process or protocol.

Component The component that is responsible for this entry in the MFDB. Possible values are IGMP Snooping, GMRP, and Static Filtering.

Description The text description of this multicast table entry.

Interfaces The list of interfaces that are designated for forwarding (Fwd:) and filtering (Flt:).

Forwarding Interfaces
The forwarding list is derived from combining all of the component forwarding interfaces and removing the interfaces that are listed as the static filtering interfaces.

Protocol-based VLAN commands

config protocol create

Use this command to add a protocol-based VLAN group to the Ethernet switch module. The parameter *groupname* is a character string of 1 through 16 characters. When it is created, the protocol group will be assigned a unique number that will be used to identify the group in subsequent commands. Use the **show protocol** command to display the assigned number.

Syntax:

```
config protocol create groupname
```

config protocol delete

Use this command to remove the protocol-based VLAN group identified by the specified *groupname*.

Syntax:

```
config protocol delete groupname
```

where *groupname* is a character string ranging from 1 through 16 characters.

config protocol interface add

Use this command to add one or more interfaces to the protocol-based VLAN identified by *groupid*. If `all` is selected, all physical interfaces will be added to the protocol group. A group may have more than one interface associated with it. Each interface and protocol combination can only be associated with one group. If adding an interface to a group causes any conflicts with protocols currently associated with the group, this command will fail and the interfaces will not be added to the group.

Syntax:

```
config protocol interface add groupid port/listofports/all
```

config protocol interface remove

Use this command to remove the interface from the protocol-based VLAN group identified by *groupid*. If `all` is selected, all ports will be removed from the protocol group.

Syntax:

```
config protocol interface remove groupid port/listofports/all
```

config protocol protocol add

Use this command to add the specified protocol to the protocol-based VLAN identified by *groupid*. A group may have more than one protocol associated with it. Each interface and protocol combination can only be associated with one group. If adding a protocol to a group causes any conflicts with interfaces currently associated with the group, this command will fail and the protocol will not be added to the group. The possible values for protocol are IP, ARP, and IPX.

Syntax:

```
config protocol protocol add groupid protocol
```

config protocol protocol remove

Use this command to remove the *protocol* from the protocol-based VLAN group that is identified by the *groupid*. The possible values for protocol are IP, ARP, and IPX.

Syntax:

```
config protocol protocol remove groupid protocol
```

config protocol vlan add

Use this command to attach a *vlan* to the protocol-based VLAN identified by *groupid*. A group may only be associated with one VLAN at a time, however the VLAN association can be changed.

Syntax:

```
config protocol vlan add groupid vlan
```

config protocol vlan remove

Use this command to remove the *vlan* from the protocol-based VLAN group identified by the *groupid*.

Syntax:

```
config protocol vlan remove groupid vlan
```

show protocol

Use this command to display the protocol-based VLAN information for either the specified group or for all groups.

Syntax:

```
show protocol groupid/all
```

Return values:

Group Name This field displays the group name of an entry in the protocol-based VLAN table.

Group ID This field displays the group identifier of the protocol group.

Protocols This field indicates the protocols included in the group, one or more of IP, ARP, and IPX.

VLAN This field indicates the VLAN ID associated with this protocol group. All ports in the group will assign this VLAN ID to untagged packets received for the protocols identified for the group.

Interfaces This field lists the port interfaces that are associated with this protocol group. Note that an interface can only belong to one group for a given protocol.

Spanning tree commands

This section contains the following 4 types spanning tree commands:

- Spanning tree bridge commands
- Spanning tree Common Spanning Tree (CST) commands
- Spanning tree port commands
- Spanning tree summary commands

config spanningtree bridge forwarddelay

Use this command to configure the Bridge Forward Delay parameter to a new value. Forwarddelay is used by bridges to ensure that a new network topology has stabilized before leaving the blocking state.

Syntax:

```
config spanningtree bridge forwarddelay seconds
```

where *seconds* is an integer value ranging from 4 through 30 with the value being greater than or equal to ((Bridge Max Age / 2) + 1), and representing the forward delay in seconds.

Default:
15

config spanningtree bridge hellotime

Use this command to configure the Hello Time parameter to a new value. Hellotime determines how often a hello message is broadcast; it cannot be longer than MaxAge but should be longer than forwarddelay.

Syntax:

```
config spanningtree bridge hellotime hellotime_value
```

where *hellotime_value* is an integer ranging from 1 through 10 with the value being less than or equal to ((Bridge Max Age / 2) - 1), and representing how often a hello message is broadcast, in seconds.

Default:
2

config spanningtree bridge maxage

Use this command to configure the Bridge Max Age parameter to a new value. This is the value that all bridges use for maxage when this bridge is acting as the root: A BPDU will be discarded when its age exceeds maxage.

Syntax:
```
config spanningtree bridge maxage seconds
```

where *seconds* is an integer ranging from 6 through 40, with the value being less than or equal to (2 times (Bridge Forward Delay - 1)), and representing the maxage in seconds.

Default:
6

config spanningtree bridge priority

Use this command to configure the Bridge Priority parameter to a new value. The bridge priority value is the first two octets of the eight octet Bridge ID. The lower the number the higher the priority. The twelve least significant bits will be masked according to the IEEE 802.1s specification. This will cause the priority to be rounded down to the next lower valid priority.

Syntax:
```
config spanningtree bridge priority priority_value
```

where *priority_value* is a value ranging from 0 through 61440.

Default:
32768

show spanningtree bridge

Use this command to display the STP settings for the bridge.

Syntax:
```
show spanningtree bridge
```

Return values:

Bridge Priority
The priority component of the bridge identifier. Valid values range from 0-61440, in increments of 4096. The lower the number the higher the priority. The factory default is 32768.

Bridge Identifier
The unique identifier associated with this bridge instance. It consists of the bridge priority and the bridge base MAC address.

Bridge Max Age

The value that all bridges use for Max Age when this bridge is acting as the root: a BPDU will be discarded when its age exceeds maxage.

Bridge Hello Time

The value that all bridges use for HelloTime when this bridge is acting as the root. Hellotime determines how often a hello message is broadcast; it cannot be longer than maxage but should be longer than forwarddelay.

Bridge Forward Delay

The value that all bridges use for Forward Delay when this bridge is acting as the root. Forwarddelay is used by bridges to ensure that a new network topology has stabilized before leaving the blocking state. Note that IEEE 802.1D specifies that the range for this parameter is related to the value of STP Bridge Maximum Age.

Bridge Hold Time

Minimum time between transmission of Configuration Bridge Protocol Data Units (BPDUs).

config spanningtree cst port edgeport

Use this command to specify whether a port is an edge port within the Common Spanning Tree (CST). This will enable the port to transition to Forwarding State without delay. The *port* is the port to be affected. The edgeport value can either be “true” or “false”.

Syntax:

```
config spanningtree cst port edgeport port true/false
```

Default:

false

config spanningtree cst port pathcost

Use this command to configure the path cost to a new value for the specified port in the CST. The *port* is the port to be affected. The pathcost value can be specified as a number in the range of 1 through 200000000 or auto. If `auto` is specified, the pathcost value will be set based on Link Speed.

Syntax:

```
config spanningtree cst port pathcost port cost/auto
```

where *cost* is a value ranging from 1 through 200000000.

Default:

auto

config spanningtree cst port priority

Use this command to configure the port priority to a new value for use within the CST. The *port* is the port to be affected.

Syntax:

```
config spanningtree cst port priority port priority_value
```

where *priority_value* is an integer in the range of 0 through 240 in increments of 16.

Default:
128

show spanningtree cst detailed

Use this command to display STP settings for the CST.

Syntax:
```
show spanningtree cst detailed
```

Return values:

Bridge Priority
The value of the first two octets of the eight octet Bridge ID. Valid values are 0 through 61440. Factory default is 32768.

Bridge Identifier
The unique identifier associated with this bridge instance.

Time Since Topology Change
The time (in seconds) since the last time a topology change was detected by the bridge entity.

Topology Change Count
The total number of topology changes detected by this bridge since the management entity was last reset or initialized.

Topology Change in progress
Boolean value of the topology change parameter for the switch indicating whether a topology change is in progress on any port assigned to the CST.

Designated Root
The identifier of the bridge currently assumed to be the root of the spanning tree.

Root Path Cost
The cost of the path to the root as seen from this bridge.

Root Port Identifier
The port number of the port which offers the lowest cost path from this bridge to the root bridge.

Root Port Max Age
The maximum age of STP information learned from the network on any port before it is discarded.

Root Port Bridge Forward Delay
The value that all bridges use for forwarddelay when this bridge is acting as the root. Values range from 4 through 30. The Factory default is 15 seconds.

Hello Time The amount of time between the transmission of Configuration BPDUs by this node or any port when it is the root of the spanning tree or trying to become the root.

Bridge Hold Time
Minimum time between transmission of Configuration BPDUs.

CST Regional Root
The regional root bridge.

Regional Root Path Cost
The cost of the path to the regional root as seen from this bridge.

Associated FIDs
List of forwarding database identifiers currently associated with this bridge instance.

Associated VLANs
List of VLAN IDs currently associated with this bridge instance.

show spanningtree cst port detailed

Use this command to display the settings and parameters for a specific switch port within the CST. The *port* is the port to be affected.

Syntax:

```
show spanningtree cst port detailed port
```

Return values:

Port Identifier The port identifier for this port within the CST.

Port Priority The priority of the port within the CST.

Port Forwarding State
The forwarding state of the port within the CST.

Port Role The role of the specified interface within the CST.

Auto-calculate Port Path Cost
Indicates whether automatic calculation of the port path cost is enabled.

Port Path Cost
The configured path cost for the specified interface.

Designated Port Cost
Path Cost offered to the LAN by the designated port.

Designated Bridge
The bridge containing the designated port.

Designated Port Identifier
Port used to forward frames towards the root bridge for this CST on this LAN. It is the port with the lowest cost path to the bridge and the highest port priority.

Topology Change Acknowledgement
Value of flag in next Configuration BPDU transmission indicating if a topology change is in progress for this port.

Hello Time The hello time in use for this port.

Edge Port The configured value indicating if this port is an edge port.

Edge Port Status
The derived value of the edge port status. True if operating as an edge port; false otherwise.

Point To Point MAC Status
Derived value indicating if this port is part of a point to point link.

CST Regional Root
The regional root identifier in use for this port.

CST Path Cost
The configured path cost for this port.

show spanningtree cst port summary

Use this command to display the status of one, some, or all ports within the CST. The parameter *port*/*listofports*/`all` indicates the port or ports to be affected.

Syntax:

```
show spanningtree cst port summary port/listofports/all
```

Return values:

Port The interface being displayed.

STP Mode Whether the STP is enabled or disabled on the port.

STP State The current spanning tree state of the port. This state controls what action a port takes on receipt of a frame. Possible states are: disabled, blocking, listening, learning, forwarding, and broken.

Port Role The role of the specified port within the spanning tree.

Link Status The operational status of the link. Possible values are “Up” or “Down”.

Link Trap The link trap configuration for the specified interface.

config spanningtree port migrationcheck

Use this command to force the specified port to transmit RST BPDUs. The *port* parameter specifies the ports to be affected. To set the migration check for all ports with a single command, `all` can be specified. Note that the forceversion parameter for the switch must be set to 802.1w for this command to work.

Syntax:

```
config spanningtree port migrationcheck port/listofports/all enable/disable
```

Default:
disable

config spanningtree port mode

Use this command to configure the Administrative Switch Port State to a new value for the specified port. The *port* parameter specifies the ports to be affected. To enable or disable all ports with a single command, `all` can be specified. Note that a maximum of 4095 ports can be enabled.

Syntax:

```
config spanningtree port mode port/listofports/all enable/disable
```

Default:
disable

show spanningtree port

Use this command to display the STP statistics for a specific switch port.

Syntax:

```
show spanningtree port port
```

Return values:

Port mode
Enabled or disabled.

Port Up Time Since Counters Last Cleared
The time in days, hours, minutes, and seconds since the counters were last reset.

STP BPDUs Transmitted
The number of STP BPDUs sent by this port.

STP BPDUs Received
The number of STP BPDUs received by this port.

RSTP BPDUs Transmitted
The number of Rapid Reconfiguration STP BPDUs sent by this port.

RSTP BPDUs Received
The number of Rapid Reconfiguration STP BPDUs received by this port.

config spanningtree adminmode

Use this command to configure the STP operational mode. While the operational mode is disabled, the spanning tree configuration is retained and can be changed, but it is not activated.

Syntax:

```
config spanningtree adminmode enable/disable
```

Default:
disable

config spanningtree forceversion

Use this command to select which version of the STP will be used. The `version` can be one of the following:

- 802.1D - IEEE 802.1D functionality supported: STP BPDUs are transmitted rather than R(Rapid)STP BPDUs
- 802.1w - IEEE 802.1w functionality supported: RSTP BPDUs are transmitted rather than STP BPDUs

Syntax:

```
config spanningtree forceversion 802.1D/802.1w
```

Default:
IEEE 802.1D

show spanningtree summary

Use this command to display STP settings and parameters for the switch.

Syntax:

```
show spanningtree summary
```

Return values:

Spanning Tree Adminmode
Enabled or disabled.

Spanning Tree Version
Indicates which version of the STP is being run. Possible values are IEEE 802.1w, or IEEE 802.1D.

Configuration Digest Key
Calculated value used as part of the configuration identifier.

Configuration Format Selector
Identifies the level of the IEEE 802.1 standard in use by the switch.

Virtual Local Area Network (VLAN) commands

config vlan bcaststorm

Use this command to enable or disable broadcast storm control for a particular Virtual Local Area Network (VLAN). If broadcast storm control is enabled, storms are controlled by counting the number of broadcast packets within a certain time period. If the [*packets_per_second*] count limit is exceeded, the packets are discarded.

Syntax:

```
config vlan bcaststorm vlan_id enable/disable [packets_per_second]
```

where `vlan_id` is an integer ranging from 1 through 4094 representing an existing VLAN.

Default:
disable

where *packets_per_second* is:

- an integer ranging from 1 through 148800 for a 100 Mbps link
- an integer ranging from 1 through 1488100 for a 1000 Mbps link

config vlan create

Use this command to create a new VLAN and assign it an ID.

Syntax:

```
config vlan create vlan_id
```

where `vlan_id` is an integer ranging from 2 through 4094 representing a new VLAN. (ID 1 is reserved for the default VLAN)

config vlan delete

Use this command to delete an existing VLAN.

Syntax:

```
config vlan deletevlan_id
```

where `vlan_id` is an integer ranging from 2 through 4094 representing an existing VLAN. (The default VLAN (ID 1) cannot be deleted.

config vlan makestatic

Use this command to change a dynamically created VLAN (one that is created by GVRP registration) to a static VLAN (one that is permanently configured and defined) The number identifies an existing VLAN.

Syntax:

```
config vlan makestatic vlan_id
```

where *vlan_id* is an integer ranging from 2 through 4094 representing an existing VLAN.

config vlan mcaststorm

Use this command to enable or disable multicast storm control for a particular VLAN. If multicast storm control is enabled, storms are controlled by counting the number of multicast packets within a certain time period. If the [packets_per_second] count limit is exceeded, the packets are discarded.

Syntax:

```
config vlan mcaststorm  vlan_id enable/disable [packets_per_second]
```

where *vlan_id* is an integer ranging from 1 through 4094 representing an existing VLAN.

Default:
disable

config vlan name

Use this command to change the name of a VLAN. The name is an alphanumeric string of up to 16 characters, and the number identifies an existing VLAN.

Syntax:

```
config vlan name name vlan_id
```

where *vlan_id* is an integer ranging from 2 through 4094 representing an existing VLAN.

Default:
The name for VLAN ID 1 is always default. The default name for other VLANs is a blank string.

config vlan participation

Use this command to configure the degree of participation for a specific interface in a VLAN. The number identifies an existing VLAN, and the parameter `port/listofports/all` indicates the port or ports to be affected.

Syntax:

```
config vlan participation exclude/include/auto vlan_id port/listofports/all
```

where

- *vlan_id* is an integer ranging from 1 through 4094 representing an existing VLAN.
- Participation options are:

Include The interface is always a member of this VLAN. This is equivalent to registration fixed.

Exclude The interface is never a member of this VLAN. This is equivalent to registration forbidden.

Auto The interface is dynamically registered in this VLAN by GVRP. The interface will not participate in this VLAN unless a join request is received on this interface. This is equivalent to registration normal.

config vlan port acceptframe

Use this command to configure the frame acceptance mode for the specified ports. Possible values are:

all Both tagged and untagged frames are accepted. Untagged frames will be assigned the PVID and default priority configured for the ports for this VLAN.

vlan Untagged frames are discarded.

With either option, VLAN tagged packets are forwarded in accordance with the IEEE 802.1Q VLAN Specification.

Syntax:

```
config vlan port acceptframe all/vlanonly port/listofports/all
```

Default:
all

config vlan port ingressfilter

Use this command to enable or disable ingress filtering for the specified ports for the specified VLAN. If ingress filtering is disabled, tagged packets received with VLAN IDs that do not match the VLAN membership of the receiving interface are admitted and forwarded to ports that are members of that VLAN.

Syntax:

```
config vlan port ingressfilter enable/disable port/listofports/all
```

Default:
disable

config vlan port priority

Use this command to change the default IEEE 802.1p port priority assigned to untagged frames received on the specified ports for the specified VLAN.

Syntax:

```
config vlan port priority priority_number port/listofports/all
```

where *priority_number* is an integer ranging from 0 through 7.

Default:
0

config vlan port pvid

Use this command to change the VLAN ID that the specified ports will assign to untagged frames if untagged frames are accepted.

Syntax:

```
config vlan port pvid vlan_id port/listofports/all
```

where *vlan_id* is an integer ranging from 1 through 4094 representing an existing VLAN.

Default:

1

config vlan port tagging

Use this command to configure the tagging behavior for a specific interface in a VLAN. If tagging is enabled, all traffic is transmitted as tagged frames. If tagging is disabled, all traffic is transmitted as untagged frames. The parameter *port*/*listofports*/`all` indicates the port or ports to be affected.

Syntax:

```
config vlan port tagging enable/disable port/listofports/all
```

show vlan detailed

Use this command to display detailed information, including interface information, for a specific VLAN.

Syntax:

```
show vlan detailed
```

Return values:

VLAN ID
There is a VLAN Identifier (VLAN ID) associated with each VLAN. The range of the VLAN ID is 1 through 4094.

VLAN Name
A string associated with this VLAN as a convenience. It can be up to 16 alphanumeric characters long, including blanks. The default is blank. VLAN ID 1 always has a name of “Default”. This field is optional.

VLAN Type
The type of VLAN. A VLAN can be:

- the Default VLAN (VLAN ID = 1)
- a static VLAN, one that is created using the config vlan create command
- a Dynamic VLAN, one that is created by GVRP registration

In order to change a VLAN from Dynamic to Static, use the config vlan makestatic command.

Broadcast Storm Control
Displays the administrative mode of broadcast storm control for this VLAN. The threshold value for broadcast storm control is in packets per second.

Multicast Storm Control
Displays the administrative mode of multicast storm control for this VLAN. The threshold value for broadcast storm control in packets per second.

Port Indicates which port is associated with the fields on this line.

Current Displays the degree of participation of this port in this VLAN. The permissible values are:

Include This port is always a member of this VLAN. This is equivalent to registration fixed in the IEEE 802.1Q standard.

Exclude This port is never a member of this VLAN. This is equivalent to registration forbidden in the IEEE 802.1Q standard.

Autodetect This port will not participate in this VLAN unless a GVRP join request is received on this port. This is equivalent to registration normal in the IEEE 802.1Q standard.

Configured Displays the configured degree of participation of this port in this VLAN. The permissible values are:

Include This port is always a member of this VLAN. This is equivalent to registration fixed in the IEEE 802.1Q standard.

Exclude This port is never a member of this VLAN. This is equivalent to registration forbidden in the IEEE 802.1Q standard.

Autodetect This port will not participate in this VLAN unless a GVRP join request is received on this port. This is equivalent to registration normal in the IEEE 802.1Q standard.

Tagging Displays the tagging behavior for this port in this VLAN. The default is untagged.

Tagged All frames transmitted for this VLAN will be tagged.

Untagged All frames transmitted for this VLAN will be untagged.

show vlan port

Use this command to display VLAN port information.

Syntax:

```
show vlan port port/listofports/all
```

Return values:

Port Indicates which port is associated with the fields on this line.

Port VLAN ID The VLAN ID that this port will assign to untagged frames or priority tagged frames received on this port if the acceptable frame types parameter is set to Admit All. The factory default is 1.

Acceptable Frame Types
The types of frames that may be received on this port. The options are VLAN only and admit all. When set to VLAN only, untagged frames or priority tagged frames received on this port are discarded. When set to admit all, untagged frames or priority tagged frames received on this port are accepted and assigned the

value of the Port VLAN ID for this port. With either option, VLAN tagged frames are forwarded in accordance with the IEEE 802.1Q VLAN specification.

Ingress Filtering
Specifies whether ingress filtering is enabled or disabled on this port. When enabled, a frame is discarded if this port is not a member of the VLAN with which the frame is associated. In a tagged frame, the VLAN is identified by the VLAN ID in the tag. In an untagged frame, the VLAN is the Port VLAN ID specified for the port that received this frame. When disabled, all frames are accepted and forwarded in accordance with the 802.1Q VLAN bridge specification. The factory default is disabled.

GVRP Indicates whether GVRP is enabled or disabled on the port.

Default Priority
The IEEE 802.1p priority that will be assigned to untagged frames accepted on this port for this VLAN.

show vlan summary

Use this command to display information about all configured VLANs.

Syntax:

```
show vlan summary
```

Return values:

VLAN ID There is a VLAN Identifier (VLAN ID) associated with each VLAN. The range of the VLAN ID is 1 through 4094.

VLAN Name A string associated with this VLAN as a convenience. It can be up to 16 alphanumeric characters long, including blanks. The default is blank. VLAN ID 1 always has a name of ‘Default’. This field is optional.

VLAN Type What type of VLAN this is. A VLAN can be:

- the Default VLAN (VLAN ID = 1)
- a static VLAN, one that is created using the **config vlan create** command
- a Dynamic VLAN, one that is created by GVRP registration

In order to change a VLAN from dynamic to static, use the **config vlan makestatic** command.

BcastStorm This displays the administrative mode of broadcast storm control for this VLAN. If storm control is enabled, storms are controlled by counting the number of broadcast packets within a certain time period. If a count limit is exceeded, the packets are discarded.

McastStorm This displays the administrative mode of multicast storm control for this VLAN. If storm control is enabled, storms are controlled by counting the number of multicast packets within a certain time period. If a count limit is exceeded, the packets are discarded.

Chapter 4. Routing commands

This section describes the following nine groups of Routing commands:

- Address Resolution Protocol (ARP) commands
- Internet Protocol (IP) commands
- Open Shortest Path First (OSPF) commands
- Router BOOTP/DHCP Relay commands
- Router Route commands
- Router (rtr) Discovery commands
- Routing Information Protocol (RIP) commands
- Virtual Local Area Network (VLAN) commands
- Virtual Router Redundancy Protocol (VRRP) commands

The commands in each group fall into one of two functional categories:

- Show commands - display parameter settings, statistics, and other information.
- Config commands - configure features and options of the switch.

Address Resolution Protocol (ARP) commands

config arp agetime

Use this command to configure the ARP entry ageout time.

Syntax:
```
config arp agetime seconds
```

where the value for *seconds* is a positive integer ranging from 15 through 3600 representing the IP ARP entry ageout time in seconds.

Default:
1200

config arp cachesize

Use this command to configure the size of the ARP cache.

Syntax:
```
config arp cachesize size
```

where the value for *size* is a positive integer ranging from 10 through 3072 representing the size of the ARP cache.

Default:
3072

config arp create

Use this command to create an entry in the ARP table.

Syntax:
```
config arp create arpentry macaddr
```

where:

- the value for *arpentry* is the IP address of a device on the network in dotted decimal notation.
- the value for *macaddr* is the MAC address of the device entered as six, two-digit, hexadecimal numbers separated by hyphens (for example, 00-06-29-32-81-40).

config arp delete

This command deletes an entry from the ARP table.

Syntax:

```
config arp delete arpentry
```

where the value for *arpentry* is the IP address of the entry.

config arp resptime

Use this command to specify the response timeout for ARP requests in seconds.

Syntax:

```
config arp resptime timeout
```

where the value for *timeout* is a positive integer ranging from 1 through 10 that indicates the response timeout, in seconds.

Default:
1

config arp retries

Use this command to specify the maximum number of times a ARP request will be retried.

Syntax:

```
config arp retries number_retries
```

where the value for *number_retries* is a positive integer ranging from 1 through 10 that indicates the number of ARP request retries.

Default:
4

show arp table

Use this command to display the ARP table. To view the total ARP entries, the operator should view the **show arp table** results in conjunction with the **show arp cache** results.

Syntax:

```
show arp table
```

Return values:

Age Time (seconds)
The time it takes for an ARP entry to age out. Age time is measured in seconds.

Response Time (seconds)
The number of seconds the switch will wait for a response to an ARP request.

Retries The maximum number of times an ARP request is retried.

Cache Size The maximum number of entries in the ARP cache.

IP address The IP address of a device on a subnet that is attached to one of the routing interfaces of the switch.

MAC address The unicast MAC address for the device. The format is six, two-digit, hexadecimal numbers separated by hyphens, for example, 00-06-29-32-81-40.

Interface The routing interface associated with the ARP entry.

Type The type of the ARP entry. The possible values are:

- **Local** - An ARP entry associated with one of the MAC addresses of the switch routing interface.
- **Gateway** - An ARP entry whose IP address is that of a router.
- **Static** - An ARP entry configured by the user.
- **Dynamic** - An ARP entry which has been learned by the router.

Internet Protocol (IP) commands

config interface encaps

Use this command to configure the link layer encapsulation type for packets transmitted on the specified interface.

Syntax:

```
config interface encaps port encapstype
```

where:

- the *port* identifies a configured routing interface.
- acceptable values for *encapstype* are Ethernet and SNAP. Routed frames are always Ethernet encapsulated when a frame is routed to a VLAN.

Default:
Ethernet

config ip forwarding

This command enables or disables the forwarding of IP frames.

Syntax:

```
config ip forwarding enable/disable
```

Default:
enable

config ip interface create

Use this command to configure the IP address for the specified routing interface.

Syntax:

```
config ip interface create port ipaddr subnetmask
```

where:

- the *port* identifies a configured routing interface.

- the value for *ipaddr* is a four-digit dotted-decimal number that will identify the interface on the network.
- the value for *subnetmask* is a four-digit dotted-decimal number used with the IP address to identify the subnet in which the interface will participate.

config ip interface delete

This command deletes the IP address of an interface.

Syntax:

```
config ip interface delete port ipaddr subnetmask
```

where:

- the *port* identifies a configured routing interface.
- the value for *ipaddr* is the IP address of the interface.
- the value for *subnetmask* is a four-digit dotted-decimal number representing the subnet mask of the interface.

config ip interface mtu

This command sets the Maximum Transmission Unit (MTU) size for the specified interface, in bytes.

Syntax:

```
config ip interface mtu port mtu_size
```

where:

- *port* identifies a configured routing interface.
- *mtu_size* is 576 through 1500, in bytes.

Default:
1500

config ip interface netdirbcast

This command enables or disables the forwarding of network-directed broadcasts through the specified interface.

Syntax:

```
config ip interface netdirbcast enable/disable
```

Default:
enable

config routing

This command enables or disables the routing function for the switch module.

Syntax:

```
config routing enable/disable
```

show ip interface

Use this command to display information about the specified IP interface.

Syntax:

```
show ip interface port
```

where the *port* identifies a configured routing interface.

Return values:

IP address The IP address of the router interface.

Subnet Mask The mask that defines the portion of the interface IP address that identifies the attached subnetwork.

Routing Mode
Indicates whether routing is enabled or disabled on the interface.

Administrative Mode
The administrative mode of the specified interface. The possible values of this field are enable or disable.

Forward Net Directed Broadcasts
Displays how network-directed broadcast packets will be handled. If set to enable directed broadcasts will be forwarded. If set to disable they will be dropped. The default is disable.

Active State Displays whether the interface is active or inactive. An interface is considered active if its link is up and it is in forwarding state.

Link Speed Date Rate
An integer representing the physical link data rate of the specified interface in Megabits per second (Mbps).

MAC address The burned-in physical address of the specified interface. The format is six, two digit, hexadecimal numbers separated by hyphens.

Maximum Transmission Unit
The maximum transmission unit (MTU) size for the interface, in bytes. The default value is 1500, the maximum value is 1500 and the minimum value is 576.

Encapsulation Type
The encapsulation type for the specified interface. The types are Ethernet or SNAP.

show ip stats

Use this command to display IP statistical information as specified in RFC 1213.

Syntax:

```
show ip stats port
```

where the *port* identifies a configured routing interface.

Return values:

IpInReceives The total number of input datagrams received, 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 on.

IpInAddrErrors
The number of input datagrams discarded because the destination IP address was not valid to be received at this entity. This count

includes invalid addresses (for example, 0.0.0.0) and addresses of unsupported Classes (for example, Class E).

IpForwDatagrams
The number of input datagrams for which this entity 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.

IpInUnknownProtos
The number of locally-addressed datagrams received successfully but discarded because of an unknown or unsupported protocol.

IpInDiscards The number of input IP datagrams for which no problems were encountered to prevent their continued processing, but which were discarded (for example, for lack of buffer space). Note that this counter does not include any datagrams discarded while awaiting re-assembly.

IpInDelivers The total number of input datagrams successfully delivered to IP user-protocols (including ICMP).

IpOutRequests
The total number of IP datagrams which local IP user-protocols (including ICMP) supplied to IP in requests for transmission. Note that this counter does not include any datagrams counted in IpForwDatagrams.

IpOutDiscards
The number of output IP datagrams for which no problem was encountered to prevent their transmission to their destination, but which were discarded (for example, lack of buffer space). Note that this counter would include datagrams counted in IpForwDatagrams if any such packets met this (discretionary) discard criterion.

IpOutNoRoutes
The number of IP datagrams discarded because no route could be found to transmit them to their destination. Note that this counter includes any packets counted in IpForwDatagrams which meet this `no-route' criterion.

IpReasmTimeout
The maximum number of seconds during which received fragments are held while they are awaiting reassembly at this entity.

IpReasmReqds
The number of IP fragments received which needed to be reassembled at this entity.

IpReasmOKs The number of IP datagrams successfully re-assembled.

IpReasmFails The number of failures detected by the IP re-assembly algorithm (for whatever reason: timed out, errors, and so on.). Note that this is not necessarily a count of discarded IP fragments since some algorithms can lose track of the number of fragments by combining them as they are received.

IpFragOKs The number of IP datagrams that have been successfully fragmented at this entity.

IpFragFails The number of IP datagrams that have been discarded because they needed to be fragmented at this entity but could not be, for example, because their Don't Fragment flag was set.

IpFragCreates
The number of IP datagram fragments that have been generated as a result of fragmentation at this entity.

IpRoutingDiscards
The number of routing entries which were chosen to be discarded even though they are valid. One possible reason for discarding such an entry could be to free-up buffer space for other routing entries.

IcmpInMsgs The total number of ICMP messages which the entity received. Note that this counter includes all those counted by icmpInErrors.

IcmpInErrors The number of ICMP messages which the entity received which had ICMP-specific errors (bad ICMP checksums, bad length, and so on.).

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 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 attempted to send. Note that this counter includes all those counted by icmpOutErrors.

IcmpOutErrors
The number of ICMP messages which this entity did not send due to problems discovered within ICMP such as a lack of buffers. This value does not include errors discovered outside the ICMP layer such as the inability of IP to route the resultant datagram.

IcmpOutDestUnreachs
The number of ICMP Destination Unreachable messages sent.

IcmpOutTimeExcds
The number of ICMP Time Exceeded messages sent.

IcmpOutParmProbs
The number of ICMP Parameter Problem messages sent.

IcmpOutSrcQuenchs
The number of ICMP Source Quench messages sent.

IcmpOutRedirects
The number of ICMP Redirect messages sent.

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.

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.

show ip summary

Use this command to display information applicable to all IP interfaces.

Syntax:

```
show ip summary
```

Return values:

Default Time to Live
The default value inserted into the Time-To-Live (TTL) field of the IP header of datagrams originated by the switch, if a TTL value is not supplied by the transport layer protocol.

Router ID A 32-bit integer in dotted decimal format identifying the router.

Routing Mode
Shows whether the routing mode is enabled or disabled. You must enable routing for the switch before you can route through any of the interfaces. The default is disable.

IP Forwarding Mode
Shows whether forwarding of IP frames is enabled or disabled.

show router ip interface summary

Use this command to display summary information about IP configuration settings for all ports in the router.

Syntax:

```
show router ip interface summary
```

Return values:

Port The interface associated with the information on the line.

IP address The IP address of the routing interface in dotted decimal format.

IP Mask The subnet mask of the routing interface in dotted decimal format.

Netdir Bcast Indicates if net-directed broadcasts are forwarded on this interface. Possible values are enable or disable.

MultiCast Fwd
Indicates the multicast forwarding administrative mode on the interface. Possible values are enable or disable.

In Access Mode
Indicates whether inbound access list checking is enabled or disabled for this interface.

Out Access Mode
Indicates whether outbound access list checking is enabled or disabled for this interface.

Open Shortest Path First (OSPF) configuration/summary commands

config router ospf 1583compatibility

This command enables or disables OSPF 1583 compatibility.

Syntax:

```
config router ospf 1583compatibility enable/disable
```

config router ospf adminmode

This command enables or disables the administrative mode of OSPF.

Syntax:

```
config router ospf adminmode enable/disable
```

Default:
disable

config router ospf area authentication

This command sets the OSPF Authentication Type and Key for the specified area.

Syntax:

```
config router ospf area authentication areaid type
```

where there are three possible values for *type*:

none This is the initial interface state. If you specify none, no authentication protocols will be run for this interface.

simple
If you specify simple, you must provide an authentication key which will be included, in the clear, in the OSPF header of all packets sent from this interface. All routers on the network must be configured with the same key. The key may be up to eight alphanumeric characters.

encrypt
If you specify encrypt, you must provide both a key and an authentication ID. Encryption uses the MD5 Message-Digest algorithm. All routers on the network must be configured with the same key and ID.

config router ospf area range create

This command creates an address range for the specified OSPF area. An area consists of a set of address ranges, where the range is defined by the combination of an IP address and subnet mask.

Syntax:

```
config router ospf area range create areaid ipaddr subnetmask [summ]
[enable/disable]
```

where:

- the value for *areaid* is an IP address that uniquely identifies the area to which the interface connects.
- the *ipaddr* is a valid IP address.
- the *subnetmask* is a valid subnet mask.
- (optional) the *[summ]* is the LSDB type.
- (optional) the enable/disable parameter indicates whether the address range should be advertised.

Default:
The default value for *[summ]* is network summary.

config router ospf area range delete

This command deletes a specified address range from a specified OSPF area.

Syntax:

```
config router ospf area range delete areaid ipaddr subnetmask [summ]
```

where:

- the value for *areaid* is an IP address that uniquely identifies the area to which the interface connects.
- the *ipaddr* is a valid IP address.
- the *subnetmask* is a valid subnet mask.
- (optional) the *[summ]* is the LSDB type.

config router ospf area stub create

Use this command to configure the specified area as a stub area. A stub area is characterized by the fact that AS External LSAs are not propagated into the area. Removing AS External LSAs and Summary LSAs can significantly reduce the size of the LSDB of routers within the stub area.

Syntax:

```
config router ospf area stub create areaid
```

where the value for *areaid* is an IP address that uniquely identifies the area to which the interface connects.

config router ospf area stub delete

This command deletes the specified stub area designation. The area will be returned to normal state.

Syntax:

```
config router ospf area stub delete areaid
```

where the value for *areaid* is an IP address that uniquely identifies the area to which the interface connects.

config router ospf area stub metric type

Use this command to configure the type of metric used to advertise link costs for the specified stub area.

Syntax:

```
config router ospf area stub metric type areaid type
```

where:

- the value for *areaid* is an IP address that uniquely identifies the area to which the interface connects.
- valid values for *type* are:

  OSPF metric An internal OSPF metric.

  Comparable cost
  An external Type 1 metric that is directly comparable to the OSPF metric.

  Non-comparable cost
  An external Type 2 metric assumed to be larger than the OSPF metric.

config router ospf area stub metric value

Use this command to configure the default metric for the specified stub area.

Syntax:

```
config router ospf area stub metric value areaid cost
```

where:

- the value for *areaid* is an IP address that uniquely identifies the area to which the interface connects.
- the value for *cost* is an integer value ranging from 1 through 16777215 that represents the cost of sending packets and is the cost advertised for the default route.

config router ospf area stub summarylsa

Use this command to configure the Summary LSA mode for the specified stub area. The Summary LSA mode can be configured as enabled or disabled. If you enter enable, summary LSAs will be imported into the stub area.

Syntax:

```
config router ospf area stub summarylsa areaid enable/disable
```

where the value for *areaid* is an IP address that uniquely identifies the area to which the interface connects.

config router ospf asbr

This command enables or disables operation of the router as an Autonomous System Border Router (ASBR).

Syntax:

```
config router ospf asbr enable/disable
```

Default:

disable

config router ospf exoverflowinterval

Use this command to configure the exit overflow interval for OSPF. It describes the number of seconds after entering overflow state that a router will wait before attempting to leave the overflow state. This allows the router to again originate non-default, AS-external, LSAs.

Syntax:

```
config router ospf exoverflowinterval interval_time
```

where the value of *interval_time* is an integer ranging from 0 through 2147483647 seconds. When set to 0, the router will not leave overflow state until restarted.

Default:

0

config router ospf extlsdblimit

Use this command to configure the external LSDB limit for OSPF.

When the number of non-default AS-external LSAs in a router's LSDB reaches the external LSDB limit, the router enters overflow state. The router never holds more than the external LSDB limit non-default, AS-external, LSAs in its database. The external LSDB limit MUST be set identically in all routers attached to the OSPF backbone or any regular OSPF area.

Syntax:

```
config router ospf extlsdblimit limit
```

where the value of *limit* is an integer ranging from -1 through 2147483647. If the value is -1, then there is no limit.

Default:

-1

config router ospf interface areaid

This command sets the OSPF area to which the specified router interface belongs.

Syntax:

```
config router ospf interface areaid port areaid
```

where:

- the *port* identifies a configured routing interface.
- the value for *areaid* is an IP address that uniquely identifies the area to which the interface connects. If you assign an area ID which does not exist, the area will be created with default values.

config router ospf interface authentication encrypt

This command configures MD5 encryption for the specified OSPF interfaces. You must provide both a key and a key ID for authentication. Encryption uses the MD5 Message-Digest algorithm. All routers must be configured with the same key and ID.

Syntax:

```
config router ospf interface authentication encrypt port key keyid
```

where the *port* identifies a configured routing interface.

- **Key:** Enter the OSPF Authentication key for the specified interface. If you do not use authentication, you will not be prompted to enter a key. If you choose simple authentication, you cannot use a key of more than 8 octets. If you choose encrypt, the key may be up to 16 octets long. The key value will only be displayed if you are logged on with Read/Write privileges; otherwise, it will be displayed as asterisks.
- **Key ID:** Enter the ID to be used for authentication. You will only be prompted to enter an ID when you select Encrypt as the authentication type. The ID is a number ranging from 0 through 255.

Default:

key	The default password key is not configured.

config router ospf interface authentication none

This command configures the authentication type to none for the specified OSPF interfaces. None is the initial interface state, or the default authentication type. If you use this type no authentication protocols will be run for this interface.

Syntax:

```
config router ospf interface authentication none port
```

Default:
This is the default authentication type.

config router ospf interface authentication simple

This command configures authentication type simple for the specified OSPF interfaces. If you use this authentication type, you must provide an authentication key which will be included, in the clear, in the OSPF header of all packets sent from this interface. All routers on the network must be configured with the same key. The key may be up to eight alphanumeric characters.

Syntax:

```
config router ospf interface authentication simple port key
```

Default:
The default authentication type is none.

config router ospf interface cost

This command sets the cost for the specified router interface, as reported in LSAs.

Syntax:

```
config router ospf interface cost ipaddr port  cost
```

where:

- the *ipaddr* and *port* parameters identify the interface on which to configure the cost.
- the *cost* has a range of 1 through 65535.

Default:
10

config router ospf interface iftransitdelay

This command sets the OSPF Transit Delay for the specified router interface. It specifies the length of time, in seconds, it takes to transmit a link-state update packet over this interface.

Syntax:

```
config router ospf interface iftransitdelay port time
```

where the valid range of *time* values is ranging from 1 through 3600 (1 hour) seconds.

Default:
1

config router ospf interface interval dead

This command sets the OSPF dead interval for the specified router interface.

Syntax:

```
config router ospf interface interval dead port wait_time
```

where the value for *wait_time* is a positive integer ranging from 0 through 2147483647 that indicates the length of time, in seconds, that the router will wait to see Hello packets from a neighbor router before declaring that the neighbor router is down. This value must be the same for all routers attached to the network. This value should be a multiple of the Hello Interval.

Default:
40

config router ospf interface interval hello

This command sets the OSPF hello interval for the specified router interface.

Syntax:

```
config router ospf interface interval hello port hello_interval
```

where the value for *hello_interval* is a positive integer ranging from 1 through 65535 that indicates the length of time, in seconds, between transmission of Hello packets by this router. The value must be the same for all routers attached to the network.

Default:
10

config router ospf interface interval retransmit

This command sets the OSPF retransmit Interval for the specified router interface.

Syntax:

```
config router ospf interface interval retransmit port retransmit_interval
```

where the value for *retransmit_interval* is a positive integer ranging from 0 through 3600 (1 hour) that indicates the length of time, in seconds, between LSA retransmissions for adjacencies belonging to this router interface. This value is also used when retransmitting database descriptions and link-state request packets.

Default:
5

config router ospf interface mode

This command enables or disables OSPF on the specified router interface.

Syntax:

```
config router ospf interface mode port enable/disable
```

Default:
disable

config router ospf interface priority

This command sets the OSPF priority for the specified router interface.

Syntax:

```
config router ospf interface priority port priority_value
```

where the value for *priority_value* is an integer ranging from 0 through 255. A value of 0 indicates that the router is not eligible to become the designated router on this network. A value of 1 indicates the highest router priority.

Default:
1

config router ospf preference

This command sets the route preference value for OSPF. When more than one route exists for a given destination the preference is used to choose the best route.

Syntax:

```
config router ospf preference intra/inter/type1/type2 preference
```

where the value for *preference* is a number ranging from 0 - 255. The lower the number the higher the rate preference.

Default:

intra	8
inter	10
type1	1 - 13
type2	150

show router ospf area info

Use this command to display information about the area specified by the *areaid*.

Syntax:

```
show router ospf area info areaid
```

Return values:

OSPF Area ID A 32-bit integer in dotted decimal format that uniquely identifies the OSPF area.

Aging Interval
The LSA aging timer interval.

External Routing
A definition of the router capabilities for the area, including whether or not AS-external-LSAs are flooded into/throughout the area. If the area is not a stub area, the only possibility is Import External LSAs. If the area is a stub area, Import No LSAs is also a possibility.

SPF Runs The number of times that the intra-area route table has been calculated using this area LSDB.

Area Border Router Count
The total number of area border routers reachable within this area.This is initially zero, and is calculated in each SPF Pass.

Area LSA Count
Total number of LSAs in this area's LSDB, excluding AS External LSAs.

Area LSA Checksum
The 32-bit, unsigned, sum of the LSAs' LS checksums contained in this area LSDB. This sum excludes external LSAs and can be used to determine if there has been a change in a router LSDB. It can also be used to compare the LSDBs of two routers.

Stub Mode Indicates whether the specified area is a stub area or not. The possible values are enabled and disabled.

Import Summary LSAs
Indicates whether the import of Summary LSAs is enabled or disabled.

Metric Value A number representing the Metric Value for the specified area.

Metric Type The type of metric for the stub area.

show router ospf area range

Use this command to display information about the area ranges for the specified *areaid*.

Syntax:

```
show router ospf area range areaid
```

Return values:

OSPF Area ID A 32-bit integer in dotted decimal format that uniquely identifies the OSPF area.

IP address The IP address for this area range.

Subnet Mask The subnet mask for this area range.

LSDB Type The type of link advertisement associated with this area range.

Advertisement
This indicates whether the advertisement status is enabled or disabled.

show router ospf info

Use this command to display information about OSPF.

Note: Once OSPF is initialized on the router, it will remain initialized until the router is reset.

Syntax:

```
show router ospf info
```

Return values:

Router ID
A 32-bit integer in dotted decimal format identifying the router.

OSPF Admin Mode
Indicates whether OSPF is enabled or disabled.

ASBR Mode
Reflects whether ASBR mode is enabled or disabled. Enable implies that the router is an autonomous system border router.

RFC 1583 Compatibility
Enables or disables preference rules that will be used when choosing among multiple Autonomous System (AS)-external LSAs advertising the same destination.

ABR Status
Indicates whether the router is an OSPF area border router (ABR).

Exit Overflow Interval
The number of seconds that, after entering overflow state, the router will wait before attempting to leave overflow state.

External LSA Count
The number of external (LS type 5) LSAs in the Link-State Database (LSDB).

External LSA Checksum
The sum of the LS checksums of the external LSAs contained in the LSDB. This sum can be used to determine whether there has been a change in a router LSDB, and to compare the LSDBs of two routers.

New LSAs Originated
In any given OSPF area, a router will originate several LSAs. Each router originates a router LSA. If the router is also the Designated Router for any of the area networks, it will originate network LSAs for those networks. This value represents the number of LSAs originated by this router.

LSAs Received
The number of LSAs received that were determined to be new instantiations.

External LSDB Limit
The maximum number of non-default, AS-external, LSA entries that can be stored in the LSDB. This parameter establishes the external LSDB limit for OSPF.

show router ospf interface info

Use this command to display information for the specified router interface.

Syntax:

```
show router ospf interface info port
```

Return values:

IP address The IP address of the specified interface.

Subnet Mask The mask that defines the portion of the IP address of the router interface that identifies the attached subnetwork.

OSPF Admin Mode
Shows whether OSPF is enabled or disabled on the router interface. You can configure OSPF parameters without enabling OSPF Admin Mode, but they will have no effect until you enable Admin Mode.

OSPF Area ID A 32-bit integer in dotted decimal format that uniquely identifies the OSPF area to which the router interface connects.

Router Priority
The OSPF priority for the router interface. A value of ‘0’ indicates that the router is not eligible to become the designated router on this network.

Retransmit Interval
The number of seconds between LSAs for adjacent routers belonging to this router interface. This value is also used when retransmitting database descriptions and link-state request packets.

Hello Interval The OSPF Hello Interval for this router interface. This parameter must be the same for all routers attached to a network.

Dead Interval Specifies how long the router will wait to see Hello packets from a neighbor router before declaring that the router is down.

LSA Ack Interval
The number of seconds between LSA Acknowledgement packet transmissions. This value must be less than the Retransmit Interval.

Iftransit Delay Interval
The estimated number of seconds it takes to transmit a link-state update packet over this router interface.

Authentication Type
The OSPF Authentication Type options for this router interface. Possible values are none, simple, and encrypt.

Metric Cost The cost of this router interface, as reported in LSAs.

The information below will only be displayed if OSPF is enabled:

OSPF Interface Type
The OSPF Interface Type will always be broadcast.

State The state of the OSPF interface. The possible values are:

Down This is the initial interface state. In this state, the lower-level protocols have indicated that the interface is unusable. In this state, interface parameters will be set to their initial values. All interface timers will be disabled, and there will be no adjacent routers associated with the interface.

Loopback

In this state, the router's interface to the network is looped back either in hardware or software. The interface is unavailable for regular data traffic. However, it may still be desirable to gain information on the quality of this interface, either through sending ICMP pings to the interface or through something like a bit error test. For this reason, IP packets may still be addressed to an interface in Loopback state. To facilitate this, such interfaces are advertised in router- LSAs as single host routes, whose destination is the IP interface address.

Waiting

The router is trying to determine the identity of the (Backup) Designated Router for the network by monitoring received Hello Packets. The router is not allowed to elect a Backup Designated Router or a Designated Router until it transitions out of Waiting state. This prevents unnecessary changes of (Backup) Designated Router.

Designated router

This router is itself the Designated Router on the attached network. Adjacencies are established to all other routers attached to the network. The router must also originate a network-LSA for the network node. The network- LSA will contain links to all routers (including the Designated Router itself) attached to the network.

Backup designated router

This router is itself the Backup Designated Router on the attached network. It will be promoted to Designated Router if the present Designated Router fails. The router establishes adjacencies to all other routers attached to the network. The Backup Designated Router performs slightly different functions during the Flooding Procedure, as compared to the Designated Router.

Other designated router

The interface is connected to a broadcast or NBMA network on which other routers have been selected to be the Designated Router and Backup Designated Router either. The router attempts to form adjacencies to both the Designated Router and the Backup Designated Router.

Designated Router

The router ID of the Designated Router for this network, in the view of the advertising router.

Backup Designated Router

The router ID of the Backup Designated Router for this network, in the view of the advertising router.

Number of Link Events

The number of times this router interface has changed its state.

show router ospf interface stats

Use this command to display the statistics for a specified router interface. The information below will only be displayed if OSPF is enabled.

Syntax:

```
show router ospf interface stats port
```

Return values:

OSPF Area ID A 32-bit integer in dotted decimal format that uniquely identifies the OSPF area to which this router interface connects.

SPF Runs The number of times that the intra-area route table has been calculated using this area LSDB.

Area Border Router (ABR) Count
The total number of ABRs reachable within this area. This is initially zero, and is recalculated with each SPF pass.

AS Border Router Count
The total number of autonomous system (AS) border routers reachable within this area.

Area LSA Count
The total number of LSAs in this area's LSDB, excluding AS External LSAs.

IP address The IP address that is associated with this OSPF interface.

OSPF Interface Events
The number of times the specified OSPF interface has either changed its state or an error has occurred.

Virtual Events
The number of state changes or errors that occurred on this virtual link.

Neighbor Events
The number of times this neighbor relationship has either changed state or an error has occurred.

External LSA Count
The number of external (LS type 5) LSAs in the LSDB.

LSAs Received
The number of LSAs that have been received that have been determined to be new instantiations. This number does not include newer instantiations of self-originated LSAs.

Originate New LSAs
The number of new LSAs that have been originated. In any given OSPF area, a router will originate several LSAs. Each router originates a router-LSA. If the router is also the Designated Router for any of the area's networks, it will originate network-LSAs for those networks.

show router ospf lsdb summary

Use this command to display the LSDB. The information below will only be displayed if OSPF is enabled.

Syntax:

```
show router ospf lsdb summary
```

Return values:

Router ID A 32-bit dotted decimal number representing the LSDB interface.

Area ID The IP address identifying the area to which the interface is attached.

LSA Type The types are

- Router
- Network
- IPnet summary
- ASBR summary
- AS external

LS ID An IP address that uniquely identifies an LSA that a router originates from all other self-originated LSAs of the same LS type. This IP address is not configurable by the user.

Age A number representing the age of the LSA in seconds.

Sequence A number used to distinguish the sequence in which otherwise identical LSAs were transmitted.

Checksum The total number LSA checksum.

show router ospf neighbor detailed

Use this command to display detailed information from the OSPF neighbor table. The information below will only be displayed if OSPF is enabled and the specified interface has a neighbor. The IP address is the IP address of the neighbor.

Syntax:

```
show router ospf neighbor detailed port ipaddr
```

Return values:

Interface The interface through which adjacency is established with neighbor.

Neighbor Router Id
The neighbor portion of the virtual link identification. Virtual links may be configured between any pair of area border routers having interfaces to a common (non-backbone) area.

Options An integer value that indicates the optional OSPF capabilities supported by the neighbor. The neighbor’s optional OSPF capabilities are also listed in its Hello packets. This enables received Hello Packets to be rejected (for example, neighbor relationships will not even start to form) if there is a mismatch in certain crucial OSPF capabilities.

Router Priority
Displays the OSPF priority for the specified interface. The priority of an interface is expressed as an integer ranging from 0 through 255. A value of ‘0’ indicates that the router is not eligible to become the designated router on this network.

State The types are:

- Attempt - no recent information has been received from the neighbor but a more concerted effort will be made to contact the neighbor.
- Init - a Hello packet has recently been received from the neighbor, but bi-directional communication has not yet been established.
- 2-way - communication between the two routers is bi-directional.
- Exchange Start - the first step in creating an adjacency between the two neighboring routers, the goal is to decide which router is the master and to decide upon the initial Database Description (DD) sequence number.
- Exchange - the router is describing its entire LSDB by sending DD packets to the neighbor.
- Loading - link-state Request packets are sent to the neighbor asking for the more recent LSAs that have been discovered (but not yet received) in the Exchange state.
- Full - the neighboring routers are fully adjacent and they will now appear in router-LSAs and network-LSAs.

Events The number of times this neighbor relationship has changed state, or an error has occurred.

Permanence This variable displays the status of the entry, either dynamic or permanent. This refers to how the neighbor became known.

Hellos Suppressed
This indicates whether Hellos are being suppressed to the neighbor. The types are enabled and disabled.

Retransmission Queue Length
An integer representing the current length of the retransmission queue of the specified neighbor router ID of the specified interface.

show router ospf neighbor table

Use this command to display a summary of the OSPF neighbor table. The information below will only be displayed if OSPF is enabled.

Syntax:

```
show router ospf neighbor table port
```

Return values:

Router ID Four-digit dotted decimal number representing the neighbor interface.

IP address An IP address representing the neighbor interface.

Neighbor Interface Index
A port identifying the neighbor interface index.

show router ospf stub table

Use this command to display the OSPF stub table. The information below will only be displayed if OSPF is initialized on the switch.

Syntax:

```
show router ospf stub table
```

Return values:

Area ID
A 32-bit identifier for the created stub area.

Type of Service
The type of service (TOS) associated with the stub metric. Switch module only supports Normal TOS.

Metric Value
The metric value is applied based on the TOS. It defaults to the least metric of the type of service among the interfaces to other areas. The OSPF cost for a route is a function of the metric value.

Metric Type
The type of metric advertised as the default route.

Import Summary LSA
Controls the import of summary LSAs into stub areas.

OSPF virtif commands

config router ospf virtif authentication encrypt

This command configures MD5 encryption for the specified OSPF virtual interfaces. You must provide both a key and a key ID for authentication. Encryption uses the MD5 Message-Digest algorithm. All routers must be configured wit the same key and ID.

Syntax:

```
config router ospf virtif authentication encrypt areaid neighbor key keyid
```

Default:

key
The default password key is not configured.

config router ospf virtif authentication none

This command configures the authentication type to none for the specified OSPF virtif interfaces. None is the initial interface state, or the default authentication type. If you use this type no authentication protocols will be run for this interface.

Syntax:

```
config router ospf virtif authentication none areaid neighbor
```

Default:
This is the default authentication type.

config router ospf virtif authentication simple

This command configures authentication type simple for the specified OSPF virtual interfaces. If you use this authentication type, you must provide an authentication key which will be included, in the clear, in the OSPF header of all packets sent from this interface. All routers on the network must be configured with the same key. The key may be up to eight alphanumeric characters.

Syntax:

```
config router ospf virtif authentication simple areaid neighbor key
```

Default:
The default authentication type is none.

config router ospf virtif create

This command creates an OSPF virtual interface for the specified *areaid* and *neighbor*. The *neighbor* parameter is the IP address of the neighbor.

Syntax:

```
config router ospf virtif create areaid neighbor
```

config router ospf virtif delete

This command deletes the OSPF virtual interface from the given interface. The *neighbor* parameter is the IP address of the neighbor.

Syntax:

```
config router ospf virtif delete areaid neighbor
```

config router ospf virtif interval dead

Use this command to configure the dead interval for the OSPF virtual interface identified by *areaid* and *neighbor*.

Syntax:

```
config router ospf virtif interval dead areaid neighbor interval_time
```

where the value for *interval_time* is a number ranging from 1 through 65535, in seconds.

Default:

40

config router ospf virtif interval hello

Use this command to configure the hello interval for the OSPF virtual interface identified by *areaid* and *neighbor*.

Syntax:

```
config router ospf virtif interval hello areaid neighbor interval_time
```

where the value for *interval_time* is a number ranging from 1 through 65535, in seconds.

Default:

10

config router ospf virtif interval retransmit

Use this command to configure the retransmit interval for the OSPF virtual interface identified by *areaid* and *neighbor*.

Syntax:

```
config router ospf virtif interval retransmit areaid neighbor interval_time
```

where the value for *interval_time* is a number ranging from 1 through 3600, in seconds.

Default:

5

config router ospf virtif transdelay

Use this command to configure the transit delay for the OSPF virtual interface identified by *areaid* and *neighbor*.

Syntax:

```
config router ospf virtif interval transdelay areaid neighbor delay_time
```

where the value for *delay_time* is a number ranging from 1 through 3600 (1 hour), in seconds.

Default:
1

show router ospf virtif detailed

Use this command to display the OSPF Virtual Interface information for the specified area and neighbor. The *areaid* parameter identifies the area and the *neighbor* parameter identifies the neighbor's IP address.

Syntax:

```
show router ospf virtif detailed areaid neighbor
```

Return values:

Area ID The requested OSPF area ID.

Neighbor IP address
The requested neighbor IP address.

Hello Interval The configured hello interval for the OSPF virtual interface.

Dead Interval The configured dead interval for the OSPF virtual interface.

Iftransit Delay Interval
The configured transit delay for the OSPF virtual interface.

Retransmit Interval
The configured retransmit interval for the OSPF virtual interface.

Authentication Type
The configured authentication type of the OSPF virtual interface. Possible choices are none, simple, and encrypt.

show router ospf virtif summary

Use this command to display the OSPF Virtual Interface information for all areas in which the router participates.

Syntax:

```
show router ospf virtif summary
```

Return values:

Area Id The ID of the OSPF area.

Neighbor Router ID
The neighbor interface of the OSPF virtual interface. Virtual links may be configured between any pair of area border routers having interfaces to a common (non-backbone) area.

Hello Interval The configured hello interval for the OSPF virtual interface. This parameter must be the same for all routers attached to a network.

Dead Interval
Specifies how long the router will wait to see a Hello packets from a neighbor router before declaring that the router is down. This parameter must be the same for all routers attached to a network.

Retransmit Interval
The number of seconds between LSAs for adjacencies belonging to this router interface. This value is also used when retransmitting database descriptions and link-state request packets.

Transit Delay Specifies the estimated number of seconds it takes to transmit a link state update packet over the selected interface.

Router BOOTP/DHCP relay commands

config router bootpdhcprelay adminmode

This command enables or disables the forwarding of BOOTP/DHCP Requests on the system.

Syntax:

```
config bootpdhcprelay adminmode enable/disable
```

Default:
disable

config router bootpdhcprelay cidoptmode

This command enables or disables the circuit ID option mode for BOOTP/DHCP Relay on the system. When enabled, the relay agent will add options to BOOTP/DHCP requests to indicate that the requesting client is connected by high-speed modem, and will remove such options from replies.

Syntax:

```
config bootpdhcprelay cidoptmode enable/disable
```

Default:
disable

config router bootpdhcprelay maxhopcount

Use this command to configure the maximum allowable relay agent hops for BOOTP/DHCP Relay on the system.

Syntax:

```
config bootpdhcprelay maxhopcount max_hops
```

where the value for *max_hops* is a number ranging from 1 through 16.

Default:
4

config router bootpdhcprelay minwaittime

Use this command to configure the minimum wait time in seconds for BOOTP/DHCP Relay on the system. When the BOOTP relay agent receives a

BOOTREQUEST message, it may compare the seconds-since-client-began-booting field of the request to the minwaittime when deciding whether to relay the request or not.

Syntax:

```
config bootpdhcprelay minwaittime wait_time
```

where the value for *wait_time* is a number ranging from 1 through 100, in seconds.

Default:
0

config router bootpdhcprelay serverip

Use this command to configure the address of the BOOTP/DHCP server to which the Relay Agent will forward requests. The `ipaddr` parameter is an IP address in a four-digit dotted decimal format.

Syntax:

```
config bootpdhcprelay serverip ipaddr
```

Default:
0.0.0.0

show router bootpdhcprelay

Use this command to display the BOOTP/DHCP Relay information.

Syntax:

```
show router bootpdhcprelay
```

Return values:

Maximum Hop Count
Maximum number of hops a client request can go without being discarded.

Minimum Wait Time (Seconds)
The minimum time, in seconds, the client has been waiting before its request is forwarded to the BOOTP/DHCP server.

Admin Mode
Represents whether relaying of requests is enabled or disabled. When enabled the relay forwards the BOOTP/DHCP requests to the IP address given by “Server IP address.”

Server IP address
The IP address of the BOOTP/DHCP Relay server or the IP address of the next BOOTP/DHCP Relay Agent.

Circuit Id Option Mode
The Relay agent option which can be either enabled or disabled. Enabled adds Relay agent options to the request before forwarding it to Server and removes the options before forwarding the reply to clients.

Requests Received
The number of BOOTP/DHCP requests received from all clients since the system boot time.

Requests Relayed

The number of BOOTP/DHCP requests forwarded to the BOOTP/DHCP Server since the system boot time.

Packets Discarded

The number of BOOTP/DHCP requests discarded by this Relay Agent since the system boot time.

Router discovery commands

config rtrdiscovery address

Use this command to configure the address to be used to advertise the router for the interface.

Syntax:

```
config router rtrdiscovery address port ipaddr
```

Default:

224.0.0.1

config rtrdiscovery adminmode

This command enables or disables Router Discovery on an interface. The possible values for `mode` are enable and disable.

Syntax:

```
config router rtrdiscovery adminmode port enable/disable
```

Default:

enable

config rtrdiscovery lifetime

Use this command to configure the value, in seconds, of the lifetime field of the router advertisement sent from this interface. This is the maximum length of time that the advertised addresses are to be considered as valid router addresses by hosts.

Syntax:

```
config router rtrdiscovery lifetime port lifetime_period
```

where the value for *`lifetime_period`* is a number ranging from the maxinterval to 9000, in seconds.

Default:

3 * maxinterval

config rtrdiscovery maxinterval

Use this command to configure the maximum time, in seconds, allowed between sending router advertisements from the interface.

Syntax:

```
config router rtrdiscovery maxinterval port max_time
```

where the value for *`max_time`* is a number ranging from 4 through 1800, in seconds.

Default:
600

config rtrdiscovery mininterval

Use this command to configure the minimum time, in seconds, allowed between sending router advertisements from the interface.

Syntax:
```
config router rtrdiscovery mininterval port min_time
```

where the value for `min_time` sets the minimum time, in seconds, between sending router advertisements. The range for *min_time* is from 3 seconds through 1800 seconds.

Default:
0.75 * maxinterval

config rtrdiscovery preference

Use this command to configure the preferability of the address as a default router address, relative to other router addresses on the same subnet.

Syntax:
```
config router rtrdiscovery preference port address
```

where the value for `address` is an integer ranging from -2147483648 through 2147483647. Higher numbered addresses are preferred.

Default:
0

show rtrdiscovery

Use this command to display the router discovery information for all interfaces or a specified interface.

Syntax:
```
show router rtrdiscovery port/listofports/all
```

Return values:

Advertise Mode
Indicates whether router discovery is enabled or disabled on this interface. If enabled, Router Advertisements will be transmitted from the selected interface.

Maximum Advertise Interval
The maximum time allowed between sending router advertisements from the interface in seconds.

Minimum Advertise Interval
The minimum time allowed between sending router advertisements from the interface in seconds.

Advertise Lifetime
The maximum length of time that the advertised addresses are to be considered as valid router addresses by hosts.

Preference Level
The preference of the address as a default router address, relative to other router addresses on the same subnet. Higher numbered addresses are preferred.

Router route commands

config router id

This command sets the dotted-decimal number which will uniquely identify the router.

Syntax:

```
config router id routerid
```

where *routerid* is in dotted-decimal format.

Default:
The default value is 0.0.0.0, although this is not a valid Router ID.

config router route create

Use this command to configure a static route.

Syntax:

```
config router route create networkaddr subnetmask nexthopip metric
```

where:

- the *networkaddr* and *nexthopip* are valid IP addresses.
- the *subnetmask* is a valid subnet mask
- (optional) the *metric* is an integer ranging from 0 through 255

Default:
1

config router route default create

Use this command to configure the default route. The value for *nexthopip* is a valid IP address of the next hop router.

Syntax:

```
config router route default create nexthopip
```

config router route default delete

This command causes the static default route to be deleted.

Syntax:

```
config router route default delete
```

config router route delete

This command causes a static route to be deleted. The *networkaddr* and *nexthopip* are valid IP addresses. The *subnetmask* is a four-digit dotted-decimal number representing a valid subnet mask.

Syntax:

```
config router route delete networkaddr subnetmask nexthopip
```

config router route staticpreference

This command sets the static route preference value of local and static routes in the router.

Syntax:

```
config router route staticpreference preference
```

where *preference* is a number ranging from 1 through 255. Lower route preference values are preferred when determining the best route.

Default:

Local	0
Static	60

show router route bestroutes

Displays the single best route to each destination known to the router, based on the preference level of the route.

Syntax:

```
show router route bestroutes
```

Return values:

Network Address
Specifies the IP route prefix for the destination. In order to create a route a valid routing interface must exist and the next hop IP address must be on the same network as the routing interface.

Subnet Mask
Also referred to as the subnet/network mask. This indicates the portion of the IP interface address that identifies the attached network.

Protocol
Tells which protocol added the specified route. The possibilities are:

- Local
- Static
- Default
- MPLS
- OSPF Intra-area
- OSPF Inter-area
- OSPF Type-1 external
- OSPF Type-2 external
- RIP
- BGP4

Next Hop Intf
The outgoing router interface to use when forwarding traffic to the next destination.

Next Hop IP address
The outgoing router IP address to use when forwarding traffic to the next router (if any) in the path towards the destination. The next

router will always be one of the adjacent neighbors or the IP address of the local interface for a directly attached network. When creating a route, the next hop IP address must be on the same network as the routing interface. Valid next hop IP addresses can be seen by issuing the **show router route table** command.

Total Number of Routes
The total number of routes.

show router route entry

Use this command to display detailed information about the route to a specific network to be displayed. The value for `networkaddr` is a valid IP address.

Syntax:

```
show router route entry networkaddr
```

Return values:

Network Address
A valid network address identifying the network on the specified interface.

Subnet Mask
A mask of the network and host portion of the IP address for the attached network.

Route Type
Specifies whether the route is default or static. If creating a default route, all you need to specify is the next hop IP address, otherwise each field needs to be specified.

Protocol
Tells which protocol added the specified route. The possibilities are:

- Local
- Static
- Default
- MPLS
- OSPF Intra-area
- OSPF Inter-area
- OSPF Type-1 external
- OSPF Type-2 external
- RIP
- BGP4

Next Hop Interface
The outgoing router interface to use when forwarding traffic to the next destination.

Next Hop IP address
The outgoing router IP address to use when forwarding traffic to the next router (if any) in the path towards the destination. The next router will always be one of the adjacent neighbors or the IP address of the local interface for a directly attached network. When creating a route, the next hop IP must be on the same network as the routing interface. Valid next hop IP addresses can be seen by issuing the **show router route table** command.

Metric
The administrative cost of the path to the destination. If no value is entered, default is 1. Range is 0 - 255.

show router route preferences

Use this command to configure the default preference for each protocol (for example, 60 for static routes, 170 for BGP). These values are arbitrary values in the range of 1 through 255 and are independent of route metrics. Most routing protocols use a route metric to determine the shortest path known to the protocol, independent of any other protocol. The best route to a destination is chosen by selecting the route with the lowest preference value. When there are multiple routes to a destination, the preference values are used to determine the preferred route. If there is still a tie, the route with the best route metric will be chosen. To avoid problems with mismatched metrics (for example, Routing Information Protocol (RIP) and OSPF metrics are not directly comparable) you should configure different preference values for each of the protocols.

Syntax:

```
show router route preferences
```

show router route table

This command displays all routes to each destination known to the router using the route table.

Syntax:

```
show router route table
```

Return values:

Network Address
The IP route prefix for the destination.

Subnet Mask
A mask of the network and host portion of the IP address that identifies the attached network.

Protocol
Tells which protocol added the specified route to the table. The possibilities are:

- Local
- Static
- MPLS
- OSPF Intra
- OSPF Inter
- OSPF Type-1
- OSPF Type-2
- RIP
- BGP4

Next Hop Intf
The outgoing router interface to use when forwarding traffic to the next destination.

Next Hop IP address
The IP address of the next router in the path towards the destination. The next router will always be one of the adjacent neighbors or the IP address of the local interface for a directly attached network.

Total Number of Routes
The total number of routes in the route table.

Routing Information Protocol (RIP) commands

config router rip adminmode

This command sets the administrative mode of RIP in the router to active or inactive.

Syntax:

```
config router rip adminmode enable/disable
```

Default:
disable

config router rip autosummary

This command enables or disables autosummary for RIP.

Syntax:

```
config router rip autosummary enable/disable
```

config router rip hostrouteaccept

This command enables of disables RIP host routes accepted by RIP.

Syntax:

```
config router rip hostroutesaccept enable/disable
```

config router rip interface authentication encrypt

This command configures enables MD5 encryption for the specified RIP interface.

Syntax:

```
config router rip interface authentication encrypt port key keyid
```

Default:

key The default password key is not configured.

config router rip interface authentication none

This command configures the authentication type to none for the specified RIP interface. None is the initial interface state, or the default authentication type.

Syntax:

```
config router rip interface authentication none port
```

Default:
This is the default authentication type.

config router rip interface authentication simple

This command configures authentication type simple for the specified RIP interface.

Syntax:

```
config router rip interface authentication simple port key
```

Default:
The default authentication type is none.

config router rip interface authentication

This command sets the RIP v2 Authentication Type and Key for the specified interface.

Syntax:

```
config router rip interface authentication port type [key]
```

where the value of *type* is:

none This is the initial interface state. If you select this option from the pull-down menu on the second screen you will be returned to the first screen and no authentication protocols will be run.

simple
If you select Simple you will be prompted to enter an authentication key. This key will be included, in the clear, in the OSPF header of all packets sent on the network. All routers on the network must be configured with the same key.

encrypt
If you select Encrypt you will be prompted to enter both an authentication key and an authentication ID. Encryption uses the MD5 Message-Digest algorithm. All routers on the network must be configured with the same key and ID.

The key is composed of standard, displayable, non-control keystrokes from a Standard 101/102-key keyboard. If you do not choose to use authentication you will not be prompted to enter a key. If you choose simple authentication you cannot use a key of more than 8 octets. If you choose encrypt the key may be up to 16 octets long. The key value will only be displayed if you are logged on with Read/Write privileges, otherwise it will be displayed as asterisks.

Default:
The default authentication type is none. The default password key is an empty string. Unauthenticated interfaces do not need an authentication key.

config router rip interface defaultmetric

This command specifies the metric value used for the default route entry (0.0.0.0 with subnet mask = 0.0.0.0) in RIP updates originating from this interface.

Note that a metric value of 0 suppresses default route originations (although a default route may be propagated on this interface from another router). A metric value of 1 instructs the router to always advertise a default route entry with a metric of 1 in its route update messages, which could adversely affect network operation.

Syntax:

```
config router rip interface defaultmetric port metric
```

where *metric* is 0 through 15.

Default:
0

config router rip interface mode

This command enables or disables RIP on a router interface.

Syntax:
```
config router rip interface mode enable/disable
```

Default:
disable

config router rip interface version receive

Use this command to configure the interface to enable RIP control packets of the specified versions to be received.

Syntax:
```
config router rip interface version receive port mode
```

where the value for *port* is a valid routing port number or ‘all’ for selecting every routing port.

The value for *mode* can be

rip1 to receive only RIP version 1 formatted packets.

rip2 for RIP version 2.

both to receive packets from either format.

none to prevent any RIP control packets from being received.

Default:
both

config router rip interface version send

Use this command to configure the interface to enable RIP control packets of the specified versions to be sent.

Syntax:
```
config router rip interface version send port mode
```

where the value for *port* is a valid routing port number or ’all’ for selecting every routing port.

The value for *mode* can be

rip1 to broadcast RIP v1 formatted packets.

rip1c RIP v1 compatibility mode) which sends RIP v2 formatted packets via broadcast.

rip2 for sending RIP v2 using multicast.

none to not allow any RIP control packets to be sent.

Default:
rip1c

config router rip preference

Use this command to configure the default preference for each protocol (for example, 60 for static routes, 170 for BGP). These values are arbitrary values in the range of 1 through 255 and are independent of route metrics. Most routing protocols use a route metric to determine the shortest path known to the protocol, independent of any other protocol. The best route to a destination is chosen by selecting the route with the lowest preference value. When there are multiple routes to a destination, the preference values are used to determine the preferred route. If there is still a tie, the route with the best route metric will be chosen. To avoid problems with mismatched metrics (for example, Routing Information Protocol (RIP) and OSPF metrics are not directly comparable) you should configure different preference values for each of the protocols.

Syntax:

```
config router rip preference preference_value
```

where the *preference_value* is 1 through 255.

Default:
15

config router rip splithorizon

This command activates and configures the RIP split horizon mode.

Syntax:

```
config router rip splithorizon none/simple/poison
```

where:

- *none* provides no special processing
- *simple* does not include a route update sent to the router from which it is learned
- *poison* includes a route update sent to the router from which is learned

Default: Simple

show router rip info

Use this command to display information relevant to the RIP protocol.

Syntax:

```
show router rip info
```

Return values:

Router ID
A 32-bit dotted decimal number representing the router.

RIP Admin Mode
RIP administrative mode; enable activates and disable de-activates the RIP capability of the switch.

Global Route Changes
The number of route changes made by RIP to the IP Route Database. This does not include the refresh of the age of the route.

Global Queries
The number of responses sent to RIP queries from other systems.

show router rip interface detailed

Use this command to display information related to a particular RIP interface.

Syntax:

```
show router rip interface detailed port
```

Return values:

Interface The requested port.

IP address The IP source address used by the specified RIP interface.

Send version The RIP versions to which RIP control packets sent from the interface conform. The types are:

- **None** RIP control packets will not be transmitted.
- **RIP-1** RIP version 1 packets will be sent using broadcast.
- **RIP-1c** RIP version 1 compatibility mode. RIP version 2 formatted packets will be transmitted using broadcast.
- **RIP-2 (Default)** RIP version 2 packets will be sent using multicast.

Receive version The RIP versions allowed when receiving updates from the specified interface. The types are:

- **RIP-1** Only RIP v1 formatted packets will be received.
- **RIP-2** Only RIP v2 formatted packets will be received.
- **Both** Packets will be received in either format.
- **None (Default)** No RIP packets will be received.

RIP Admin Mode RIP administrative mode; enable or disable.

Link-State Indicates whether the interface is up or down.

Authentication Type The RIP Authentication Type for the specified interface. The types are:

- **None** No authentication protocols will be run.
- **Simple** If you enter Simple you will be prompted to enter an authentication key. This key will be included, in the clear, in the RIP header of all packets sent on the network. All routers on the network must be configured with the same key.
- **Encrypt** If you select Encrypt you will be prompted to enter both an authentication key and an authentication ID. Encryption uses the MD5 Message-Digest algorithm. All routers on the network must be configured with the same key and ID.

Authentication Key The RIP Authentication Key for the specified interface. The key value will only be displayed if you are logged on with Read/Write privileges to avoid compromising privacy, otherwise it will be displayed as asterisks. If you do not choose to use authentication you will not be prompted to enter a key. If you choose simple authentication you cannot use a key of more than 8 octets. If you choose encrypt the key may be up to 16 octets long.

Default Metric
A number which represents the metric used for default routes in RIP updates originated on the specified interface. The range for the default metric is 0 through 15. Note that a metric value of 0 suppresses default route originations (although a default route may be propagated on this interface from another router). A metric value of 1 instructs the router to always advertise a default route entry with a metric of 1 in its route update messages, which could adversely affect network operation.

The following information will be invalid if the link-state is down.

Bad Packets Received
The number of RIP response packets received by the RIP process which were subsequently discarded for any reason.

Bad Routes Received
The number of routes contained in valid RIP packets that were ignored for any reason.

Updates Sent The number of triggered RIP updates actually sent on this interface. This explicitly does NOT include full updates sent containing new information.

show router rip interface summary

Use this command to display general information for each RIP interface. For this command to display successful results, routing must be enabled for at least one interface.

Syntax:

```
show router rip interface summary
```

Return values:

Port The interface whose information is displayed at this line.

IP address The IP source address used by the specified RIP interface.

Send version The RIP versions to which RIP control packets sent from the interface conform. The types are:

None RIP control packets will not be transmitted.

RIP-1 RIP version 1 packets will be sent using broadcast.

RIP-1c
RIP version 1 compatibility mode. RIP version 2 formatted packets will be transmitted using broadcast.

RIP-2 (Default)
RIP version 2 packets will be sent using multicast.

Receive version
The RIP versions allowed when receiving updates from the specified interface. The types are none, RIP-1, RIP-2, and Both.

RIP-1 Only RIP v1 formatted packets will be received.

RIP-2 Only RIP v2 formatted packets will be received.

Both (Default)
Packets will be received in either format.

None No RIP packets will be received.

RIP Mode RIP administrative mode; enables or disables.

Link-State The mode of the interface (up or down).

Virtual Local Area Network (VLAN) routing commands

config ip vlan routing create

This command enables routing on a VLAN. The `vlan` value has a range from 1 through 4094 and identifies an existing VLAN. A logical interface number will be assigned to the routed VLAN. Use the **show ip vlan** command to display the new interface number, which you will need to use with the **config ip interface create** command to specify the IP address and subnet mask for the new interface.

Syntax:

```
config ip vlan routing create vlan
```

config ip vlan routing delete

This command disables routing on a VLAN.

Syntax:

```
config ip vlan routing delete vlan
```

where the *vlan* value has a range from 1 through 4094.

show ip vlan

Use this command to display information for all routing enabled VLANs in the system.

Syntax:

```
show ip vlan
```

Return values:

MAC address used by Routing VLANs
The MAC address that is associated with the internal bridge/router interface (IBRI). The same MAC address is used by all VLAN routing interfaces.

VLAN ID The ID of the VLAN whose data is displayed in the current table row.

Logical Interface
Indicates the logical slot and port associated with the VLAN routing interface.

IP address The configured IP address of the VLAN Routing Interface. This will be 0.0.0.0 when the VLAN Routing Interface is first configured and must be specified using the **config ip interface create** command.

Subnet Mask The configured subnet mask of the VLAN Routing Interface. This will be 0.0.0.0 when the VLAN Routing Interface is first configured and must be specified using the config ip interface create command.

Virtual Router Redundancy Protocol (VRRP) commands

config router vrrp adminmode

This command sets the administrative mode of VRRP in the router.

Syntax:

```
config router vrrp adminmode enable/disable
```

Default:
disable

config router vrrp interface adminmode

This command enables and disables the virtual router configured on the specified interface and sets the Virtual Router ID (VRID). The adminmode can be set to a value of enable or disable.

Syntax:

```
config router vrrp interface adminmode port vrid enable/disable
```

where *vrid* has an integer value ranging from 1 through 255.

Default:
Disable

config router vrrp interface advinterval

This command sets the advertisement value for a virtual router.

Syntax:

```
config router vrrp interface advinterval port vrid seconds
```

where:

- the *vrid* has an integer value ranging from 1 through 255.
- the value for *seconds* is the time between the transmission of VRRP advertisements.

Default:
1

config router vrrp interface authdetails

This command sets the authorization values for the virtual router configured on the specified interface. The options for the parameter auth type are None or Simple. The parameter [key] is optional, it is only required when the authorization type is Simple.

Syntax:

```
config router vrrp interface authdetails port vrid none/simple [key]
```

where *vrid* has an integer value ranging from 1 through 255.

Default:
None

config router vrrp interface ipaddress

This command sets the IP address value for a virtual router. The value for *ipaddr* is the IP address which is to be configured on the specified interface for VRRP.

Syntax:

```
config router vrrp interface ipaddress port vrid ipaddr
```

where *vrid* has an integer value ranging from 1 through 255.

config router vrrp interface preemptmode

This command sets the preemption value for the virtual router configured on the specified interface which determines whether a higher priority backup virtual router will preempt a lower priority router. If Disable is specified and this Virtual Router is a backup, it will never preempt a router.

Syntax:

```
config router vrrp interface preemptmode port vrid enable/disable
```

where *vrid* has an integer value ranging from 1 through 255.

Default:
enable

config router vrrp interface priority

This command sets the priority value for the virtual router configured on the specified interface.

Syntax:

```
config router vrrp interface priority port vrid priority
```

where:

- the *vrid* has an integer value ranging from 1 through 255.
- the *priority* of the interface is an integer from 1 through 254.

Default:
100

config router vrrp interface routerid

This command sets the virtual router ID on the specified interface.

Syntax:

```
config router vrrp interface routerid port vrid
```

where *vrid* has an integer value ranging from 1 through 255.

config router vrrp removedetails

This command removes all VRRP configuration details for a specific interface.

Syntax:

```
config router vrrp removedetails port vrid
```

where *vrid* has an integer value ranging from 1 through 255.

show router vrrp info

Use this command to display global VRRP information.

Syntax:

```
show router vrrp info
```

Return values:

VRRP Admin Mode
Displays the administrative mode of VRRP functionality on the switch.

Router Checksum Errors
The total number of VRRP packets received with an invalid VRRP checksum value.

Router Version Errors
The total number of VRRP packets received with unknown or unsupported version number.

Router VRID Errors
The total number of VRRP packets received with an invalid Virtual Router ID (VRID) for this virtual router.

show router vrrp interface detailed

Use this command to display all configuration information and VRRP router statistics for a virtual router configured on a specific interface.

Syntax:

```
show router vrrp interface detailed port vrid
```

Return values:

IP address
This field contains the configured IP address for the virtual router. The default is 0.0.0.0.

VMAC address
The virtual MAC address, associated with the virtual router, is a 48-bit field composed of a 24 bit enterprise unique identifier, and a 16 bit constant identifying the VRRP address block and the 8 bit VRID.

Authentication type
The authentication type for the specified virtual router. The choices are:

- 0-None - No authentication will be performed.
- 1-Simple - Authentication will be performed using a text password.

Priority
The priority value used by the VRRP router in the election for the master virtual router.

Advertisement interval
The time, in seconds, between the transmission of advertisement packets by the virtual router.

Preempt Mode
The preemption mode configured on the specified virtual router.

- Enable - If the virtual router is a backup router and the IP address of the virtual router is not owned by the master router, then the virtual router will preempt the master router if it has a priority greater than the priority of the master router.
- Disable - if the virtual router is a backup router it will not preempt the master router even if the virtual router priority is greater.

Administrative Mode
The status (enable or disable) of the virtual router.

State The state (Initialize/Master/Backup) of the virtual router.

show router vrrp interface stats

Use this command to display statistical information about each virtual router configured on the switch.

Syntax:

```
show router vrrp interface stats port vrid
```

Return values:

UpTime The time, in days, hours, minutes, and seconds, that has elapsed since the virtual router transitioned to the initialized state.

State Transitioned to Master
The total number of times the virtual router state has changed to Master.

Advertisement Received
The total number of VRRP advertisements received by this virtual router.

Advertisement Interval Errors
The total number of VRRP advertisements received for which the advertisement interval was different than the configured value for this virtual router.

Authentication Failure
The total number of VRRP packets received that did not pass the authentication check.

IP TTL errors The total number of VRRP packets received by the virtual router with IP TTL (time to live) not equal to 255.

Zero Priority Packets Received
The total number of VRRP packets received by the virtual router with a priority of ‘0’.

Zero Priority Packets Sent
The total number of VRRP packets sent by the virtual router with a priority of ‘0’.

Invalid Type Packets Received
The total number of VRRP packets received by the virtual router with an invalid type field.

Address List Errors
The total number of VRRP packets received for which the address list does not match the locally configured list for the virtual router.

Invalid Authentication Type
The total number of VRRP packets received with unknown authentication type.

Authentication Type Mismatch
The total number of VRRP advertisements received for which auth type is not equal to the auth type configured locally for this virtual router.

Packet Length Errors
The total number of VRRP packets received with packet length less than the length of the VRRP header.

show router vrrp interface summary

Use this command to display information about each virtual router.

Syntax:

```
show router vrrp interface summary
```

Return values:

Port The interface used by the virtual router.

VRID The router ID of the virtual router.

Virtual IP address
The router IP address.

Interface IP address
The actual IP address that is associated with the interface used by the Virtual Router.

VMAC address
The virtual MAC address, associated with the virtual router, is a 48-bit field composed of a 24-bit enterprise unique identifier, a 16-bit constant identifying the VRRP address block, and the 8-bit VRID.

Mode Whether the virtual router is enabled or disabled.

State The state (Initialize/Master/Backup) of the virtual router.

Chapter 5. Class of service commands

This chapter describes the two class of service commands available for the Ethernet switch module.

config classofservice 802.1pmapping

Use this command to map a user priority to a traffic class priority queue.

Syntax:

```
config classofservice 802.1pmapping user_priority
traffic_class_priority_queue
```

where

- *user_priority* is an integer ranging from 0 through 7.
- *traffic_class_priority_queue* is an integer ranging from 0 through 7.

Default:

Table 2. Classofservice 802.1p Mapping

IEEE 802.1p priority	IXE5416 priority queue
0	2
1	1
2	0
3	3
4	4
5	5
6	6
7	7

show classofservice 802.1pmapping

Use this command to show the current mapping of IEEE 802.1p priority values to traffic class priority queues.

Syntax:

```
show classofservice 802.1pmapping
```

Return values:

User Priority The IEEE 802.1p priority number. The range is 0 through 7.

Traffic Class Priority Queue
The priority queue number. The range is 0 through 7.

Chapter 6. Security configuration commands

This section describes the following commands that you use to configure and manage the security features of the Ethernet switch module:

- Authentication commands
- IEEE 802.1X Port-based network access control
- Remote Authentication Dial-In User Service (RADIUS)
- Secure Shell (SSH) commands
- Secure Socket Layer (SSL) commands

Authentication commands

config authentication login create

Use this command to create an authentication login list. The *listname* is up to 15 alphanumeric characters and is case sensitive. Up to 10 authentication login lists can be configured on the switch. When a list is created, the authentication method “local” is set as the first method. Authentication methods can be changed using the config authentication login set command.

Syntax:

```
config authentication login create listname
```

config authentication login delete

Use this command to delete the specified authentication login list. The command will fail if any of the following conditions are true:

- The login list name is invalid or does not identify an existing login list.
- The specified login list is currently assigned to a user or to the nonconfigured user.
- The specified login list is the default login list included with the default configuration and was not created using the **config authentication login set** command.

Syntax:

```
config authentication login delete listname
```

config authentication login set

Use this command to configure an ordered list of methods for the specified authentication login list. You may specify up to three methods. The possible methods are local, radius, and reject.

The value of local indicates that the user locally stored ID and password should be used for authentication. The value of radius indicates that the user ID and password will be authenticated using the RADIUS server. The value of reject indicates that the user is never authenticated.

To authenticate a user, the authentication methods in the user login list will be attempted in order until an authentication attempt succeeds or fails.

Note that the default login list included with the default configuration can not be changed.

Syntax:
```
config authentication login set listname local/radius/reject
[local/radius/reject] [local/radius/reject]
```

config users defaultlogin

Use this command to assign the authentication login list to be used when a non-configured user attempts to log in to the system. This setting is overridden by the authentication login list assigned to a specific user if the user is configured locally. If this value is not configured, users will be authenticated using local authentication only.

Syntax:
```
config users defaultlogin listname
```

config users login

Use this command to assign the specified authentication login list to the specified user for system login. The *user* must be a configured user and *listname* must be a configured login list.

If the user is assigned a login list that requires remote authentication, all access to the interface from CLI, web, and Telnet sessions will be blocked until the authentication is complete. Refer to the discussion of maximum delay in the config radius maxretransmit and config radius timeout commands.

Note that the login list associated with the user with Read/write privileges cannot be changed, to prevent accidental lockout from the switch.

Syntax:
```
config users login user listname
```

show authentication login info

Use this command to display the ordered authentication methods for all authentication login lists.

Syntax:
```
show authentication login info
```

Return values:

Authentication Login List
The login list whose information is displayed on this line.

Method 1 The first method in the login list, if any.

Method 2 The second method in the login list, if any.

Method 3 The third method in the login list, if any.

show authentication login users

Use this command to display information about the users assigned to the specified login list. If the login list is assigned to non-configured users, the word “default” will appear as the user name.

Syntax:
```
show authentication login users listname
```

Return values:

User	The user assigned to the specified login list.
Component	The component, either user or 802.1X, for which the login list is assigned.

show users authentication

Use this command to display all user and authentication login information for the switch, including the login list assigned to the default user.

Syntax:

```
show users authentication
```

Return values:

User	A list of all users with an assigned login list.
System login	The authentication login list assigned to the user for system login.
802.1X	The authentication login list assigned to the user for IEEE 802.1X port security.

IEEE 802.1X commands

clear dot1x port stats

Use this command to reset the IEEE 802.1X statistics for the specified ports.

Syntax:

```
clear dot1x port stats port/all
```

config dot1x adminmode

Use this command to enable or disable authentication support on the switch. The default value is disable. In disabled mode, the dot1x configuration is retained and can be changed, but it is not activated.

Syntax:

```
config dot1x adminmode enable/disable
```

Default:
disable

config dot1x defaultlogin

Use this command to assign the authentication login list to use for non-configured users for IEEE 802.1X port security. This setting is overridden by the authentication login list assigned to a specific user if the user is configured locally. If this value is not configured, users will be authenticated using local authentication only.

Syntax:

```
config dot1x defaultlogin listname
```

config dot1x login

Use this command to assign the specified authentication login list to the specified user for port security. The `user` must be a configured user and the `listname` must be a configured login list.

Syntax:

```
config dot1x login user listname
```

config dot1x port controlmode

Use this command to configure the authentication mode to be used on the specified port or ports.

Syntax:

```
config dot1x port controlmode port/listofports/all
forceunauthorized/forceauthorized/auto
```

Where the type of controlmode is one of the following:

forceunauthorized
The authenticator Port Access Entity (PAE) unconditionally sets the controlled ports to unauthorized mode.

forceauthorized
The authenticator PAE unconditionally sets the controlled ports to authorized mode.

auto
The authenticator PAE sets the controlled ports mode to reflect the result of the authentication exchanges between the supplicant, authenticator, and authentication server.

Default:
auto

config dot1x port initialize

Use this command to begin the initialization sequence on the specified port. This command is only valid if dot1x is enabled and the control mode for the specified port is “auto”.

Syntax:

```
config dot1x port initialize port
```

Default:
disable

config dot1x port maxrequests

Use this command to configure the maximum number of times the authenticator state machine on the specified port will retransmit an Extensible Authentication Protocol Over LANs (EAPOL) EAP Request/Identity before timing out the supplicant.

Syntax:

```
config dot1x port maxrequests port requests
```

where *requests* is an integer ranging from 1 through 10 and represents the maximum requests.

Default:
2

config dot1x port quietperiod

Use this command to configure the value, in seconds, of the timer used by the authenticator state machine on the specified port to define periods of time in which it will not attempt to acquire a supplicant. The quiet period is the period for which the authenticator does not attempt to acquire a supplicant after a failed authentication exchange with the supplicant. The quiet period must be a value in the range of 0 and 65535.

Syntax:

```
config dot1x port quietperiod port seconds
```

where *seconds* is an integer from 0 through 65535 and represents the quiet period, in seconds.

Default:
60

config dot1x port reauthenabled

Use this command to enable or disable reauthentication of the supplicant for the specified port. The reauthenabled value must be true or false. If the value is true reauthentication will occur. Otherwise, reauthentication will not be allowed.

Syntax:

```
config dot1x port reauthenabled port true/false
```

Default:
false

config dot1x port reauthenticate

Use this command to begin the reauthentication sequence on the specified port. This command is only valid if dot1x is enabled and the control mode for the specified port is “auto”.

Syntax:

```
config dot1x port reauthenticate port
```

Default:
disable

config dot1x port reauthperiod

Use this command to configure the value, in seconds, of the timer used by the authenticator state machine on this port to determine when reauthentication of the supplicant takes place.

Syntax:

```
config dot1x port reauthperiod port seconds
```

where *seconds* is an integer from 1 through 65535 and represents the reauthorization timer in seconds.

Default:
3600

config dot1x port servertimeout

Use this command to configure the value, in seconds, of the timer used by the authenticator on the specified port to timeout the authentication server.

Syntax:

```
config dot1x port servertimeout port seconds
```

where *seconds* is an integer from 1 through 65535 and represents the timeout timer in seconds.

Default:
30

config dot1x port supptimeout

Use this command to configure the value, in seconds, of the timer used by the authenticator state machine on the specified port to timeout the supplicant.

Syntax:

```
config dot1x port supptimeout port seconds
```

where *seconds* is an integer from 1 through 65535 and represents the timeout timer in seconds.

Default:
30

config dot1x port transmitperiod

Use this command to configure the value, in seconds, of the timer used by the authenticator state machine on the specified port to determine when to send an EAPOL EAP Request/Identity frame to the supplicant.

Syntax:

```
config dot1x port transmitperiod port seconds
```

where *seconds* is an integer from 1 through 65535 and represents the transmit period in seconds.

Default:
30

config dot1x port users add

Use this command to add the specified user to the list of users with access to the specified ports. The user must be a configured user and the port must be a valid port. By default, a user is given access to all ports.

Syntax:

```
config dot1x port users add user port/all
```

Default:
all

config dot1x port users remove

Use this command to remove the specified user from the list of users with access to the specified ports.

Syntax:

```
config dot1x port users remove user port/all
```

show dot1x port detailed

Use this command to display the details of the IEEE 802.1X configuration parameters for the specified port.

Syntax:

```
show dot1x port detailed port
```

Return values:

Port The interface whose configuration is displayed on this row.

Protocol Version
The version of IEEE 802.1X active on the port. Currently this is always 1.

PAE Capabilities
The port access entity state of the port. Either authenticator of supplicant.

Authenticator PAE State
The current state of the authenticator state machine. Possible values are initialize, disconnected, connecting, authenticating, authenticated, aborting, held, forceauthorized, and forceunauthorized.

Backend Authentication State
The current state of the back-end authentication state machine. Possible values are request, response, success, fail, timeout, idle, and initialize.

Quiet Period (secs)
The timer used by the authenticator state machine on this port to define periods of time in which it will not attempt to acquire a supplicant. The value is expressed in seconds and is an integer from 0 through 65535.

Transmit Period (secs)
The timer used by the authenticator state machine on the specified port to determine when to send an EAPOL EAP Request/Identity frame to the supplicant. The value is expressed in seconds and is an integer from 1 through 65535.

Supplicant Timeout (secs)
The timer used by the authenticator state machine on this port to timeout the supplicant. The value is expressed in seconds is an integer from 1 through 65535.

Server Timeout (secs)
The timer used by the authenticator on this port to timeout the authentication server. The value is expressed in seconds and is an integer from 1 through 65535.

Maximum Requests

The maximum number of times the authenticator state machine on this port will retransmit an EAPOL EAP Request/Identity before timing out the supplicant. The value is an integer from 1 through 10.

Reauthentication Period (secs)

The timer used by the authenticator state machine on this port to determine when reauthentication of the supplicant takes place. The value is expressed in seconds and is an integer from 1 through 65535.

Reauthentication Enabled

Indicates whether reauthentication is enabled for the port.

Key Transmission Enabled

Indicates whether a key is transmitted to the supplicant from the port.

Control Direction

Indicates the control direction for the port. Possible values are both and in.

show dot1x port stats

Use this command to display the IEEE 802.1X statistics for the specified port.

Syntax:

show dot1x port stats *port*

Return values:

Port The interface whose statistics are displayed on this row.

EAPOL Frames Received

The number of valid Extensible Authentication Protocol over LANs (EAPOL) frames of any type that have been received by the authenticator port.

EAPOL Frames Transmitted

The number of valid EAPOL frames of any type that have been transmitted by the authenticator port.

EAPOL Start Frames Received

The number of EAPOL start frames that have been received by the authenticator port.

EAPOL Logoff Frames Received

The number of EAPOL logoff frames that have been received by the authenticator port.

Last EAPOL Frame Version

The protocol version number in the most recently received EAPOL frame.

Last EAPOL Frame Source

The source MAC address in the most recently received EAPOL frame.

EAP Response/ID Frames Received

The number of EAP response/identity frames that have been received by the authenticator port.

EAP Response Frames Received
The number of EAP response frames (other than response/identity frames) that have been received by the authenticator port.

EAP Request/ID Frames Transmitted
The number of EAP response/identity frames that have been transmitted by the authenticator port.

EAP Response Frames Transmitted
The number of EAP response frames (other than response/identity frames) that have been transmitted by the authenticator port.

Invalid EAPOL Frames Received
The number of EAPOL frames that have been received by the authenticator port with an unrecognized frame type.

EAP Length Error Frames Received
The number of EAPOL frames that have been received by the authenticator port with an incorrect length.

show dot1x port summary

Use this command to display a summary of the IEEE 802.1x configuration parameters for the specified ports.

Syntax:

```
show dot1x port summary port/listofports/all
```

Return values:

Port The interface whose configuration is displayed on this row.

Control Mode The configured control mode: forceunauthorized, forceauthorized or auto.

Operating Control Mode
The active control mode.

Reauthentication Enabled
Indicates whether reauthentication is enabled for the port.

Transmission Enabled
Indicates whether a key is transmitted to the supplicant from the port.

Port Status Indicates whether a port is authorized.

show dot1x port users

Use this command to display IEEE 802.1X port security information about locally configured users.

Syntax:

```
show dot1x port users port
```

Return values:

User The locally configured users with access to the specified port.

show dot1x summary

Use this command to display a summary of the IEEE 802.1X configuration parameters for the switch.

Syntax:

```
show dot1x summary
```

Return values:

Administrative mode
Indicates whether authentication control is enabled on the switch.

Remote Authentication Dial-In User Service (RADIUS) commands

config radius accounting mode

Use this command to enable or disable the RADIUS accounting function.

Syntax:

```
config radius accounting mode enable/disable
```

Default:
disable

config radius accounting server add

Use this command to configure the IP address to be used to access the accounting server. Only a single accounting server can be configured. If an accounting server is currently configured it must be removed using the config radius accounting server remove command before this command will succeed.

Syntax:

```
config radius accounting server add ipaddr
```

config radius accounting server port

Use this command to configure which User Datagram Protocol (UDP) port will be used to access the accounting server. The IP address specified must match that of the previously configured accounting server. If a port is already configured for the accounting server, the new port will replace the previously configured value.

Syntax:

```
config radius accounting server port ipaddr port
```

where *`port`* is an integer from 0 through 65535 and represents the UDP port that will be used to access the accounting server.

Default:
1813

config radius accounting server remove

Use this command to remove a configured accounting server. The IP address specified must match that of the previously configured accounting server. Since only a single accounting server is supported, issuing this command will cause future accounting attempts to fail.

Syntax:

```
config radius accounting server remove ipaddr
```

config radius accounting server secret

Use this command to configure the secret shared between the RADIUS client and accounting server. The IP address specified must match that of the previously configured accounting server. When you enter this command, you will be prompted to enter the secret, which must be an alphanumeric value of 20 characters or less.

Syntax:

```
config radius accounting server secret ipaddr
```

show radius accounting stats

Use this command to display the RADIUS statistics for the accounting server.

Syntax:

```
show radius accounting stats ipaddr
```

Return values:

Accounting Server IP address
The IP address of the server whose statistics are displayed on this row.

Round Trip Time
The time, in hundredths of a second, between the most recent RADIUS accounting response and the matching accounting request from this RADIUS accounting server.

Accounting Requests
The number of RADIUS accounting request packets sent to this accounting server, not including retransmissions.

Accounting Retransmissions
The number of RADIUS accounting request packets retransmitted to this accounting server.

Accounting Responses
The number of RADIUS packets received from this accounting server.

Malformed Accounting Responses
The number of malformed RADIUS accounting response packets received from this accounting server, including packets with invalid length but not including packets with bad authenticators or unknown types.

Bad Authenticators
The number of RADIUS accounting response packets received from this accounting server, including packets with invalid authenticators.

Pending Requests
The number of RADIUS accounting request packets sent to this accounting server that have not yet timed out or received a response.

Timeouts
The number of RADIUS packets sent to this accounting server that have timed out.

Unknown Types
The number of RADIUS packets of unknown type received from this accounting server.

Packets Dropped
The number of RADIUS packets received from this accounting server dropped for a reason not otherwise included in this list.

show radius accounting summary

Use this command to display a summary of the RADIUS accounting configuration parameters for the switch.

Syntax:
```
show radius accounting summary
```

Return values:

Accounting Mode
Indicates whether accounting mode is enabled or disabled.

IP address The IP address of the RADIUS accounting server currently in use.

Port The port used to access the accounting server.

Secret configured
Indicates whether a secret has been configured for the accounting server.

clear radius stats

Use this command to reset all RADIUS statistics for the switch. You will be prompted to confirm this choice.

Syntax:
```
clear radius stats
```

config radius maxretransmit

Use this command to configure the maximum number of times a request packet is retransmitted when no response is received from the RADIUS server.

Consideration should be given to the maximum delay time when configuring RADIUS maxretransmit and timeout values. If multiple RADIUS servers are configured, the maxretransmit value on each will be exhausted before the next server is attempted. A retransmit will not occur until the configured timeout value on that server has passed without a response from the RADIUS server. Therefore, the maximum delay in receiving a response from the RADIUS application equals the sum of maxretransmit times timeout for all configured servers. If the RADIUS request was generated by a user login attempt, all user interfaces will be blocked until the RADIUS application returns a response.

Syntax:
```
config radius maxretransmit max_times
```

where *max_times* is an integer from 1 through 15 and represents the maximum number of times a request packet is retransmitted when no response is received from the RADIUS server.

Default:
4

config radius timeout

Use this command to configure the timeout value (in seconds) after which a request must be retransmitted to the radius server if no response is received.

Consideration should be given to the maximum delay time when configuring RADIUS maxretransmit and timeout values. If multiple RADIUS servers are configured, the maxretransmit value on each will be exhausted before the next server is attempted. A retransmit will not occur until the configured timeout value on that server has passed without a response from the RADIUS server. Therefore, the maximum delay in receiving a response from the RADIUS application equals the sum of maxretransmit times timeout for all configured servers. If the RADIUS request was generated by a user login attempt, all user interfaces will be blocked until the RADIUS application returns a response.

Syntax:

```
config radius timeout seconds
```

where *seconds* is an integer from 1 through 30 and represents the timeout value (in seconds) after which a request must be retransmitted to the radius server if no response is received.

Default:
5

show radius stats

Use this command to display RADIUS statistics for the switch that are not associated with a specific server or accounting server.

Syntax:

```
show radius stats
```

Return values:

Invalid Server Address
The number of RADIUS access response packets received from an unknown address.

show radius summary

Use this command to display a summary of the RADIUS configuration parameters for the switch.

Syntax:

```
show radius summary
```

Return values:

Current Server IP address
The IP address of the RADIUS server currently used for authentication.

Number of Configured Servers
The number of RADIUS servers that have been configured.

Max Number of Retransmits
The maximum number of times a request packet will be retransmitted.

Timeout Duration (secs)
The timeout value, in seconds, for request retransmissions.

Accounting Mode
Indicates whether accounting is currently enabled.

config radius server add

Use this command to configure the IP address used to connect to a RADIUS server. Up to three servers can be configured for each RADIUS client. If three servers are currently configured, one must be removed using the **config radius server remove** command before the add command will succeed. Once a server has been added it will be identified in future commands by its IP address.

Syntax:

```
config radius server add ipaddr
```

config radius server msgauth

Use this command to enable or disable the message authenticator attribute for the specified RADIUS server. Enabling the message authenticator attribute provides additional security for the connection between the RADIUS client and server. Some RADIUS servers require that the message authenticator attribute be enabled before authentication requests from the RADIUS client will be accepted. The IP address specified must match that of a configured server.

Syntax:

```
config radius server msgauth ipaddr enable/disable
```

config radius server port

Use this command to configure which UDP port will be used to access the specified RADIUS server. The IP address specified must match that of the previously configured RADIUS server.

Syntax:

```
config radius server port ipaddr port
```

where *port* is an integer from 0 through 65535.

Default:
1812

config radius server primary

Use this command to specify which configured server should be the primary server for this RADIUS client. The primary is the server that is used by default for handling RADIUS requests. The remaining configured servers are used only if the primary server cannot be reached. A maximum of three servers can be configured on each client. Only one server can be configured as the primary server. If a primary server is currently configured and this command is issued, the server specified by the IP address used in this command will become the new primary server. The IP address specified must match that of a configured server.

Syntax:

```
config radius server primary ipaddr
```

config radius server remove

Use this command to remove a configured RADIUS server. The IP address specified must match that of the previously configured RADIUS server. When a server is removed all configuration for the server is erased including the shared secret. If the removed server was the primary server, one of the remaining configured servers will be used as the RADIUS server for future RADIUS requests.

Syntax:

```
config radius server remove ipaddr
```

config radius server secret

Use this command to configure the secret shared between the RADIUS client and server. A secret must be configured for each RADIUS server. The IP address specified must match that of a previously configured RADIUS server. When you enter this command, you will be prompted to enter the secret, which must be an alphanumeric value of 20 characters or less.

Syntax:

```
config radius server secret ipaddr
```

show radius server stats

Use this command to display the statistics for a configured RADIUS server.

Syntax:

```
show radius server stats ipaddr
```

Return values:

Server IP address
The IP address of the server whose information is displayed on this row.

Round Trip Time
The time, in seconds, between the most recent RADIUS access reply/access challenge, and the matching access request from this RADIUS server.

Access Requests
The number of RADIUS access request packets sent to this server, not including retransmissions.

Access Retransmissions
The number of RADIUS access request packets retransmitted to this server.

Access Accepts
The number of RADIUS Access-Accept packets, both valid and invalid, received from this server.

Access Rejects
The number of RADIUS Access-Reject packets, both valid and invalid, received from this server.

Access Challenges
The number of RADIUS access challenge packets, both valid and invalid, received from this server.

Malformed Access Responses
The number of malformed RADIUS access response packets received from this server, including packets with invalid length but not including packets with bad authenticators, bad signature attributes or unknown types.

Bad Authenticators
The number of RADIUS access response packets received from this server, including packets with invalid authenticators or signature attributes.

Pending Requests
The number of RADIUS access request packets sent to this server that have not yet timed out or received a response.

Timeouts The number of RADIUS packets sent to this server that have timed out.

Unknown Types
The number of RADIUS packets of unknown type received from to this server.

Packets Dropped
The number of RADIUS packets received from this server dropped for a reason not otherwise included in this list.

show radius server summary

Use this command to display a summary of the configured RADIUS servers.

Syntax:

```
show radius server summary
```

Return values:

Current Indicates the server currently in use for authentication.

IP address The IP address of the authentication server.

Port The port used to access the authentication server.

Type Indicates whether the server is primary or secondary.

Secret configured
Indicates whether a secret has been configured for the authentication server.

Secure Shell (SSH) commands

config ssh adminmode

Use this command to enable or disable SSH.

Syntax:

```
config ssh adminmode enable/disable
```

Default:
Disabled

config ssh protocol

Use this command to set or remove protocol levels (or versions) for SSH. Either SSH1 (1), SSH2 (2), or both (1 and 2) can be set.

Syntax:

```
config ssh protocol ssh1/ssh2/both
```

Default:
both

show ssh info

Syntax:

```
show ssh info
```

Return values:

Administrative Mode
Indicates whether the administrative mode of SSH is enabled or disabled.

Protocol Level
The protocol level may have the values of version 1, version 2 or both versions 1 and 2.

Connections Specifies the current SSH connections.

Secure Socket Layer (SSL) commands

config http secureport

Use this command to configure the SSL port.

Syntax:

```
config http secureport port
```

where *port* is an integer from 1 through 65535.

Default:
443

config http secureprotocol

Use this command to enable or disable SSL and set protocol levels (versions). The protocol level can be set to TLS1, SSL3, or to both TLS1 and SSL3.

Syntax:

```
config ip http secure-protocol ssl3/tls1/both add/remove
```

Default:
both

config http secureserver adminmode

Command is used to enable/disable the SSL for secure HTTP.

Syntax:

```
config http secureserver adminmode enable/disable
```

Default:
disable

show http info

Displays the http settings for the switch.

Syntax:
```
show http info
```

Return values:

Mode Privileged EXEC

Secure-Server Administrative Mode
Indicates whether the administrative mode of secure HTTP is enabled or disabled.

Secure Protocol Level
The protocol level may have the values of SSL3, TSL1 or both.

Secure Port Specifies the port configured for SSL.

HTTP Mode Indicates whether the HTTP mode is enabled or disabled.

Chapter 7. Quality of Service (QoS) commands

This section describes the following commands that you use to configure and manage the Quality of Service (QoS) features of the Ethernet switch module:

- Access Control Lists (ACLs)
- Bandwidth provisioning

Access Control List (ACL) commands

An ACL consists of a set of rules which are matched sequentially against a packet. When a packet meets the match criteria of a rule, the specified rule action (permit/deny) is taken and the additional rules are not checked for a match. This section describes the commands you use to specify the interfaces to which an ACL applies and its match criteria. ACLs can not be applied directly to a LAG interface. They must be applied to all member pots in a LAG to take effect.

config acl create

Use this command to create an ACL.

Syntax:
```
config acl create aclid
```

where `aclid` is an integer from 1 through 100 representing a new ACL.

config acl delete

Use this command to delete an ACL from the system.

Syntax:
```
config acl delete aclid
```

where `aclid` is an integer from 1 through 100 representing an existing ACL.

config acl interface add

Use this command to associate an ACL with an interface and specify whether it affects inbound or outbound traffic. The `direction` parameter only supports inbound.

Syntax:
```
config acl interface add port direction aclid
```

where `aclid` is an integer from 1 through 100 representing an ACL to add.

config acl interface remove

Use this command to disassociate an ACL from an interface for the specified direction. The `direction` parameter can have the values of in or out. The `aclid` parameter specifies the ACL to remove.

Syntax:
```
config acl interface remove port direction aclid
```

where `aclid` is an integer from 1 through 100 representing an ACL to remove.

config acl rule action

Use this command to specify the action for the ACL and rule referenced by the parameters `aclid` and `rulenum`. The values of permit or deny indicate how this rule is applied.

Syntax:

```
config acl rule action aclid rulenum permit/deny
```

where

- *aclid* is an integer from 1 through 100.
- *rulenum* is an integer from 1 through 10 representing a user-specified rule.

config acl rule create

Use this command to create a rule within the ACL. An ACL may have up to 10 user-specified rules ranging from 1 through 10. Rules are created with a default action of deny.

Syntax:

```
config acl rule create aclid rulenum
```

where

- *aclid* is an integer from 1 through 100 representing an existing ACL.
- *rulenum* is an integer from 1 through 10 representing a user-specified rule.

Default:
deny

config acl rule delete

Use this command to remove a rule from the ACL. The rule is identified by the `rulenum` parameter.

Syntax:

```
config acl rule delete aclid rulenum
```

where

- *aclid* is an integer from 1 through 100 representing an existing ACL.
- *rulenum* is an integer from 1 through 10 representing a user-specified rule.

config acl rule match dstip

Use this command to specify a destination IP address and mask match condition for the ACL rule referenced by the `aclid` and `rulenum` parameters. The `ipaddr` and `ipmask` parameters are 4-digit dotted-decimal numbers which represent the destination IP address and IP mask, respectively.

Syntax:

```
config acl rule match dstip aclid rulenum ipaddr ipmask
```

where

- *aclid* is an integer from 1 through 100 representing an existing ACL.
- *rulenum* is an integer from 1 through 10 representing a user-specified rule.

config acl rule match dstl4port keyword

Use this command to specify a destination layer 4 port match condition for the ACL rule referenced by the `aclid` and `rulenum` parameters. The `portkey` parameter uses a single keyword notation and currently has the values of domain, echo, ftp, ftpdata, http, smtp, snmp, Telnet, tftp, and www. Each of these values translates into its equivalent port number, which is used as both the start and end of a port range.

This command and the **config acl match destl4port number** command are two methods of specifying the destination layer 4 port range as a match condition. Either command can be used to configure or modify the destination layer 4 port range.

Syntax:

```
config acl rule match dstl4port keyword aclid rulenum portkey
```

where

- *aclid* is an integer from 1 through 100 representing an existing ACL.
- *rulenum* is an integer from 1 through 10 representing a user-specified rule.

config acl rule match dstl4port number

Use this command to specify a destination layer 4 port match condition for the ACL rule referenced by the `aclid` and `rulenum` parameters. The `startport` and `endport` parameters identify the first and last ports that are part of the port range. They have values from 0 through 65535. The ending port must have a value equal to or greater than the starting port. The starting port, ending port and all ports in between will be part of the destination port range.

Either this command or the **config acl match destl4port keyword** command may be used to specify a destination layer 4 port range as a match condition.

Syntax:

config acl rule match dstl4port number *aclid rulenum startport endport*

where

- *aclid* is an integer from 1 through 100.
- *rulenum* is an integer from 1 through 10 representing a user-specified rule.

config acl rule match every

Use this command to specify a match condition in which all packets will be considered to match the ACL rule referenced by the `aclid` and `rulenum` parameter. If the parameter `true/false` is set to true, all packets will be either permitted or denied based on the action setting for the rule and no other match conditions may be specified. Specifying false allows other match conditions to be specified.

Syntax:

```
config acl rule match every aclid rulenum true/false
```

where

- *aclid* is an integer from 1 through 100.
- *rulenum* is an integer from 1 through 10 representing a user-specified rule.

config acl rule match protocol keyword

Use this command to specify the IP protocol of a packet as a match condition for the ACL rule referenced by the `aclid` and `rulenum` parameters. The `protocolkey` parameter identifies the protocol using a single keyword notation and has the possible values of ICMP, IGMP, IP, TCP, and UDP. A protocol keyword of ip is interpreted to match all protocol number values.

Either this command or the **config acl match protocol number** command can be used to specify an IP protocol value as a match criterion.

Syntax:

```
config acl rule match protocol keyword aclid rulenum protocolkey
```

where

- *aclid* is an integer from 1 through 100.
- *rulenum* is an integer from 1 through 10 representing a user-specified rule.

config acl rule match protocol number

Use this command to specify a protocol number as a match condition for the ACL rule referenced by the `aclid` and `rulenum` parameters. The `protocolnum` parameter identifies the protocol by number. The protocol number is a standard value assigned by IANA and is an integer from 0 through 255. Either this command or the **config acl match protocol keyword** command can be used to specify an IP protocol value as a match criterion.

Syntax:

```
config acl rule match protocol number aclid rulenum protocolnum
protocolmask
```

where

- *aclid* is an integer from 1 through 100.
- *rulenum* is an integer from 1 through 10 representing a user-specified rule.

config acl rule match srcip

Use this command to specify a packet source IP address and Mask as a match condition for the ACL rule referenced by the `aclid` and `rulenum` parameters. The `ipaddr` and `ipmask` parameters are 4-digit dotted-decimal numbers which represent the source IP address and IP mask, respectively.

Syntax:

```
config acl rule match srcip aclid rulenum ipaddr ipmask
```

where

- *aclid* is an integer from 1 through 100.
- *rulenum* is an integer from 1 through 10 representing a user-specified rule.

config acl rule match srcl4port keyword

Use this command to specify a source layer 4 port match condition for the ACL rule referenced by the `aclid` and `rulenum` parameters. The `portkey` uses a single keyword notation and has the possible values of domain, echo, ftp, ftpdata, http, smtp, snmp, Telnet, tftp, and www. Each of these values translates into its equivalent port number, which is used as both the start and end of the port range.

This command and the **config acl match srcl4port number** command are two methods of specifying the source layer 4 port range as a match condition. Either command can be used to configure or modify the source layer 4 port range.

Syntax:

```
config acl rule match srcl4port keyword aclid rulenum portkey
```

where

- *aclid* is an integer from 1 through 100.
- *rulenum* is an integer from 1 through 10 representing a user-specified rule.

config acl rule match srcl4port number

Use this command to specify a packet source layer 4 port match condition for the ACL rule referenced by the `aclid` and `rulenum` parameters. The `startport` and `endport` parameters identify the first and last ports that are part of the port range and have values from 0 through 65535. The ending port must have a value equal or greater than the starting port. The starting port, ending port and all ports in between will be part of the contiguous source port range.

Either this command or **config acl match srcl4port keyword** can be used to specify a source layer 4 port range as a match criterion.

Syntax:

```
config acl rule match srcl4port range aclid rulenum startport endport
```

where

- *aclid* is an integer from 1 through 100.
- *rulenum* is an integer from 1 through 10 representing a user-specified rule.

show acl detailed

Use this command to display an ACL and all of the rules that are defined for the ACL. The `aclid` is the number used to identify the ACL.

Syntax:

```
show acl detailed aclid
```

where `aclid` is an integer from 1 through 100.

Return values:

Rule Number Displays the number identifier for each rule that is defined for the ACL.

Action Displays the action that will be taken if a packet matches the rule's criteria. The choices are permit or deny.

Protocol Displays which IP protocol (if any) is a match condition for the rule. The possible values are ICMP, IGMP, IP, TCP, and UDP.

Source IP address
Displays the source IP address (if any) that is a match condition for this rule.

Source IP Mask
Displays the source IP mask (if any) that is a match condition for this rule.

Source Ports Displays the source port range (if any) that is a match condition for this rule.

Service Type Field Match
Indicates whether an IP DSCP, IP Precedence or IP TOS match condition is specified for this rule.

Service Type Field Value
Indicates the value specified for the Service Type Field Match (IP DSCP, IP Precedence or IP TOS) if it a match condition for this rule.

show acl summary

Use this command to display a summary of the ACLs associated with interfaces in the system.

Syntax:

```
show acl summary
```

Return values:

ACL ID Displays the ACL identifier.

Rules Displays the number of rules that are associated with this ACL.

Interfaces Displays the interfaces associated with this ACL.

Direction Displays the packet filtering direction for the ACL on the interface. The possible values displayed are inbound and outbound.

Bandwidth provisioning commands

config bwprovisioning bwallocation create

Use this command to create a bandwidth allocation profile.

Syntax:

```
config bwprovisioning bwallocation create name
```

where *name* is an alphanumeric string up to 15 characters, and represents the bandwidth allocation profile.

config bwprovisioning bwallocation delete

Use this command to delete a bandwidth allocation profile from the system. A bandwidth allocation profile may not be deleted while it is associated with a traffic class.

Syntax:

```
config bwprovisioning bwallocation delete name
```

where *name* is an alphanumeric string up to 15 characters, and is the user supplied name associated with the bandwidth allocation profile.

config bwprovisioning bwallocation maxbandwidth

This commands configures the maximum allowable bandwidth for this bandwidth allocation profile.

Syntax:

```
config bwprovisioning bwallocation maxbandwidth name maxbandwidth
```

where

- *name* is an alphanumeric string up to 15 characters, representing the user supplied name associated with the bandwidth allocation profile.
- *maxbandwidth* is an integer from 0 to the maximum bandwidth of the interface to be associated with this profile. The bandwidth allocation profile maximum bandwidth must be greater than or equal to the minimum bandwidth. If this value is set to 0, it will not allow any traffic for this bandwidth allocation profile.

Default:
100 Mbps

show bwprovisioning bwallocation detailed

Use this command to display detailed bandwidth allocation information for the specified bandwidth allocation profile.

Syntax:

```
show bwprovisioning bwallocation detailed name
```

where *name* is an alphanumeric string up to 15 characters, representing the user supplied name associated with the bandwidth allocation profile.

Return values:

Bandwidth Allocation Profile Name
Displays the user-defined name of this bandwidth allocation profile.

Minimum Bandwidth
Displays the minimum guaranteed bandwidth of this bandwidth allocation profile in Mbps.

Maximum Bandwidth
Displays the maximum allowable bandwidth of this bandwidth allocation profile in Mbps.

Associated Traffic Class(es)
Displays the traffic classes that have been associated with this bandwidth allocation profile. This field is blank if there are no traffic classes associated with this bandwidth allocation profile.

show bwprovisioning bwallocation summary

Use this command to display the bandwidth allocation information for all bandwidth allocation profiles in the system.

Syntax:

```
show bwprovisioning bwallocation summary
```

Return values:

Bandwidth Allocation Profile Name
Displays the user-defined name of this bandwidth allocation profile.

Minimum Bandwidth
Displays the minimum guaranteed bandwidth of this bandwidth allocation profile in Mbps.

Maximum Bandwidth

Displays the maximum allowable bandwidth of this bandwidth allocation profile in Mbps.

config bwprovisioning trafficclass bwallocation

Use this command to associate a bandwidth allocation profile with a traffic class. The *bwprofile* parameter must represent a valid bandwidth allocation profile.

Syntax:

```
config bwprovisioning trafficclass bwallocation name bwprofile
```

where

- *name* is an alphanumeric string up to 15 characters, representing the user supplied name associated with the bandwidth allocation profile.
- *bwprofile* is the name of the bandwidth allocation profile.

config bwprovisioning trafficclass create

Use this command to create a traffic class.

Syntax:

```
config bwprovisioning trafficclass create type name
```

where

- *type* is the type of traffic class. The only supported value for type is the string vlan.
- *name* is an alphanumeric string up to 15 characters, representing the traffic class.

config bwprovisioning trafficclass delete

Use this command to delete a traffic class from the system. When a traffic class is deleted, its association with a bandwidth allocation profile is automatically removed.

Syntax:

```
config bwprovisioning trafficclass delete name
```

where *name* is an alphanumeric string up to 15 characters, and identifies the traffic class to be deleted.

config bwprovisioning trafficclass port

Use this command to attach a traffic class to a specific interface. The *port* interface must indicate a valid physical or logical interface. The sum of the minimum bandwidth allocations of all traffic classes associated with the same interface should not exceed the total bandwidth of the interface. There is no restriction on the sum of the maximum bandwidth of all traffic classes attached to the same port. When a traffic class is attached to a LAG interface, the bandwidth allocation profile minimum bandwidth parameter will not be applicable to the traffic class.

Syntax:

```
config bwprovisioning trafficclass port name port
```

where *name* is an alphanumeric string up to 15 characters, and identifies the traffic class.

config bwprovisioning trafficclass vlan

Use this command to associate a VLAN with a traffic class.

Syntax:

```
config bwprovisioning trafficclass vlan name vlanid
```

where

- *name* is an alphanumeric string up to 15 characters, representing the user supplied name associated with the traffic class.
- *vlanid* is an integer from 1 through 4094 representing a VLAN. The VLAN parameter can identify an invalid VLAN (the VLAN does not have to exist in the system).

config bwprovisioning trafficclass weight

Use this command to configure the priority for this traffic class.

Syntax:

```
config bwprovisioning trafficclass weight name weight
```

where

- *name* is an alphanumeric string up to 15 characters, representing the user supplied name associated with the traffic class.
- *weight* is an integer from 1 through 1024 representing an ACL to add.

Default:

1

show bwprovisioning trafficclass allocatedbw

Use this command to display the bandwidth allocated. The allocated minimum bandwidth should not exceed the interface bandwidth unless the interface is a LAG interface.

Syntax:

```
show bwprovisioning trafficclass allocatedbw port
```

Return values:

Port The specified interface.

Allocated Minimum Bandwidth
Displays the sum of the minimum guaranteed bandwidth for all traffic classes configured on this interface.

Allocated Maximum Bandwidth
Displays the sum of the maximum allowable bandwidth for all traffic classes configured on this interface.

show bwprovisioning trafficclass detailed

Use this command to display the traffic class information for the specified traffic class.

Syntax:

```
show bwprovisioning trafficclass detailed name
```

name is an alphanumeric string up to 15 characters, representing the user supplied name associated with the traffic class.

Return values:

Traffic Class Name
Displays the name of this traffic class.

Port Displays the port to which this traffic class is attached.

VLAN ID Displays the VLAN ID with which this traffic class is associated.

Weight Displays the weight of this traffic class.

Accept Byte Count
Displays the number of bytes accepted.

Bandwidth Allocation Profile
Displays the bandwidth allocation profile associated with this traffic class. This field is blank when there is no bandwidth allocation profile associated with this traffic class.

The following attributes are only displayed when there is a bandwidth allocation profile associated with this traffic class.

Minimum Bandwidth
Displays the minimum bandwidth defined for this traffic class.

Maximum Bandwidth
Displays the maximum bandwidth defined for this traffic class.

show bwprovisioning trafficclass summary

Use this command to display the traffic class information for all traffic classes in the system.

Syntax:

```
show bwprovisioning trafficclass summary
```

Return values:

Traffic Class Name
Displays the user-defined name of this traffic class.

Port Displays the interface to which this traffic class is attached.

VLAN ID Displays the Virtual Local Area Network (VLAN) ID with which this traffic class is associated.

Weight Displays the weight of this traffic class.

Bandwidth Allocation Profile
Displays the bandwidth allocation profile associated with this traffic class. This field is blank when there is no bandwidth allocation profile associated with this traffic class.

Chapter 8. Multicast commands

This section describes the following Multicast commands for the Ethernet switch module:

- Distance Vector Multicast Routing Protocol (DVMRP) commands
- Internet Group Management Protocol (IGMP) commands
- Multicast (Mcast) commands
- Protocol Independent Multicast - Dense Mode (PIM-DM) commands
- Protocol Independent Multicast - Sparse Mode (PIM-SM) commands

The commands in each group fall into one of two functional categories:

- Show commands - displays parameter settings, statistics, and other information.
- Config commands - configures features and options of the switch.

Distance Vector Multicast Routing Protocol (DVMRP) commands

config router dvmrp adminmode

This command enables or disables the administrative mode of DVMRP in the router. IGMP must be enabled before DVMRP can be enabled.

Syntax:

```
config router dvmrp adminmode enable/disable
```

Default:
disable

config router dvmrp interface metric

Use this command to configure the DVMRP metric for an interface. This value is used in DVMRP messages as the cost to reach this network.

Syntax:

```
config router dvmrp interface metric port metric
```

where *metric* is 1 through 63.

Default:
1

config router dvmrp interface mode

This command enables or disables the administrative mode of DVMRP on the specified interface.

Syntax:

```
config router dvmrp interface mode port enable/disable
```

Default:
disable

show router dvmrp info

Use this command to display system-wide information for DVMRP.

Syntax:

```
show router dvmrp info
```

Return values:

Admin Mode Indicates whether DVMRP is enabled or disabled.

The following fields are only displayed if DVMRP is enabled.

Version String
Displays the version of DVMRP being used.

Number of Routes
Shows the number of routes in the DVMRP routing table.

Reachable Routes
Indicates the number of entries in the routing table with non-infinite metrics.

The following fields are displayed for each interface.

Port Indicates the port of this interface.

Interface Mode
The mode of this interface. Possible values are enabled and disabled.

Protocol State
Displays the current state of DVMRP on this interface. Possible values are operational or non-operational.

show router dvmrp interfaceinfo

Use this command to display DVMRP information for the specified interface.

Syntax:

```
show router dvmrp interfaceinfo port
```

Return values:

Interface Mode
Indicates whether DVMRP is enabled or disabled on the specified interface.

Interface Metric
Used to calculate distance vectors for the selected interface.

The following fields are only displayed if DVMRP is operational on this interface.

Local Address
The IP address used as a source address in packets sent from the selected interface.

Generation ID
The Generation ID used by the router for the selected interface. This value is reset every time an interface is restarted and is placed in prune messages. A change in Generation ID informs neighbor routers that any previous information about this router should be discarded.

Received Bad Packets
The number of invalid packets received on the selected interface.

Received Bad Routes
The number of invalid routes received on the selected interface.

Sent Routes
The number of routes that have been sent on the selected interface.

show router dvmrp neighborinfo

Use this command to display the neighbor information for DVMRP.

Syntax:

```
show router dvmrp neighborinfo
```

Return values:

Neighbor Interface Index
Displays the value of the interface used to reach the neighbor.

Neighbor IP Address
The IP address of the DVMRP neighbor whose information is displayed.

State
The state of the neighboring router. Possible values for this field are active or down.

Neighbor Up Time
Shows the time since this neighboring router was learned.

Neighbor Expiry Time
The time remaining before the neighbor ages out. This field is not applicable if the State is down.

Received Bad Packets
The number of invalid packets received from the neighbor on the selected interface.

Received Bad Routes
The number of invalid routes received from the specified neighbor on the selected interface.

Major Version
The DVMRP Major Version for the specified neighbor on the selected interface.

Minor Version
The DVMRP Minor Version for the specified neighbor on the selected interface.

Capabilities
The DVMRP capabilities for the specified neighbor on the selected interface.

show router dvmrp nexthopinfo

Use this command to display the next hop information on outgoing interfaces for routing multicast datagrams.

Syntax:

```
show router dvmrp nexthopinfo
```

Return values:

Next Hop Source
Displays the sources for which this entry specifies a next hop on an outgoing interface.

Next Hop Mask
Indicates the IP mask for the sources for which this entry specifies a next hop on an outgoing interface.

Interface
Shows the interface, in port format, for the outgoing interface for this next hop.

Type
States whether the network is a leaf or a branch.

show router dvmrp pruneinfo

Use this command to display the table listing the router upstream prune information.

Syntax:

```
show router dvmrp pruneinfo
```

Return values:

Group IP
Identifies the multicast address that is pruned.

Source IP
Displays the IP address of the source that has pruned.

Source Mask
Shows the network mask for the prune source. If the network mask is not all ‘1s, then both the prune source and the prune mask must match.

Expiry Time (secs)
Indicates the expiry time in seconds. This is the time remaining for this prune to age out.

show router dvmrp routeinfo

Use this command to display the multicast routing information for DVMRP.

Syntax:

```
show router dvmrp routeinfo
```

Return values:

Source IP Address
The IP address used with the source mask to identify the source network for this table entry.

Source Mask
Displays the IP mask used with the source IP address.

Upstream Neighbor
The IP address of the upstream neighbor which is the source for the packets for a specified multicast address.

Interface
Shows the interface used to receive the packets sent by the sources.

Metric
Displays the distance, in hops, to the source subnet. This field has a different meaning than the Interface Metric field.

Expiry Time (sec)
Indicates the expiry time in seconds. This is the time remaining before this entry will age out.

Up Time (secs)
Displays the time, in seconds, when a specified route was learned.

Internet Group Management Protocol (IGMP) commands

config router igmp adminmode

This command enables or disables the administrative mode of IGMP in the router.

Syntax:

```
config router igmp adminmode enable/disable
```

Default:
disable

config router igmp interface lastmemqrycnt

This command sets the number of queries to be sent upon receiving a leave group report.

Syntax:

```
config router igmp interface lastmemqrycnt port count
```

where *count* is an integer 1 through 20.

Default:
2

config router igmp interface lastmemqryint

Use this command to enter the last member query interval in tenths of a second. This is the maximum response time to be inserted into group-specific queries sent in response to leave group messages, and it is also the amount of time between group-specific query messages. This value is not used for IGMP version 1e.

Syntax:

```
config router igmp interface lastmemqryint port interval
```

where *interval* is 0 through 255.

Default:
10 tenths of a second (1 second)

config router igmp interface maxresptime

Use this command to configure the maximum response time interval for the specified interface, which is the maximum query response time advertised in IGMP v2 queries on this interface. The maximum response time is 0 to 255 tenths of a second.

Syntax:

```
config router igmp interface maxresptime port interval
```

where *interval* is 0 through 255.

Default:
100 tenths of a second (10 seconds)

config router igmp interface mode

This command enables or disables the administrative mode of IGMP on an interface in the router. IGMP will not be activated on an interface while IGMP Snooping is enabled on the interface.

Syntax:

```
config router igmp interface mode port enable/disable
```

Default:
disable

config router igmp interface queryinterval

Use this command to configure the query interval for the specified interface. This is the frequency at which IGMP Host-Query packets are transmitted on this interface.

Syntax:

```
config router igmp interface queryinterval port seconds
```

where `seconds` is 1 through 3600, in seconds.

Default:
125 seconds

config router igmp interface robustness

Use this command to configure the robustness of the interface. The robustness is the tuning for the expected packet loss on a subnet. Robustness should be increased if loss on the subnet is expected.

Syntax:

```
config router igmp interface robustness port robustvalue
```

where `robustvalue` is 1 through 255.

Default:
2

config router igmp interface startupqrycnt

This command sets the number of queries sent out on startup, separated by the startup query interval.

Syntax:

```
config router igmp interface startupqrycnt port count
```

where `count` is 1 through 20.

Default:
2

config router igmp interface startupqryint

This command sets the interval between queries sent by a querier on startup.

Syntax:

```
config router igmp interface startupqryint port interval
```

where *interval* is 1 through 300, in seconds.

Default:
31 seconds

config router igmp interface version

Use this command to configure the version of IGMP supported for this interface.

Syntax:
```
config router igmp interface version port version
```

where *version* is 1 or 2.

Default:
2

show router igmp info

Use this command to display system-wide IGMP information.

Syntax:
```
show router igmp info
```

Return values:

IGMP Admin Mode
Displays the administrative status of IGMP.

Port The interface whose information is displayed on this line.

Interface Mode
Indicates whether IGMP is enabled or disabled on the interface.

Protocol State
The current state of IGMP on this interface. Possible values are Operational or Non-Operational.

show router igmp interface detail

Use this command to display information about the registered multicast groups on the specified interface.

Syntax:
```
show router igmp interface detail port
```

Return values:

Multicast IP Address
Displays the Multicast IP address whose info is displayed.

Last Reporter Indicates the IP address of the source of the last membership report received for the specified multicast group address on this interface.

Up Time Shows the time elapsed since the entry was created for the specified multicast group address on this interface.

Expiry Time Displays the amount of time remaining to remove this entry before it is aged out.

Version 1 Host Timer
Represents the time remaining until the local router will assume that there are no longer any IGMP v1 multicast members on the IP subnet that is attached to this interface.

show router igmp interface info

Use this command to display IGMP information for the specified interface.

Syntax:

```
show router igmp interface info port
```

Return values:

Port Indicates the identifying port of the interface.

IGMP Admin Mode
Displays the administrative status of IGMP for the switch.

Interface Mode
Shows whether IGMP is enabled or disabled on the interface.

IGMP Version
Indicates the version of IGMP configured on this interface.

Query Interval
Represents the frequency at which IGMP Host-Query packets are transmitted on this interface.

Query Max Response Time
The maximum query response time advertised in IGMP v2 queries on this interface in tenths of a second.

Robustness Displays the tuning for the expected packet loss on a subnet. If a subnet is at risk of loss, the Robustness variable may be increased for that interface to compensate.

Startup Query Interval
The number of seconds between the transmission of startup queries on the selected interface.

Startup Query Count
The number of queries sent out on startup separated by the startup query interval.

Last Member Query Interval
The maximum response time to be inserted into group-specific queries sent in response to leave group messages. Also indicates the amount of time between group-specific query messages. This value is not used for IGMP v1.

Last Member Query Count
The number of group-specific queries to be sent upon receiving a leave group report.

show router igmp interface membership

Use this command to display the list of interfaces that have registered in the multicast group.

Syntax:

```
show router igmp interface membership multiipaddr
```

where *multiipaddr* is the multicast group IP address

Return values:

Port
The interface participating in the multicast group.

Interface IP
The IP address of the interface participating in the multicast group.

State
Indicates whether the interface is in querier mode or non-querier mode.

show router igmp interface stats

Use this command to display the IGMP statistical information for the specified interface. These statistics are only displayed when IGMP is enabled for the interface.

Syntax:

```
show router igmp interface stats port
```

Return values:

Querier Status
Indicates whether the selected interface is in querier or non-querier mode.

Querier IP Address
Displays the IP address of the IGMP querier on the IP subnet to which this interface is attached.

Querier Up Time
Indicates the time in seconds since the interface querier was last changed.

Querier Expiry Time
Displays the amount of time remaining before the Other Querier Present Timer expires. If the local system is the querier, the value of this object is zero.

Wrong Version Queries
Indicates the number of queries received whose IGMP version does not match the IGMP version of the interface over the lifetime of the entry. IGMP requires that all routers on a LAN be configured to run the same version of IGMP. Therefore, a configuration error is indicated if any queries are received with the wrong version number.

Number of Joins
The number of times a separate group membership has been added to this interface; that is, the number of times an entry for this interface has been added to the cache table. This gives an indication of the amount of IGMP activity on the interface.

Number of Groups
The current number of membership entries for this interface in the cache table.

show router igmp interface table

Use this command to display registered multicast groups on the interface.

Syntax:

```
show router igmp interface table port
```

Return values:

IP Address Displays the IP address of the registered multicast group on this interface.

Subnet Mask Indicates the subnet mask of the registered multicast group on this interface.

Interface Mode
Shows whether IGMP is enabled or disabled on this interface.

The following fields are not displayed if the interface is not enabled.

Querier Status
Displays whether the interface has IGMP in querier mode or non-querier mode.

Groups The list of multicast groups registered on this interface.

Multicast (Mcast) commands

clear mcast mroute all

This command clears all the entries in the mroute table.

Syntax:

```
clear mcast mroute all
```

clear mcast mroute group

This command clears mroute table entries containing the specified *groupipaddr*.

Syntax:

```
clearmcast mcast mroute group groupipaddr
```

where *groupipaddr* is the group address is the group destination IP address of the multicast packets.

clear mcast mroute source

This command clears the mroute table entries containing the specified *sourceipaddr* or *sourceipaddr*, [*groupipaddr*] pair. The source address is the source IP address of the multicast packets. The group address is the group destination IP address of the multicast packet.

Syntax:

```
clear mcast mroute source sourceipaddr [groupipaddr]
```

where

- *sourceipaddr* is the source IP address of the multicast packets.
- *groupipaddr* is the group destination IP address of the multicast packet.

config router mcast adminmode

This command enables or disables the administrative mode of the IP multicast forwarder. For multicast routing to become operational, IGMP must be currently enabled. An error message will be displayed if you enable multicast routing while IGMP is disabled. However, the IP multicast mode configuration is stored in the multicast configuration file and is automatically enabled once IGMP is enabled.

Syntax:

```
config router mcast adminmode enable/disable
```

Default:
disable

config router mcast boundary add

This command adds an administratively scoped IP multicast boundary specified by *ipaddr* and *mask*. The Multicast data packets within this range will not be forwarded. The *port* parameter indicates the interface for which this boundary limit is to be applied.

Syntax:

```
config router mcast boundary add ipaddr mask port
```

config router mcast boundary delete

This command deletes a administratively scoped IP multicast boundary specified by *ipaddr* and *mask*. The Multicast data packets within this range will not be forwarded. The *port* parameter indicates the interface for which this boundary limit is to be applied.

Syntax:

```
config router mcast boundary delete ipaddr mask port
```

config router mcast mdebug mrinforun

This command queries the neighbor information of a multicast-capable router specified by [ipaddr]. The default value is the IP address of the system at which the command is issued. The mrinforun command can take up to 2 minutes to complete. Only one mrinforun command may be in process at a time. The results of this command will be available in the results bufferpool which can be displayed by using **show router mcast mdebug mrinforun**.

Syntax:

```
config router mcast mdebug mrinforun [ipaddr]
```

config router mcast mdebug mstatrun

This command finds the packet rate and loss information path from a source to a receiver (unicast router id of the host running mstatrun). The results of this command will be available in the results bufferpool which can be displayed by using **show router mcast mdebug mrstatrun**. If a debug command is already in progress, a message is displayed and the new request fails. The *source* is the IP address of the remote multicast-capable source. The [receiveripaddr] is the IP address of the receiver. The default value is the IP address of the system at which the command is issued. The [groupipaddr] is the multicast address of the group to be displayed.

Syntax:

```
config router mcast mdebug mstatrun sourceipaddr [groupipaddr]
[receiveripaddr]
```

config router mcast mdebug mtraceadminmode

This command enables or disables the processing capability of mtracerun query on this router. If the mode is enable, mtracerun queries received by the router are processed and forwarded appropriately. If the mode is disable, this router does not respond to the mtracerun queries it receives from other router devices.

Syntax:

```
config router mcast mdebug mtraceadminmode enable/disable
```

config router mcast mdebug mtracerun

This command finds the multicast path from a source to a receiver (unicast router ID of the host running mtrace). A trace query is passed hop-by-hop along the reverse path from the receiver to the source, collecting hop addresses, packet counts, and routing error conditions along the path, and then the response is returned to the requestor. The results of this command will be available in the results buffer pool which can be displayed by using **show router mcast mdebug mtracerun**. If a debug command is already in execution, a message is displayed and the new request fails.

Syntax:

```
config router mcast mdebug mtracerun sourceipaddr [groupipaddr]
[receiveripaddr]
```

where

- *sourceipaddr* is the IP address of the remote multicast-capable source.
- *receiveripaddr* is the IP address of the receiver. The default value is the IP address of the system at which the command is issued.
- *groupipaddr* is the multicast address of the group to be displayed.

config router mcast staticroute add

This command creates a static route used to perform RPF checking in multicast packet forwarding. The combination of the *sourceipaddr* and the *mask* fields specifies the network IP address of the multicast packet source. The *groupipaddr* is the IP address of the next hop toward the source. The *metric* is the cost of the route entry for comparison with other routes to the source network in the range of 0 and 255. The *port* is the incoming interface number used for RPF checking for multicast packets matching this multicast static route entry.

Syntax:

```
config router mcast staticroute add sourceipaddr mask groupipaddr metric
port
```

config router mcast staticroute delete

This command adds or deletes a static route in the static multicast table. The *sourceipaddr* is the IP address of the multicast packet source.

Syntax:

```
config router mcast staticroute delete sourceipaddr
```

config router mcast ttlthreshold

This command applies the given *ttlthreshold* to the routing interface *port*. The *ttlthreshold* is the TTL threshold to be applied to the multicast packets forwarded from the interface specified by *port*. It has a range from 0 through 255.

Syntax:

```
config router mcast ttlthreshold port ttlthreshold
```

Default:
0

show router mcast boundary

Use this command to display the configured, administratively scoped boundaries for the interface specified by *port*. If `all` is selected, the configured, administratively scoped boundaries for all interfaces will be displayed.

Syntax:

```
show router mcast boundary port/listofports/all
```

Return values:

Syntax:

Port The interface whose information is displayed.

Group Ip The destination group IP address whose multicast routes will be displayed or cleared.

Mask The group IP address mask.

show router mcast info

Use this command to display system-wide multicast information.

Syntax:

```
show router mcast info
```

Return values:

Admin Mode Displays the administrative status of multicast forwarding.

Protocol State
Indicates the current state of the multicast forwarding module. Possible values are Operational or Non-Operational.

Table Maximum Entry Count
The maximum number of entries in the IP multicast routing table.

Number Of Packets For Which Source Not Found
The number of multicast packets expected to be routed but failing the Reverse Path Forwarding (RPF) check.

Number Of Packets For Which Group Not Found
The number of multicast packets expected to be routed but for which no multicast route was found.

Protocol Indicates the Multicast protocol presently activated on the router.

Table Entry Count
The number of entries in the Multicast route table.

Table Highest Entry Count
Displays the highest entry count that has been present in the Multicast table.

show router mcast interfaceinfo

Use this command to display the multicast information for the specified interface.

Syntax:

```
show router mcast interfaceinfo port
```

Return values:

Port Indicates the port of the interface.

TTL Displays the time-to-live value for this interface.

show router mcast mdebug mrinforun

Use this command to display the neighbor information of a multicast-capable router from the results buffer pool of the router subsequent to the execution/completion of a **config router mcast mdebug mrinforun** command. The results will be available in the bufferpool after a maximum of two minutes after the completion of the command. A subsequently issued mrinforun will overwrite the contents of the buffer pool with fresh results.

Syntax:

```
show router mcast mdebug mrinforun
```

Return values:

Router Interface
The IP address of this neighbor

Neighbor The neighbor associated with the router interface

Metric The metric value associated with this neighbor

TTL The TTL threshold associated with this neighbor

Flags Status of the neighbor

show router mcast mdebug mstatrun

Use this command to display packet rate and loss information from the results buffer pool, subsequent to the execution/completion of a **config router mcast mdebug mstatrun** command. Within two minutes of the completion of the mstatrun command, the results will be available in the buffer pool. The next mstatrun command would overwrite the buffer pool with fresh results.

Syntax:

```
show router mcast mdebug mstatrun
```

show router mcast mdebug mtracerun

Use this command to display multicast trace path information from the results bufferpool of the router, subsequent to the execution/completion of a **config router mcast mdebug mtracerun** command. The results will be available in the bufferpool within 2 minutes. Another mtracerun command will overwrite the results in the bufferpool.

Syntax:

```
show router mcast mdebug mtracerun
```

Return values:

Hops Away From Destination
The number of intermediate routers between the source and the destination.

Intermediate Router Address
The IP address of the intermediate router in the path being traced between source and destination for the hop number in the previous field.

Mcast Protocol In Use
The multicast routing protocol used for the out interface of the specified intermediate router.

TTL Threshold
The Time-To-Live threshold of the out interface on the specified intermediate router.

Time Elapsed Between Hops (msecs)
The time between arrival at one intermediate router to the arrival at the next.

show router mcast mroute detailed all

Use this command to display the details of the multicast table.

Syntax:

```
show router mcast mroute detailed all
```

Return values:

Source IP Addr
The IP address of the multicast packet source to be combined with the group IP address to fully identify a single route whose Mroute table entry will be displayed.

Group IP Addr
The destination group IP address whose multicast routes will be displayed.

Expiry Time The time in seconds before this entry will age out and be removed from the table.

Up Time The time since the entry was created, in seconds.

RPF Neighbor
The IP address of the Reverse Path Forwarding (RPF) neighbor.

Flags The flags associated with this entry. Possible values are RPT or SPT. For other protocols “-----” is displayed.

show router mcast mroute detailed group

Use this command to display the multicast detailed information for a specific group.

Syntax:

```
show router mcast mroute detailed group groupipaddr
```

Return values:

Source IP Addr
The IP address of the multicast packet source to be combined with the group IP address to fully identify a single route whose Mroute table entry will be displayed.

Group IP Addr
The destination group IP address whose multicast routes will be displayed.

Expiry Time The time in seconds before this entry will age out and be removed from the table.

Up Time The time since the entry was created, in seconds.

RPF Neighbor
The IP address of the Reverse Path Forwarding (RPF) neighbor.

Flags The flags associated with this entry. Possible values are RPT or SPT. For other protocols “-----” is displayed.

show router mcast mroute detailed source

Use this command to display Multicast information for a specific source.

Syntax:

```
show router mcast mroute detailed source sourceipaddr [groupipaddr]
```

Return values:

Source IP Addr
The IP address of the multicast packet source to be combined with the group IP address to fully identify a single route whose Mroute table entry will be displayed.

Group IP Addr
The destination group IP address whose multicast routes will be displayed.

Expiry Time The time in seconds before this entry will age out and be removed from the table.

Up Time The time since the entry was created, in seconds.

RPF Neighbor
The IP address of the Reverse Path Forwarding (RPF) neighbor.

Flags The flags associated with this entry. Possible values are RPT or SPT. For other protocols “-----” is displayed.

show router mcast mroute summary all

Use this command to display configuration settings such as flags, timer settings, incoming, and outgoing interfaces, RPF neighboring routers, and expiration times of all the entries in the multicast mroute table.

Syntax:

```
show router mcast mroute detailed source sourceipaddr [groupipaddr]
```

Return values:

Source IP Addr
The IP address of the multicast data source.

Group IP Addr
The IP address of the destination of the multicast packet.

Protocol The Multicast routing protocol which created this entry. Possible values are PIM-SM, DVMRP, and PIM-DM.

Incoming Interface
The interface on which the packet for this source/group arrives.

Outgoing Interface List
The list of outgoing interfaces on which multicast packets for this source/group are forwarded.

show router mcast mroute summary group

Use this command to display multicast configuration settings such as flags, timer settings, incoming and outgoing interfaces, RPF neighboring routers, and expiration times of all the entries in the multicast mroute table containing the given *groupipaddr*.

Syntax:

```
show router mcast mroute summary group groupipaddr
```

Return values:

Source IP Addr
The IP address of the multicast data source.

Group IP Addr
The IP address of the destination of the multicast packet.

Protocol The Multicast routing protocol which created this entry. Possible values are PIM-SM, DVMRP, and PIM-DM.

Incoming Interface
The interface on which packets for this source/group arrive.

Outgoing Interface List
The list of outgoing interfaces on which multicast packets for this source/group are forwarded.

show router mcast mroute summary source

Use this command to display the multicast configuration settings such as flags, timer settings, incoming and outgoing interfaces, RPF neighboring routers, and expiration times of all the entries in the multicast mroute table containing the given *sourceipaddr* or *sourceipaddr*/[*groupipaddr*] pair.

Syntax:

```
show router mcast mroute summary source sourceipaddr [groupipaddr]
```

Return values:

Source IP Addr
The IP address of the multicast data source.

Group IP Addr
The IP address of the destination of the multicast packet.

Protocol The multicast routing protocol which created this entry. Possible values are PIM-SM, DVMRP, and PIM-DM.

Incoming Interface
The interface on which packets for this source/group arrive.

Outgoing Interface List
The list of outgoing interfaces on which multicast packets for this source/group are forwarded.

show router mcast staticroute all

Use this command to display all the static routes configured in the static mcast table.

Syntax:

```
show router mcast staticroute all
```

Return values:

Source IP Address
The IP address of the multicast packet source.

Source Mask The mask applied to the IP address of the multicast packet source.

RFP Address The IP address to be used as RPF for the given source and mask.

Metric The link-state cost of the path to the multicast source. This metric can be changed for a configured route.

Port The incoming interface number whose IP address is used as RPF for the given source and mask is expected.

show router mcast staticroute source

This command shows the static route associated with the particular *sourceipaddr*.

Syntax:

```
show router mcast staticroute source sourceipaddr
```

Return values:

Source Address
The IP address of the multicast packet source.

Source Mask The mask applied to the IP address of the multicast packet source.

RPF Address The IP address to be used as RPF for the given source and mask.

Metric The link-state cost of the path to the multicast source. This metric can be changed for a configured route.

Port The incoming interface number whose IP address is used as RPF for the given source and mask is expected.

Protocol Independent Multicast - Dense Mode (PIM-DM) commands

config router pimdm adminmode

This command enables or disables the administrative mode of PIM-DM in the router. IGMP must be enabled before PIM-DM can be enabled.

Syntax:

```
config router pimdm adminmode enable/disable
```

Default:
disable

config router pimdm interface hellointerval

Use this command to configure the transmission frequency of hello messages between PIM-DM enabled neighbors.

Syntax:
```
config router pimdm interface hellointerval port seconds
```

where *seconds* is 10 through 3600.

config router pimdm interface mode

This command enables or disables the administrative mode of PIM-DM on an interface.

Syntax:
```
config router pimdm interface mode port enable/disable
```

Default:
disable

show router pimdm info

Use this command to display system-wide information for PIM-DM.

Syntax:
```
show router pimdm info
```

Return values:

PIM-DM Admin Mode
Indicates whether PIM-DM is enabled or disabled. IGMP must be enabled before PIM-DM can be enabled.

Port The interface whose information is displayed on this line.

Interface Mode
Shows whether PIM-DM is enabled or disabled on this interface.

State Displays the current state of PIM-DM on this interface. Possible values are Operational or Non-Operational.

show router pimdm interface info

Use this command to display the interface information for PIM-DM on the specified interface.

Syntax:
```
show router pimdm interface info port
```

Default:
30 seconds

Return values:

Interface Mode
Indicates whether PIM-DM is enabled or disabled on the specified interface.

PIM-DM Interface Hello Interval
Displays the frequency at which PIM hello messages are transmitted on this interface.

show router pimdm interface stats

Use this command to display the statistical information for PIM-DM on the specified interface.

Syntax:
`show router pimdm interface stats` *port*/*listofports*/`all`

Default:
all

Return values:

Interface The identifying port of the interface.

IP Address This field indicates the IP address that represents the PIM-DM interface.

Neighbor Count
This field displays the number of neighbors on the PIM-DM interface.

Hello Interval
This field indicates the interval, in seconds, between two hello messages sent from the selected interface.

Designated Router
This indicates the IP address of the designated router for this interface. For point-to-point interfaces, this will be 0.0.0.0

show router pimdm neighbor

Use this command to display the neighbor information for PIM-DM on the specified interface.

Syntax:
`show router pimdm neighbor` *port*/*listofports*/`all`

Default:
all

Return values:

Neighbor IP Address
The IP address of the neighbor on the interface.

Interface The interface whose information is displayed.

Up Time The time since this PIM neighbor last became a neighbor of the local router.

Expiry Time The minimum time remaining before this PIM neighbor will be aged out.

Protocol Independent Multicast - Sparse Mode (PIM-SM) commands

config router pimsm adminmode

This command enables or disables the administrative mode of PIM-SM multicast routing on the router. IGMP must be enabled before PIM-SM can be enabled.

Syntax:

```
config router pimsm adminmode enable/disable
```

Default:
disable

config router pimsm datathreshrate

This command is used to configure the data threshold rate for the PIM-SM router.

Syntax:

```
config router pimsm datathreshrate rate
```

where *rate* is 0 through 2000, in kilobytes per second.

Default:
50 kilobytes per second

config router pimsm interface cbsrpreference

Use this command to configure the preference value for the local interface as a CBSR.

Syntax:

```
config router pimsm interface cbsrpreference port preference
```

where *preference* is -1 through 255, in kilobytes per second. The value of -1 is used to indicate that the local interface is NOT a CSBR interface.

Default:
0

config router pimsm interface hellointerval

Use this command to configure the transmission frequency of hello messages between PIM enabled neighbors. This field has a range of 10 through 3600 seconds.

Syntax:

```
config router pimsm interface hellointerval port seconds
```

where *seconds* is 10 through 3600.

Default:
30 seconds

config router pimsm interface mode

This command enables or disables the administrative mode of PIM-SM multicast routing on an interface.

Syntax:

```
config router pimsm interface mode port enable/disable
```

Default:
disable

config router pimsm joinpruneintvl

This command is used to configure the global join/prune interval for the PIM-SM router. The join/prune interval is specified in seconds with a range of 10 through 3600.

Syntax:

```
config router pimsm joinpruneintvl seconds
```

where *seconds* is 10 through 3600.

Default:
60 seconds

config router pimsm regthreshrate

This command is used to configure the threshold rate for the RP router to switch to the shortest path.

Syntax:

```
config router pimsm regthreshrate rate
```

where rate is 0 through 2000.

Default:
50 kilobytes per second

show router pimsm candrptable

Use this command to display the IP multicast groups for which the local router is to advertise itself as a Candidate-RP when the value of hold time is non-zero.

Syntax:

```
show router pimsm candrptable
```

Return values:

Group Address
The IP multicast group address.

Group Mask The multicast group address subnet mask.

Address The unicast address of the interface that will be advertised as a Candidate-RP.

show router pimsm componenttable

Use this command to display the table containing objects specific to a PIM domain. One row exists for each domain to which the router is connected.

Syntax:

```
show router pimsm componenttable
```

Return values:

Component Index
A number which uniquely identifies the component.

Component BSR Address
The IP address of the bootstrap router (BSR) for the local PIM region.

Component BSR Expiry Time
The minimum time remaining before the BSR in the local domain will be declared down.

Component CRP Hold Time
The hold time of the component when it is a candidate for Rendezvous Point in the local domain.

show router pimsm info

Use this command to display system-wide information for PIM-SM.

Syntax:

```
show router pimsm info
```

Return values:

PIM-SM Admin Mode
Whether PIM-SM is enabled or disabled. IGMP must be enabled before enabling PIM-SM.

Join/Prune Interval (secs)
The interval between the transmission of PIM-SM Join/Prune messages.

Data Threshold Rate (Kbps)
The minimum source data rate in Kbps above which the last-hop router will switch to a source-specific shortest path tree.

Register Threshold Rate (Kbps)
The minimum source data rate in Kbps above which the Rendezvous Point router will switch to a source-specific shortest path tree.

Port Routing interfaces in port format.

Interface Mode
Whether PIM-SM is enabled or disabled on the interface.

Protocol State
Whether the PIM-SM protocol on the interface is Operational or Non-Operational.

show router pimsm interface info

Use this command to display interface information for PIM-SM on the specified interface.

Syntax:

```
show router pimsm interface info port
```

Return values:

Port The specified interface in port format.

IP Address The IP address of the specified interface.

Subnet Mask The subnet mask for the IP address of the PIM interface.

Interface Mode
Indicates whether PIM-SM is enabled or disabled on the specified interface. Default is disabled.

Hello Interval
The time in seconds between the transmission of PIM Hello messages on this interface. Default is 30 seconds.

CBSR Preference
The preference value for the local interface as a candidate bootstrap router (CBSR).

show router pimsm interface stats

Use this command to display the statistical information for PIM-SM on the specified interface.

Syntax:

```
show router pimsm interface stats port/listofports/all
```

Return values:

Port The interface whose information is displayed on this line.

IP Address The IP address of the PIM-SM interface.

Subnet Mask The subnet mask of the specified PIM-SM interface.

Designated Router
The IP address of the Designated Router for this interface. For point-to-point interfaces this object has a value of 0.0.0.0

Neighbor Count
The count of neighbors on the PIM-SM interface.

show router pimsm neighbor

Use this command to display the neighbor information for PIM-SM on the specified interface.

Syntax:

```
show router pimsm neighbor port/listofports/all
```

Default:
all

Return values:

Port The interface where the neighbor was discovered.

IP Address The IP address of the neighbor.

Up Time The time since this neighbor became active on this interface.

Expiry Time The minimum time remaining before this PIM neighbor will be aged out.

show router pimsm rpsettable

Use this command to display the PIM information for candidate Rendezvous Points (RPs) for all IP multicast groups or for the specific *groupaddress groupmask* provided in the command. The information in the table is displayed for each IP multicast group.

Syntax:

```
show router pimsm rpsettable all/groupaddress groupmask
```

Return values:

Group Address
The IP multicast group address.

Group Mask
The multicast group address subnet mask.

Address
The IP address of the Candidate-RP.

Hold Time
The hold time of a Candidate-RP. If the local router is not the BSR, this value is 0.

Expiry Time Component
The minimum time remaining before the bootstrap router in the local domain will be declared.

Component Index
A number which uniquely identifies the component. Each protocol instance connected to a separate domain should have a different index value.

Appendix A. Run-time switching software default settings

The following table contains the default settings for the run-time switching software variables. Variables are separated by category and further by sub-headings (listed alphabetically within category). The Command column lists the CLI command used to change the default setting.

Table 3. Default settings for run-time switching software variables

Heading	Sub-heading	Variable	Default value	Command
Multicast				
	Distance Vector Multicast Routing Protocol (DVMRP)			
		Mode	Disable	config router dvmrp adminmode
		Interface Metric	1	config router dvmrp interface metric
		Interface Mode	Disable	config router dvmrp interface mode
	Internet Group Management Protocol (IGMP)			
		Mode	Disable	config router igmp adminmode
		Interface Mode	Disable	config router igmp interface mode
		Interface Version	2	config router igmp interface version
		Last Member Maximum Response Time Interval (inserted in response to leave group messages)	10 tenths of a second	config router igmp interface lastmemqryint
		Number of Queries (sent upon receiving leave group)	2	config router igmp interface lastmemqrycnt
		Interface Maximum Response Time	100 tenths of a second	config router igmp interface maxresptime
		Interface Query Interval	125 seconds	config router igmp interface queryinterval
		Robustness	2	config router igmp interface robustness
		Startup Query Count	2	config router igmp interface startupqrycnt
		Startup Query Interval	31 seconds	config router igmp interface startupqryint
	MCAST			
		Mode	Disable	config router mcast adminmode
		Time to Live Threshold	0	config router mcast ttlthreshold

Table 3. Default settings for run-time switching software variables (continued)

Heading	Sub-heading	Variable	Default value	Command
	Protocol Independent Multicast - Dense Mode (pim-dm)			
		Interface Mode	Disable	config router pimdm interface mode
		Interface Hello Interval	30 seconds	config router pimdm interface hellointerval
		Mode	Disable	config router pimdm adminmode
	Protocol Independent Multicast - Sparse Mode (pim-sm)			
		CBSR Preference	0	config router pimsm interface cbsrpreference
		Data Threshold Rate	50 kilobytes/second	config router pimsm datathreshrate
		Global Join/Prune Interval	60 seconds	config router pimsm joinpruneintvl
		Interface Hello Interval	30 seconds	config router pimsm interface hellointerval
		Interface Mode	Disable	config router pimsm interface mode
		Mode	Disable	config router pimsm adminmode
		Registration Threshold Rate	50 kilobytes/second	config router pimsm regthreshrate
Quality of Service				
	ACL			
		ACL Rule	Deny	config acl rule create
	Bandwidth Provisioning			
		Bandwidth Allocation Maximum	100 mbps	config bwprovisioning bwallocation maximum
		Traffic Class Weight	1	config bwprovisioning trafficclass weight
Routing				
	Address Resolution Protocol (ARP)			
		Agetime	1200 seconds	config arp agetime
		Cache Size	3072	config arp cachesize
		Response time	1 second	config arp resptime
		# of Retries	4	config arp retries
	Internet Protocol (IP)			

Table 3. Default settings for run-time switching software variables (continued)

Heading	Sub-heading	Variable	Default value	Command
		Interface Netdir Broadcast	Enable	config ip interface netdirbcast
		Interface Encapsulation	Ethernet	config interface encaps
		Interface Maximum Transmission Unit	1500	config interface mtu
		Interface Forwarding	Enable	config ip forwarding
	Open Shortest Path First (OSPF)			
	Configuration/Summary			
		ASBR	Disable	config router ospf asbr
		Cost	10	config router ospf interface cost
		IfTransit Delay	1 second	config router ospf interface iftransitdelay
		Interface Mode	Disable	config router ospf interface mode
		Interval Dead	40 seconds	config router ospf interface dead
		Interval Hello	10 seconds	config router ospf interface hello
		LSDB limit	-1	config router ospf extlsdblimit
		Mode	Disable	config router ospf adminmode
		Overflow interval	0 seconds	config router ospf exoverflowinterval
		Preference	Intra - 8 Inter - 10 Type-1 - 13 Type-2 - 150	
		Priority	1	config router ospf interface priority
		Trapflags	Enable	config trapflags ospf
	OSPF Virtual Interface			
		Authentication Type Key	None. The default password key is not configured	config router ospf virtif authentication none
		Transmission Delay	1 second	config router ospf virtif transdelay
		Interval Dead	40 seconds	config router ospf virtif interval dead
		Hello interval	10 seconds	config router ospf virtif interval hello

Table 3. Default settings for run-time switching software variables (continued)

Heading	Sub-heading	Variable	Default value	Command
		Retransmission interval	5 seconds	config router ospf virtif interval retransmit
	BOOTP/DHCP Relay			
		Mode	Disable	config router bootpdhcprelay adminmode
		Circuit Option Mode	Disable	config router bootpdhcprelay circuitoptionmode
		Maximum Hop Count	4	config router bootpdhcprelay maxhopcount
		Minimum Wait Time	0 seconds	config router bootpdhcprelay minwaittime
		Server IP	0.0.0.0	config router bootpdhcprelay serverip
	Router (rtr) Discovery			
		Discovery Address	224.0.0.1	config rtr discovery address
		Mode	Enable	config rtr discovery adminmode
		Lifetime	3 * maxinterval	config rtr discovery lifetime
		Maximum Interval	600	config rtr discovery maxinterval
		Minimum Interval	0.75 * maxinterval	config rtr discovery mininterval
		Discovery Preference	0	config rtr discovery preference
	Router Route			
		Route Static Preference	60	config router route staticpreference
	Routing Information Protocol (RIP)			
		Autosummary	Enable	config router rip autosummary
		Host Route Acceptance	Enable	config router rip hostrouteaccept
		Interface Authentication Key	The default password key is an empty string	config router rip interface authentication simple
		Interface Authentication Type	None	config router rip interface authentication none
		Interface Version Receive	Both	config router rip interface version receive
		Interface Version Send	rip 1c	config router rip interface version send
		Interface Authentication Key	The default password key is an empty string	config router rip interface authentication simple
		Mode	Disable	config router rip adminmode

Table 3. Default settings for run-time switching software variables (continued)

Heading	Sub-heading	Variable	Default value	Command
		RIP Interface Default Metric	0	config router rip interface defaultmetric
		RIP Interface Mode	Disable	config router rip interface mode
		Route preference	15	config router rip preference
		Split Horizon	Simple	config router rip splithorizon
	Virtual Router Redundancy Protocol (VRRP)			
		Advertisement Value	1	config router vrrp interface advinterval
		Authentication Details	None	config router vrrp interface authdetails
		Interface Mode	Disable	config router vrrp interface adminmode
		Interface Preempt Mode	Enable	config router vrrp interface preemtpmode
		Interface Priority	100	config router vrrp interface priority
		Mode	Disable	config router vrrp adminmode
Security				
	IEEE 802.1X			
		Add users	All	config dot1x port users add
		Control Mode	Auto	config dot1x port controlmode
		Initialization	Disable	config dot1x port initialize
		Maximum # of requests	2	config dot1x port maxrequests
		Mode	Disable	config dot1x adminmode
		Port initialize	Disable	config dot1x port initialize
		Quiet Period	60 seconds	config dot1x port quietperiod
		Reauthentication Enabled	False	config dot1x port reauthenabled
		Reauthentication Period	3600 seconds	config dot1x port reauthperiod
		Reauthentication Sequence	Disable	config dot1x port reauthenticate
		Server Timeout	30 seconds	config dot1x port servertimeout
		Supplicant Time Out	30 seconds	config dot1x port supptimeout
		Transmit Period	30 seconds	config dot1x port transmitperiod

Table 3. Default settings for run-time switching software variables (continued)

Heading	Sub-heading	Variable	Default value	Command
	Remote Authentication Dial-in User Service (RADIUS)			
	Accounting			
		Accounting Server Port	1813	config radius accounting server port
		Mode	Disable	config radius accounting mode
	Configuration			
		Maximum Retransmits	4	config radius maxretransmits
		Timeout	5 seconds	config radius timeout
	Server			
		Server Port	1812	config radius accounting server port
	Secure Shell (SSH)			
		Mode	Disable	config ssh adminmode
		Protocol	Both (SSH1 and SSH2)	config ssh protocol
	Secure Socket Layer (SSL)			
		Secure port	443	config http secureport
		Secure Protocol	Both (SSL3 and TLS1)	config http secureprotocol
		Secure Server Mode	Disable	config http secureserver adminmode
Switching				
	VLAN			
		Accept frame	all	config vlan port acceptframe
		Broadcast Storm	Disable	config vlan bcaststorm
		Ingress filter	Disable	config vlan port ingressfilter
		Multicast Storm	Disable	config vlan mcaststorm
		Name	VLAN1	config vlan name
		Port priority	0	config vlan port priority
		Port VID	1	config vlan port pvid
	GARP			
		GARP GMRP administration	Disable	config garp gmrp adminmode
		GARP GMRP interface	Disable	config garp gmrp interfacemode
		GARP join timer	20 centiseconds	config garp jointimer
		GARP leave all timer	1000 centiseconds	config garp leavealltimer
		GARP leave timer	60 centiseconds	config garp leavetimer
	GVRP			
		GVRP administration	Disable	config garp gvrp adminmode

Table 3. Default settings for run-time switching software variables (continued)

Heading	Sub-heading	Variable	Default value	Command
		GVRP interface	Disable	config gvrp gmrp interfacemode
		GVRP join timer	20 centiseconds	config gvrp jointimer
		GVRP leave all timer	1000 centiseconds	config gvrp leavealltimer
		GVRP leave timer	60 centiseconds	config gvrp leavetimer
	IGMP Snooping			
		Group Membership Interval	260 seconds	config igmpsnooping groupmembershipinterval
		Interface	Disable	config igmpsnooping interfacemode
		Maximum response time	10 seconds	config igmpsnooping maxresponse
		MCRT Expiration Time	0 seconds	config igmpsnooping mcrtexpiretime
		Mode	Disable	config igmpsnooping adminmode
	Link Aggregation			
		LAG linktrap	Enable	config lag linktrap
	Spannng Tree Protocol (STP)			
	Bridge			
		Forward Delay	15 secs	config spanningtree bridge forwarddelay
		Hello Time	2 secs	config spanningtree bridge hellotime
		Max Age	6 secs	config spanningtree bridge maxage
		Priority	32768	config spanningtree bridge priority
	Configuration			
		Admin Mode	Disable	config spanningtree adminmode
		Configuration name	The base MAC address displayed using hexadecimal notation	config spanningtree configuration name
		Forced Version	IEEE 802.1D	config spanningtree forceversion
		Revision level	0	config spanningtree configuration revision
	CST			
		Edgeport	False	config spanningtree cst port edgeport
		Pathcost	Auto	config spanningtree cst port pathcost
		Priority	128	config spanningtree cst port priority

Table 3. Default settings for run-time switching software variables (continued)

Heading	Sub-heading	Variable	Default value	Command
	Port			
		Migration Check	Disable	config spanningtree port migrationcheck
		Port Mode	Disable	config spanningtree port mode
System				
		Auto log-out	10 min	
		Configuration update	Disable	
		Default gateway	0.0.0.0	
		IP address	10.90.90.9*x*, where *x* depends on the number of the bay into which you have installed the switch module.	
		Subnet mask	Class A Network - 255.0.0.0, Class B Network - 255.255.0.0, Class C Network - 255.255.255.0	
	Configuration			
		System Contact	Blank	config syscontact
		System Location	Blank	config syslocation
		System Name	Blank	config sysname
	Forwarding Database			
		Forwarding Database aging time	300 seconds	config forwardingdb agetime
	Port			
	Configuration			
		Auto Negotiation	Enable	config port autoneg
		Flow control	Disable	config port flowcontrol
		LACP mode	Disable	config port lacpmode
		Port Enable	Enable	config port adminmode
	Mirroring			
		Mirroring Mode	Disable	config mirroring mode
	Network Connectivity			
		Java enable status	Disable	config network javamode
		Web enable status	Enable	config network webmode
	SNMPcommunity			
		IP address	0.0.0.0	config snmpcommunity ipaddr
		IP Mask	0.0.0.0	config snmpcommunity ipmask

Table 3. Default settings for run-time switching software variables (continued)

Heading	Sub-heading	Variable	Default value	Command
		Mode	Default private and public communities are enabled by default. The four undefined communities are disabled by default	config snmpcommunity mode
		Type	Public/Private	config snmp community create
	Telnet			
		Max Number of Sessions	5	config telnet maxsessions
		Status	Enable	config telnet mode
		Ttimeout	5	config telnet timeout
	User Accounts			
		Password	Blank	config users passwd
		SNMPv3 Access Mode	Read/Write for admin, Read only for others	config users snmpv3 accessmode
		SNMPv3 Authentication	No authentication	config users snmpv3 authentication
		SNMPv3 Encryption	No encryption	config users snmpv3 encryption
	Transfer			
	Download			
		Transfer Download Datatype	Code	transfer download datatype
		Transfer Download IP Address	0.0.0.0	transfer download serverip
	Upload			
		Transfer Upload Datatype	Code	transfer upload datatype
		Transfer Upload IP Address	0.0.0.0	transfer upload serverip
	Trap Management			
		Authenticate Trapflags	Enable	config trapflags authentication
		Trapflags DVMRP	Enable	config trapflags dvmrp
		Trapflags Linkmode	Enable	config trapflags linkmode
		Trapflags Multiusers	Enable	config trapflags multiusers
		Trapflags OSPF	Enable	config trapflags ospf
		Trapflags PIM	Enable	config trapflags pim
		Trapflags STP	Enable	config trapflags stpmode

Appendix B. CLI Command Tree

This appendix presents the CLI command tree used with the IBM eserver BladeCenter T 4-Port Gb Ethernet Switch Module.

clear						
	config					
	dot1x	port	stats			
	igmpsnooping					
	lag					
	mcast	mroute	all			
			group			
			source			
	pass					
	radius	stats				
	stats	port				
		switch				
	transfer					
	traplog					
	vlan					
config						
	acl	create				
		delete				
		interface	add			
			remove			
		rule	action			
			create			
			delete			
			match	dstip		
				dstl4port	keyword	
					number	
				every		
				protocol	keyword	
					number	
				srcip		
				srcl4port	keyword	
					number	
	arp	agetime				
		cachesize				
		create				
		delete				
		resptime				

		retries				
	authentication	login	create			
			delete			
			set			
	bwprovisioning	bwallocation	create			
			delete			
			maxbandwidth			
		trafficclass	bwallocation			
			create			
			delete			
			port			
			vlan			
			weight			
	classofservice	802.1p mapping				
	dot1x	adminmode				
		defaultlogin				
		login				
		port	controlmode			
			initialize			
			maxrequests			
			quietperiod			
			reauthenabled			
			reauthenticate			
			reauthperiod			
			servertimeout			
			supptimeout			
			transmitperiod			
			users	add		
				remove		
	forwardingdb	agetime				
	garp	gmrp	adminmode			
			interfacemode			
		gvrp	adminmode			
			interfacemode			
		jointimer				
		leavealltimer				
		leavetimer				
	http	secureport				
		secureprotocol				
		secureserver	adminmode			
	igmpsnooping	adminmode				
		groupmembershipinterval				

		interfacemode				
		maxresponse				
		mcrtrexpiretime				
	interface	encaps				
	ip	forwarding				
		interface	create			
			delete			
			mtu			
			netdirbcast			
		vlan	routing	create		
				delete		
	lag	addport				
		adminmode				
		create				
		deletelag				
		deleteport				
		linktrap				
		name				
	loginsession	close				
	macfilter	adddest				
		create				
		deldest				
		remove				
	mirroring	create				
		delete				
		mode				
	network	javamode				
		webmode				
	port	adminmode				
		autoneg				
		flowcontrol				
		lacpmode				
		linktrap				
		physicalmode				
	prompt					
	protocol	create				
		delete				
		interface	add			
			remove			
		protocol	add			
			remove			
		vlan	add			

			remove			
	radius	accounting	mode			
			server	add		
				port		
				remove		
				secret		
		maxretransmit				
		server	add			
			msgauth			
			port			
			primary			
			remove			
			secret			
		timeout				
	router	bootpdhcprelay	adminmode			
			cidoptmode			
			maxhopcount			
			minwaittime			
			serverip			
		dvmrp	adminmode			
			interface	metric		
				mode		
		id				
		igmp	adminmode			
			interface	lastmemqrycnt		
				lastmemqryint		
				maxresptime		
				mode		
				queryinterval		
				robustness		
				startupqrycnt		
				startupqryint		
				version		
		mcast	adminmode			
			boundary	add		
				delete		
			mdebug	mrinforun		
				mstatrun		
				mtraceadminmode		
				mtracerun		
			staticroute	add		
				delete		

			ttlthreshold			
		ospf	1583compatibility			
			adminmode			
			area	authentication		
				range	create	
					delete	
				stub	create	
					delete	
					metric	type
						value
					summarylsa	
			asbr			
			exoverflowinterval			
			extlsdblimit			
			interface	areaid		
				authentication	encrypt	
					none	
					simple	
				cost		
				iftransitdelay		
				interval	dead	
					hello	
					retransmit	
				mode		
				priority		
			preference			
			virtif	authentication	encrypt	
					none	
					simple	
				create		
				delete		
				interval	dead	
					hello	
					retransmit	
				transdelay		
		pimdm	adminmode			
			interface	hellointerval		
				mode		
		pimsm	adminmode			
			datathreshrate			
			interface	cbsrpreference		
				hellointerval		

				mode		
			joinpruneintvl			
			regthreshrate			
		rip	adminmode			
			autosummary			
			hostrouteaccept			
			interface	authentication	encrypt	
					none	
					simple	
				defaultmetric		
				mode		
				version	receive	
					send	
			preference			
			splithorizon			
		route	create			
			default	create		
				delete		
			delete			
			staticpreference			
		rtrdiscovery	address			
			adminmode			
			lifetime			
			maxinterval			
			mininterval			
			preference			
		vrrp	adminmode			
			interface	adminmode		
				advinterval		
				authdetails		
				ipaddress		
				preemptmode		
				priority		
				routerid		
			removedetails			
	routing					
	snmpcommunity	accessmode				
		create				
		delete				
		ipaddr				
		ipmask				
		mode				

	snmptrap	create				
		delete				
		ipaddr				
		mode				
	spanningtree	adminmode				
		bridge	forwarddelay			
			hellotime			
			maxage			
			priority			
		cst	port	edgeport		
				pathcost		
				priority		
		forceversion				
		port	migrationcheck			
			mode			
	ssh	adminmode				
		protocol				
	syscontact					
	syslocation					
	sysname					
	telnet	maxsessions				
		mode				
		timeout				
	trapflags	authentication				
		dvmrp				
		linkmode				
		multiusers				
		ospf				
		pim				
		stpmode				
	users	add				
		defaultlogin				
		delete				
		login				
		passwd				
		snmpv3	accessmode			
			authentication			
			encryption			
	vlan	bcaststorm				
		create				
		delete				
		makestatic				

		mcaststorm				
		name				
		participation				
		port	acceptframe			
			ingressfilter			
			priority			
			pvid			
			tagging			
help						
logout						
ping						
reset	system					
save	config					
show	acl	detailed				
		summary				
	arp	switch				
		table				
	authentication	login	info			
			users			
	bwprovisioning	bwallocation	detailed			
			summary			
		trafficclass	allocatedbw			
			detailed			
			summary			
	classofservice	802.1p mapping				
	dot1x	port	detailed			
			stats			
			summary			
			users			
		summary				
	eventlog					
	forwardingdb	agetime				
		learned				
		table				
	garp	info				
		interface				
	history					
	http	info				
	igmpsnooping					
	inventory					
	ip	interface				
		stats				

		summary				
		vlan				
	lag					
	loginsession					
	macfilter					
	mfdb	gmrp				
		igmpsnooping				
		staticfiltering				
		stats				
		table				
	mirroring					
	msglog					
	network					
	port					
	protocol					
	radius	accounting	stats			
			summary			
		server	stats			
			summary			
		stats				
		summary				
	router	bootpdhcprelay				
		dvmrp	info			
			interfaceinfo			
			neighborinfo			
			nexthopinfo			
			pruneinfo			
			routeinfo			
		igmp	info			
			interface	detail		
				info		
				membership		
				stats		
				table		
		ip	interface	summary		
		mcast	boundary			
			info			
			interfaceinfo			
			mdebug	mrinforun		
				mstatrun		
				mtracerun		
			mroute	detailed	all	

					group	
					source	
				summary	all	
					group	
					source	
			staticroute	all		
				source		
		ospf	area	info		
				range		
			info			
			interface	info		
				stats		
			lsdb	summary		
			neighbor	detailed		
				table		
			stub	table		
			virtif	detailed		
				summary		
		pimdm	info			
			interface	info		
				stats		
			neighbor			
		pimsm	candrptable			
			componenttable			
			info			
			interface	info		
				stats		
			neighbor			
			rpsettable			
		rip	info			
			interface	detailed		
				summary		
		route	bestroutes			
			entry			
			preferences			
			table			
		rtrdiscovery				
		vrrp	info			
			interface	detailed		
				stats		
				summary		
	snmpcommunity					

	snmptrap					
	spanningtree	bridge				
		cst	detailed			
			port	detailed		
				summary		
		port				
		summary				
	ssh	info				
	stats	port	detailed			
			summary			
		switch	detailed			
			summary			
	sysinfo					
	telnet					
	trapflags					
	traplog					
	users	authentication				
		info				
	vlan	detailed				
		port				
		summary				
transfer	download	datatype				
		filename				
		path				
		serverip				
		start				
	upload	datatype				
		filename				
		path				
		serverip				
		start				

Appendix C. CLI Configuration Examples

This appendix provides examples of using the CLI to configure the Ethernet switch module for some key functions.

Bridging configuration example

This section provides sample CLI commands showing how to configure the Ethernet switch module for basic bridging support. Bridging support, conforming to the IEEE 802.1D compatibility mode specified in IEEE 802.1s, is enabled for the switch and for all ports by default. All ports are enabled by default, and defaults are also provided for timers and protocol parameters.

Although the switch will operate correctly as a bridge implementing the base Spanning Tree Protocol (STP) as configured at the factory, the configuration script in this section will show you how to override the defaults. Before you do so, make sure that you fully understand the protocol and that the values you provide are consistent with each other.

Set a new bridge priority level. Setting the priority level affects the likelihood of the bridge being elected as the root of the spanning tree (the lower the number the greater the probability). It is the only way to change the bridge identifier, which consists of the bridge priority concatenated with the switch base MAC address. The default value is 32768. If all bridges retain their default priority values, the bridge with the lowest MAC address will become the root bridge.

```
config spanningtree bridge priority 7680
```

Set new port priority levels. Setting the priority level affects the likelihood of the port being elected as the root port of the spanning tree (the lower the number the greater the probability). It is the only way to change the port identifier, which consists of the port priority concatenated with the port interface number. The default value is 128.

```
config spanningtree port priority ext.1 16
config spanningtree port priority ext.2 32
```

Set new timer values. The timer values will only take effect if the bridge becomes the root bridge, in which case they will take effect for all bridges in the network.

```
config spanningtree bridge maxage 30
config spanningtree bridge forwarddelay 16
config spanningtree bridge hellotime 14
```

Assign new path cost values to the ports whose priority values were changed. The lower the path cost the more likely that a port will be elected as the root port.

```
config spanningtree port pathcost ext.1 8
config spanningtree port pathcost ext.2 16
```

In addition to the parameters that affect the Spanning Tree Protocol, other parameters, and protocols are defined in IEEE 802.1D which you may also change. For example, IEEE 802.1p has been included in the latest version of 802.1D. Use the following commands to change the default priority mapping provided by the switch. These commands affect all of the interfaces on the switch and leave the defaults unchanged for priority levels 3-7.

```
config classofservice 802.1p mapping 0 0
config classofservice 802.1p mapping 1 2
config classofservice 802.1p mapping 2 1
```

The switch supports two protocols based on the Generic Attribute Registration Protocol (GARP) defined in IEEE 802.1D: GARP Multicast Registration Protocol (GMRP) and GARP VLAN Registration Protocol (GVRP). These protocols are disabled by default.

```
config garp gmrp adminmode enable
config garp gmrp interfacemode all
config garp gvrp adminmode enable
config garp gvrp interfacemode all
```

While the Spanning Tree Protocol is needed to maintain the network topology, forwarding of frames also requires that the switch learn the location of end stations. The switch does this by recording the port on which packets from a source MAC address are received. The forwarding database is used to hold this information. You can control how long an address will remain in the database if no traffic is seen from it (the aging timer).

```
config forwardingdb agetime 500
```

IEEE 802.1w configuration example

This section shows you how to configure the Ethernet switch module to support rapid reconfiguration of the spanning tree topology. The IEEE 802.1w support specified in IEEE 802.1s defines a new configuration algorithm and protocol that provide significantly faster reconfiguration of the spanning tree than the original algorithm and protocol defined in the base IEEE 802.1D standard. While the old and new protocols will successfully interoperate, the IEEE 802.1 standards committee recommends the use of the new protocol.

Configuration of the switch to support IEEE 802.1w is simple. In normal operation, the bridge timers are not used to control reconfiguration, and the default values should be adequate. Bridge and port priorities and path costs are still required, and are configured as shown for IEEE 802.1D.

Configure the switch to use rapid reconfiguration.

```
config spanningtree forceversion 802.1w
```

To disable support for rapid reconfiguration.

```
config spanningtree forceversion 802.1d
```

VLAN configuration example

This section provides sample CLI commands showing how to configure the Ethernet switch module to support IEEE 802.1Q VLANs. Configuring VLANs allows you to partition your network on a logical rather than physical basis. The only physical restriction is that both ends of a point-to-point link must be in the same VLAN. There are many possible logical partitions – one common one being department membership.

The script in the following example shows you how to create and configure VLANs on your switch.

Create and name two VLANs (the names are optional).

```
config vlan create 1
config vlan name 1 vlan_one
config vlan create 2
config vlan name 2 vlan_two
```

Assign the ports that will belong to vlan_one. This will be a tagged VLAN – only tagged packets will be accepted by member ports, and all packets transmitted from member ports will be tagged.

```
config vlan participation include 1 bay.1,bay.2
config vlan port tagging enable 1 bay.1,bay.2
config vlan port acceptframe vlanonly 1 bay.1,bay.2
```

Assign the ports that will belong to vlan_two. Untagged packets will be accepted by member ports bay.3 and bay.4 and assigned the default PVID of 2, and all packets transmitted from member ports will be untagged. Note that bay.2 is a member of both vlan_one and vlan_two, and that ext.1 and ext.2 will never be members.

```
config vlan participation include 2 bay.2,bay.3,bay.4
config vlan participation exclude 2 ext.1,ext.2
config vlan port acceptframe all 2 bay.3,bay.4
```

Assign the same default PVID to ports bay.3 and bay.4.

```
config vlan port pvid 2 bay.3,bay.4
```

Link aggregation configuration example

This section provides sample CLI commands showing how to configure the Ethernet switch module to support IEEE 802.3ad aggregated links. By defining a Link Aggregation Group (LAG) you can treat multiple physical links between two end-points as one logical link. The LAG will also be seen by management functions as a single link.

LAGs are used to increase both link bandwidth and reliability: they are often used for links to the Internet or to shared servers. The script in the following example shows you how to configure and enable two LAGs on the same switch.

Create and name two LAGs.

```
config lag create lag_internet
config lag create lag_server
```

When the switch creates the LAGs, it will assign logical interface IDs that you will use to identify them in subsequent commands. Use the following command to find out what IDs have been assigned:

```
show lag all
```

Add the physical ports to the LAGs. (Assume that lag_internet was assigned ID lag.1 and lag_server was assigned ID lag.2.)

```
config lag addport lag.1 ext.1
config lag addport lag.1 ext.2
config lag addport lag.2 ext.3
config lag addport lag.2 ext.4
```

Enable both LAGs.

```
config lag adminmode lag.1,lag.2 enable
```

The previous command could have been issued instead as:

```
config lag adminmode all enable
```

IGMP snooping configuration example

This section provides sample CLI commands showing how to configure the Ethernet switch module to support IGMP Snooping. Activating IGMP Snooping allows you to restrict the forwarding of multicast packets to network segments that need to see the packets. The switch uses information gained from examining IGMP packets to decide how to forward multicast packets.

You can activate IGMP Snooping for both individual and aggregated physical interfaces. The script in the following example show you how to configure IGMP Snooping.

Enable IGMP Snooping on the switch.

```
config igmpsnooping adminmode enable
```

IGMP Snooping will be enabled with default values for the group membership interval, maximum response, and multicast router present expiration timers. This command overrides the default for the multicast router present expiration timer.

```
config igmpsnooping mcrtrexpiretime 2400
```

Enable IGMP Snooping for a set of physical ports and for a LAG.

```
config igmpsnooping interfacemode bay.1,bay.2,bay.3,bay.4 enable
config igmpsnooping interfacemode lag.1 enable
```

To display information about the IGMP Snooping configuration issue:

```
show igmpsnooping
```

To display information about all multicast addresses issue:

```
show mfdb table all
```

Access Control List configuration example

This section provides sample CLI commands showing how to configure the IBM @server BladeCenter T 4-Port Gb Ethernet switch module to support Access Control Lists (ACLs). ACLs offer one way of adding Quality of Service support to your network.

You define an ACL to control who can use your network or network resources by allowing or prohibiting access. The ACL specifies one or more match criteria that will be used to determine whether a given packet will be admitted to the network. The first match criteria met by a packet determines whether the packet is admitted. If the packet matches none of the criteria, it will be dropped.

An ACL consists of up to ten rules, each applied to one or more of the following fields:

- Source IP address
- Destination IP address
- Source Layer-4 port
- Destination Layer-4 port
- Type of Service byte
- Internet Protocol number

The script in the following example restricts access to the network to UDP and TCP traffic from a defined set of IP source addresses.

Create Access Control List 1.

```
config acl create 1
```

Create Rule 1 for ACL 1.

config acl rule create 1 1

Define the content of ACL 1 Rule 1. Packets will be accepted only if they are TCP packets from the source IP address set defined by the specified IP address and mask.

config acl rule action 1 1 permit

config acl rule match protocol keyword 1 1 tcp

config acl rule match dstip 1 1 192.168.50.0 255.255.255.0

Create Rule 2 for ACL 1.

config acl rule create 1 2

Define the content of ACL 1 Rule 2. Packets will be accepted only if they are UDP packets from the source IP address set defined by the specified IP address and mask. This is the same source IP address set defined for TCP traffic.

config acl rule action 1 2 permit

config acl rule match protocol keyword 1 2 udp

config acl rule match dstip 1 2 192.168.50.0 255.255.255.0

Apply ACL 1 to inbound traffic received on external ports 1-4. Packets that do not match the criteria specified in Rules 1 or 2 will be dropped.

config acl interface add ext.1 inbound 1

config acl interface add ext.2 inbound 1

config acl interface add ext.3 inbound 1

config acl interface add ext.4 inbound 1

VLAN routing configuration example

This section provides sample CLI commands showing how to configure the Ethernet switch module to support VLAN Routing, which allows packets received on a VLAN to be routed rather than bridged. You can configure VLAN Routing for all VLANs on a given port, or for a subset. Configuring VLAN Routing may allow:

- More than one physical port on the switch to connect to the same subnet.
- A VLAN to span more than one physical network.
- The provision of additional security or segmentation.

After you create a VLAN as you would for a non-routing VLAN, you enable it for routing. The switch will assign a logical slot.port number for the routing VLAN which you will use in subsequent commands -- use the **show ip vlan** command to display the number. You then enable and configure routing as you would for a physical interface. This includes specifying the IP addresses and subnet masks for the logical interface.

The script in the following example creates two VLANs, and then configures them for VLAN Routing.

Create and name two VLANs (the name is optional).

config vlan create 1

config vlan name 1 route_vlan_one

config vlan create 2

config vlan name 2 route_vlan_two

Assign the ports that will belong to route_vlan_one and specify that all received and transmitted packets must be tagged.

```
config vlan participation include 1 ext.1, ext.2, ext.3
config vlan port acceptframe vlanonly 1 ext.1, ext.2, ext.3
config vlan port tagging enable 1 ext.1, ext.2, ext.3
```

Assign the ports that will belong to route_vlan_two and specify that untagged packets will be accepted and assigned a default PVID of 2.

```
config vlan participation include 1 ext.6, ext.7
config vlan port acceptframe all 1 ext.6, ext.7
config vlan port pvid 2 ext.6, ext.7
```

Configure the VLANs as routing VLANs.

```
config ip vlan routing create 1
config ip vlan routing create 2
```

Use the show command to find out the logical slot.port numbers assigned to the routing VLANs. You will use these numbers to identify the VLANs in routing commands. For this example, assume that VLAN 1 was assigned ID rtr.1 and VLAN 2 was assigned rtr.2.

```
show ip vlan
```

Enable routing for the switch.

```
config routing enable
```

Enable routing for the VLANs.

```
config interface routing rtr.1 enable
config interface routing rtr.2 enable
```

Define the IP addresses and subnet masks for the routing VLANs.

```
config ip interface create rtr.1 192.168.70.31 255.255.255.0
config ip interface create rtr.2 192.168.70.32 255.255.255.0
```

RIP configuration example

This section provides sample CLI commands showing how to configure the Ethernet switch module to support the Routing Information Protocol (RIP). RIP is one of the protocols used by routers to exchange information about the network topology. It is used primarily in small to medium-sized networks.

In order to configure RIP you must first enable routing for the switch, and for the ports that will participate in the protocol. This includes specifying the IP addresses and subnet masks for the ports.

The Ethernet switch module supports two versions of RIP:

- RIPv1 defined in RFC 1058, in which routes are specified by IP destination number and hop count and the routing table is broadcast to all stations on the network.
- RIPv2 defined in RFC 1723, in which the route specification includes subnet mask and gateway and the routing table is sent to a multicast address.

For each port you may specify the format of packets to be received or transmitted:

- Packets may be received in RIPv1 format, RIPv2 format, both formats or all RIP packets may be dropped.
- Packets may be transmitted in RIPv1 format or RIPv2 format, or transmission of RIP packets may be blocked.
- Packets may be transmitted in RIPv2 format to the RIPv1 broadcast address.

The script in the following example sets up the switch and two ports to support RIP, configures both ports to received both RIPv1 and RIPv2 packets, but to transmit only RIPv2 packets. No authorization key will be used in RIPv2 packets and no default route is defined.

Enable routing for the switch.

```
config routing enable
```

Enable routing for two ports.

```
config interface routing ext.1 enable
config interface routing ext.2 enable
```

Define the IP addresses and subnet masks for the routing interfaces.

```
config ip interface create ext.1 192.168.70.1 255.255.255.0
config ip interface create ext.2 192.168.70.2 255.255.255.0
```

Enable RIP for the switch, first specifying the router ID and the route preference.

```
config router id 192.168.1.1
config router rip preference 10
config router rip adminmode enable
```

Enable RIP for the interfaces, allowing authentication to default to none.

```
config router rip interface mode ext.1 enable
config router rip interface mode ext.2 enable
```

Specify how RIP packets will sent and received.

```
config router rip interface version receive ext.1 both
config router rip interface version receive ext.1 both
config router rip interface version send ext.1 rip2
config router rip interface version send ext.2 rip2
```

OSPF configuration example

This section provides sample CLI commands showing how to configure the Ethernet switch module to support the Open Shortest Path First (OSPF) protocol. OSPF is one of the protocols used by routers to exchange information about the network topology. It is used primarily in large networks, for which it offers the following advantages:

- Hierarchical management of the network, allowing for division of the network into areas.
- A reduction in network traffic:
  - Routing table updates are sent to a multicast address
  - Routing table updates are sent only when a change has occurred
  - Only the updated section of the routing table is sent

A complete OSPF network is called an Autonomous System (AS). The AS may be divided into a number of areas which communicate across an OSPF backbone using inter-area routing. Within each area intra-area routing is used. A router running OSPF assumes different roles depending on its location within the network, for example, a border router communicates with other border routers using inter-area protocols, while a router within an area would use only intra-area protocols.

An OSPF router determines the best route to a destination station based on the assigned cost and type of the available routes. The order of preference is:

- Intra-area route
- Inter-area route
- External type 1 route (a route external to the AS)
- External type 2 route (a route learned from other routing protocols)

In order to configure OSPF you must first enable routing for the switch, and for the ports that will participate in the protocol. This includes specifying the IP addresses and subnet masks for the ports.

The script in the first example in this section shows you how to configure the Ethernet switch module as a border router. The second example will show how to configure it as an inter-area router.

This script configures a border router. It first sets up the switch and three ports to support OSPF, then enables OSPF for the switch and ports and assigns the priority and route cost for the ports.

Enable routing for the switch.

```
config routing enable
```

Enable routing for three ports.

```
config interface routing ext.1 enable
config interface routing ext.2 enable
config interface routing ext.3 enable
```

Define the IP addresses and subnet masks for the routing interfaces.

```
config ip interface create ext.1 192.168.70.1 255.255.255.0
config ip interface create ext.2 192.168.70.5 255.255.255.0
config ip interface create ext.3 192.168.70.12 255.255.255.0
```

Enable OSPF for the switch, first specifying the router ID.

```
config router id 192.168.70.7
config router ospf adminmode enable
```

Enable OSPF for the interfaces, specifying the area to which they offer connectivity.

```
config router ospf interface areaid ext.1 0.0.0.2
config router ospf interface areaid ext.2 0.0.0.2
config router ospf interface areaid ext.2 0.0.0.2
config router ospf interface mode ext.1 enable
config router ospf interface mode ext.2 enable
config router ospf interface mode ext.3 enable
```

Specify the OSPF port priority and cost.

```
config router ospf interface priority ext.1 128
config router ospf interface priority ext.2 255
config router ospf interface priority ext.3 255
config router ospf interface cost ext.1 32
config router ospf interface cost ext.2 64
config router ospf interface cost ext.3 64
```

This script configures an inter-area router. It first sets up the switch and two ports to support OSPF, then enables OSPF for the switch and ports and assigns the priority and route cost for the ports.

Enable routing for the switch.

config routing enable

Enable routing for two ports.

config interface routing ext.1 enable

config interface routing ext.2 enable

Define the IP addresses and subnet masks for the routing interfaces.

config ip interface create ext.1 192.168.70.1 255.255.255.0

config ip interface create ext.2 192.168.70.2 255.255.255.0

Enable OSPF for the switch, first specifying the router ID.

config router id 192.168.1.1

config router ospf adminmode enable

Enable OSPF for the interfaces, specifying the areas to which they offer connectivity.

config router ospf interface areaid ext.1 0.0.0.2

config router ospf interface areaid ext.2 0.0.0.3

config router ospf interface mode ext.1 enable

config router ospf interface mode ext.2 enable

Specify the OSPF port priority and cost.

config router ospf interface priority ext.1 128

config router ospf interface priority ext.2 255

config router ospf interface cost ext.1 32

config router ospf interface cost ext.2 64

VRRP configuration example

This section provides sample CLI commands showing how to configure the Ethernet switch module to support the Virtual Router Redundancy Protocol (VRRP). VRRP is used to provide a backup router in a network using static default routes. End stations use a virtual router IP address which is normally handled by a master router. If the master router goes down, a second router, configured as the backup router will take over and continue to handle traffic using the virtual router IP address. Either a physical port or a routing VLAN may be configured to support the protocol, and more than one port may be configured as a virtual router port.

In order to configure VRRP you need to configure, at a minimum, a master router and one backup router. The script in the first example in this section shows you how to configure the Ethernet switch module as a master router. The second example will show how to configure a second Ethernet switch module as the backup router.

This script configures a VRRP master router. It first sets up the switch and a port to support routing, then enables VRRP for the switch. Before enabling VRRP on the port, the virtual IP address is assigned.

Enable routing for the switch.

config routing enable

Define the IP addresses and subnet masks for the port that will support VRRP.

config ip interface create ext.1 192.168.70.1 255.255.255.0

Enable VRRP for the switch, first specifying the router ID.

config router id 192.168.70.7

```
config router vrrp adminmode enable
```

Assign a virtual router ID to the port.

```
config router vrrp interface routerID ext.1 10
```

Specify the virtual IP address. Since this address is the same as the port non-virtual IP address, this router will always be the master router as long as it is functioning. Note that the VRID is included as a parameter, since a port may participate in more than one virtual network at a time.

```
config router vrrp interface ipaddress ext.1 10 192.168.70.1
```

Specify the port priority. Since this port owns the virtual IP address, its priority is set to 254.

```
config router vrrp interface priority ext.1 10 254
```

Enable VRRP on the port.

```
config router vrrp interface adminmode ext.1 10 enable
```

This script configures a VRRP backup router. It first sets up the switch and a port to support routing, then enables VRRP for the switch. Before enabling VRRP on the port, the virtual IP address is assigned.

Enable routing for the switch.

```
config routing enable
```

Define the IP addresses and subnet masks for the port that will support VRRP.

```
config ip interface create ext.6 192.168.70.6 255.255.255.0
```

Enable VRRP for the switch, first specifying the router ID.

```
config router id 192.168.70.5
config router vrrp adminmode enable
```

Assign a virtual router ID to the port.

```
config router vrrp interface routerID ext.6 60
```

Specify the virtual IP address. Since the address is the same as router 192.168.70.7 port ext.1 non-virtual IP address, this router will always be the backup router as long as router 192.168.70.7 is functioning. Note that the VRID is included as a parameter, since a port may participate in more than one virtual network at a time.

```
config router vrrp interface ipaddress ext.6 60 192.168.70.1
```

Specify the port priority.

```
config router vrrp interface priority ext.6 60 128
```

Enable VRRP on the port.

```
config router vrrp interface adminmode ext.6 60 enable
```

IGMP configuration example

This section provides sample CLI commands showing how to configure the Ethernet switch module to support the Internet Group Management Protocol (IGMP). IGMP is used to support the transmission and reception of multicast packets in a routed network. A router sends IGMP packets to inform its neighbors of its ability to receive multicast packets. The protocol allows routers to:

- Become members of one or more multicast groups.
- Receive multicast packets sent to groups of which they are members.
- Record and manage multicast group membership.
- Periodically check whether multicast group members are still active.

- Use group membership information to determine whether and how to forward multicast packets.

A router supporting IGMP is in one of two states:

Querier mode:
the router transmits IGMP membership queries and constructs the IGMP table entries in the Multicast Forwarding Database.

Non-querier mode:
the router does not transmit IGMP query packets. Only one router should be in querier mode on a network. If the “other querier present timer” expires the router will re-enter the querier mode.

Only one interface of a given router may be configured to listen for multicast reports or transmit multicast packets on a subnet, even if more than one interface is connected to that subnet.

There are two versions of IGMP: IGMPv1, defined in RFC 1112, and IGMPv2 defined in RFC 2236. You need to configure all of the routers in your network to run the same version of IGMP.

Note: IGMP is a base multicast protocol used by other multicast protocols such as DVMRP or PIM-DM/SM. You must configure IGMP on your switch before configuring another multicast protocol.

This script configures IGMP support on a switch. It first sets up the switch and three ports to support routing, then enables IGMP for the switch and ports.

Enable routing for the switch and assign the router id.

```
config routing enable
config router id 192.168.70.0
```

Define the IP addresses and subnet masks for three routing ports.

```
config ip interface create rtr.1 192.168.70.1 255.255.255.0
config ip interface create rtr.2 192.168.70.2 255.255.255.0
config ip interface create rtr.3 192.168.70.3 255.255.255.0
```

Enable RIP for the switch and the routing interfaces.

```
config router rip adminmode enable
config router rip interface mode rtr.1 enable
config router rip interface mode rtr.2 enable
config router rip interface mode rtr.3 enable
```

Enable multicast and IGMP for the router.

```
config router mcast adminmode enable
config router igmp adminmode enable
```

Enable IGMP for the routing interfaces and specify that they will run IGMPv1.

```
config router igmp interface mode rtr.1 enable
config router igmp interface version rtr.1 1
config router igmp interface mode rtr.2 enable
config router igmp interface version rtr.2 1
config router igmp interface mode rtr.3 enable
config router igmp interface version rtr.3 1
```

Override the IGMP defaults for one of the routing interfaces.

```
config router igmp interface queryinterval rtr.1 600
config router igmp interface maxresptime rtr.1 20
config router igmp interface robustness rtr.1 10
config router igmp interface startupqryint rtr.1 100
config router igmp interface startupqrycnt rtr.1 10
config router igmp interface lastmemqryint rtr.1 100
config router igmp interface startupqrycnt rtr.1 10
```

DVMRP configuration example

This section provides sample CLI commands showing how to configure the Ethernet switch module to support the Distance Vector Multicast Routing Protocol (DVMRP). DVMRP is a distributed, dense-mode multicast protocol. Since it is a dense-mode protocol it is best-suited for networks with plentiful bandwidth and with at least one multicast group member in each subnet. A router supporting DVMRP sends protocol messages to other routers:

Probe messages:
to determine the identity of neighboring DVMRP routers.

Prune messages:
to remove routers with no members for a given group.

Graft messages:
to cancel a previous prune message.

Graft acknowledgement messages:
to acknowledge receipt of graft messages.

DVMRP needs a unicast routing protocol such as RIP or OSPF to provide the routes in the Multicast Forwarding Database. It also needs the group membership information acquired by IGMP

Note: Since DVMRP relies on IGMP for basic functionality, you must configure IGMP on your switch before configuring DVMRP.

This script configures DVMRP support on a switch. It first sets up the switch and three ports to support routing, then enables IGMP for the switch and ports and finally enables DVMRP for the switch and ports.

Enable routing for the switch and assign the router id.

```
config routing enable
config router id 192.168.70.0
```

Define the IP addresses and subnet masks for three routing ports.

```
config ip interface create rtr.1 192.168.70.1 255.255.255.0
config ip interface create rtr.2 192.168.70.2 255.255.255.0
config ip interface create rtr.3 192.168.70.3 255.255.255.0
```

Enable RIP for the switch and the routing interfaces.

```
config router rip adminmode enable
config router rip interface mode rtr.1 enable
config router rip interface mode rtr.2 enable
config router rip interface mode rtr.3 enable
```

Enable multicast and IGMP for the router.

```
config router mcast adminmode enable
config router igmp adminmode enable
```

Enable IGMP for the routing interfaces, allowing the version to default to IGMPv2.

```
config router igmp interface mode rtr.1 enable
config router igmp interface mode rtr.2 enable
config router igmp interface mode rtr.3 enable
```

Enable DVMRP for the router.

```
config router dvmrp adminmode enable
```

Enable DVMRP for the routing interfaces.

```
config router dvmrp interface mode rtr.1 enable
config router dvmrp interface mode rtr.2 enable
config router dvmrp interface mode rtr.3 enable
```

Override the DVMRP default for one of the routing interfaces.

```
config router dvmrp interface metric rtr.1 6
```

PIM-DM configuration example

This section provides sample CLI commands showing how to configure the Ethernet switch module to support Protocol Independent Multicast - Dense Mode (PIM-DM). PIM-DM provides scalable inter-domain multicast routing independent of the underlying unicast routing protocol. It creates source-based shortest-path distribution trees using Reverse Path Forwarding (RPF), the unicast routing table and prune/graft messages. The default operation of PIM-DM is to flood traffic, prune messages are used to stop traffic being forwarded to areas of the network with no group members, but a prune state has a limited lifetime in the absence of a refresh message. The protocol is best-suited for networks with the following characteristics:

- Densely distributed receivers
- Few senders but many receivers
- Constant and high volume of multicast traffic

A router supporting DVMRP sends protocol messages to other routers:

Hello messages:
to detect neighboring PIM-DM routers.

Prune messages:
to remove routers with no members for a given group.

Graft messages:
to cancel a previous prune message.

Graft acknowledgement messages:
to acknowledge receipt of graft messages.

Join messages:
similar to a graft message, but no acknowledgement is required.

DVMRP needs a unicast routing protocol such as RIP or OSPF to provide the routes in the Multicast Forwarding Database. It also needs the group membership information acquired by IGMP, however it cannot coexist with another multicast routing protocol.

Note: Since PIM-DM relies on IGMP for basic functionality, you must configure IGMP on your switch before configuring PIM-DM.

This script configures PIM-DM support on a switch. It first sets up the switch and three ports to support routing, then enables IGMP for the switch and ports and finally enables PIM-DM for the switch and ports.

Enable routing for the switch and assign the router id.

```
config routing enable
config router id 192.168.70.0
```

Define the IP addresses and subnet masks for three routing ports.

```
config ip interface create rtr.1 192.168.70.1 255.255.255.0
config ip interface create rtr.2 192.168.70.2 255.255.255.0
config ip interface create rtr.3 192.168.70.3 255.255.255.0
```

Enable OSPF for the switch and the routing interfaces.

```
config router ospf adminmode enable
config router ospf interface area rtr.1 0.0.0.2
config router ospf interface area rtr.2 0.0.0.2
config router ospf interface area rtr.3 0.0.0.2
config router ospf interface mode rtr.1 enable
config router ospf interface mode rtr.2 enable
config router ospf interface mode rtr.3 enable
```

Enable multicast and IGMP for the router.

```
config router mcast adminmode enable
config router igmp adminmode enable
```

Enable IGMP for the routing interfaces, allowing the version to default to IGMPv2.

```
config router igmp interface mode rtr.1 enable
config router igmp interface mode rtr.2 enable
config router igmp interface mode rtr.3 enable
```

Enable PIM-DM for the router.

```
config router pimdm adminmode enable
```

Enable PIM-DM for the routing interfaces.

```
config router pimdm interface mode rtr.1 enable
config router pimdm interface mode rtr.2 enable
config router pimdm interface mode rtr.3 enable
```

Override the default hello-time interval for one of the routing interfaces.

```
config router pimdm interface hellointerval rtr.1 60
```

PIM-SM configuration example

This section provides sample CLI commands showing how to configure the Ethernet switch module to support Protocol Independent Multicast - Sparse Mode (PIM-SM). PIM-SM provides scalable inter-domain multicast routing independent of the underlying unicast routing protocol. It creates unidirectional shared trees routed in a Rendezvous Point (RP) or, optionally, source-based shortest-path distribution trees for greater efficiency. PIM-SM only sends multicast traffic to hosts who specifically request such traffic. The protocol is well-suited for networks with bandwidth constraints, those with few multicast receivers and those that may span wide area networks.

Two router roles are part of the PIM-SM protocol:

Rendezvous Point (RP)
The root of a shared distribution tree.

Designated Router (DR)
The router with responsibility for sending join and register messages to the RP.

Two methods are used by PIM-SM to build multicast routing trees:

Source sending data
A DR receiving a multicast packet from a source encapsulates the packet in a Register message and sends it to the RP.

Receiver requesting data
A host wanting to join a multicast group sends a Join message using IGMP to the RP.

If the data rate of packets from a specific source exceeds a configurable threshold, PIM-SM can switch from the shared tree to a source-specific shortest path tree to improve efficiency. The shortest path tree is built by the RP and last-hop DR using Join/Prune messages.

PIM-SM needs a unicast routing protocol such as RIP or OSPF to provide the routes in the Multicast Forwarding Database. It also needs the group membership information acquired by IGMP, however it can not coexist with another multicast routing protocol.

Note: Since PIM-SM relies on IGMP for basic functionality, you must configure IGMP on your switch before configuring PIM-SM.

This script configures PIM-SM support on a switch. It first sets up the switch and three ports to support routing, then enables IGMP for the switch and ports and finally enables PIM-SM for the switch and ports.

Enable routing for the switch and assign the router id.

```
config routing enable
config router id 192.168.70.0
```

Define the IP addresses and subnet masks for three routing ports.

```
config ip interface create rtr.1 192.168.70.1 255.255.255.0
config ip interface create rtr.2 192.168.70.2 255.255.255.0
config ip interface create rtr.3 192.168.70.3 255.255.255.0
```

Enable OSPF for the switch and the routing interfaces.

```
config router ospf adminmode enable
config router ospf interface area rtr.1 0.0.0.2
config router ospf interface area rtr.2 0.0.0.2
config router ospf interface area rtr.3 0.0.0.2
config router ospf interface mode rtr.1 enable
config router ospf interface mode rtr.2 enable
config router ospf interface mode rtr.3 enable
```

Enable multicast and IGMP for the router.

```
config router mcast adminmode enable
config router igmp adminmode enable
```

Enable IGMP for the routing interfaces, allowing the version to default to IGMPv2.

config router igmp interface mode rtr.1 enable

config router igmp interface mode rtr.2 enable

config router igmp interface mode rtr.3 enable

Enable PIM-SM for the router.

config router pimsm adminmode enable

Override the PIM-SM default join/prune interval timer for the router.

config router pimsm joinpruneintvl 60

Override the data threshold at which PIM-SM will switch to a shortest path first tree when it is the last hop router.

config router pimsm datathreshrate 1000

Override the data threshold at which PIM-SM will switch to a shortest path first tree when it is the Rendezvous Point.

config router pimsm regthreshrate 1000

Enable PIM-SM for the routing interfaces.

config router pimsm interface mode rtr.1 enable

config router pimsm interface mode rtr.2 enable

config router pimsm interface mode rtr.3 enable

Override the default hello-time interval for one of the routing interfaces.

config router pimsm interface hellointerval rtr.1 60

Specify that one of the routing interfaces is not a candidate bootstrap router.

config router pimsm interface cbsrpreference rtr.1 -1

Appendix D. Command Syntax Quick Reference

This section contains the list of Command Line Interface (CLI) management commands that are used with the IBM @server BladeCenter T 4-port Gb Ethernet Switch Module.

System commands

These commands display and configure system information and statistics.

Address Resolution Protocol (ARP) cache

- show arp switch

Forwarding DB

- config forwardingdb agetime *10 - 1000000*
- show forwarding db agetime
- show forwardingdb learned
- show forwardingdb table

Inventory

- show inventory

Logs

- show eventlog
- show msglog

Port

System and configuration

- config port admimode *port/listofports/all enable/disable*
- config port autoneg *port/listofports/all enable/disable*
- config port flowcontrol *port/listofports/all enable/disable*
- config port lacpmode *port/listofports/all enable/disable*
- config port linktrap *port/listofports/all enable/disable*
- config port physicalmode *port/listofports/all 1000f/100f/100h/10f/10h*
- show port *port/listofports/all*

Mirroring

- config mirroring create *portport*
- config mirroring delete
- config mirroring mode *enable/disable*
- show mirroring

Simple Network Management Protocol (SNMP) commands

The following SNMP commands are available for network management.

Community commands

- config snmpcommunity accessmode *readonly/readwrite name*
- config snmpcommunity create *name*
- config snmpcommunity delete *name*
- config snmpcommunity ipaddr *ipaddr name*
- config snmpcommunity ipmask *ipmask name*
- config snmpcommunity mode *enable/disable name*
- show snmpcommunity

Trap commands

- config snmptrap create *nameipaddr*
- config snmptrap delete *name ipaddr*
- config snmptrap ipaddr *ipaddroldname ipaddrnew*
- config snmptrap mode *enable/disable name ipaddr*
- show snmptrap

System configuration

The following commands are used to manage the Ethernet switch module.

Login

- config loginsession close *sessionid/all*
- show loginsession

Network connectivity

- config network javamode *enable/disable*
- config network webmode *enable/disable*
- show network

System description

- config prompt *system prompt*
- config syscontact *contact*
- config syslocation *location*
- config sysname *name*
- show stats port detailed *port*
- show stats port summary *port*
- show stats switch detailed
- show stats switch summary
- show sysinfo

Telnet

- config telnet maxsessions *0-5*
- config telnet mode *enable/disable*
- config telnet timeout *0-160*
- show telnet

User accounts

- config users add *name*
- config users delete *name*
- config users passwd *user*
- config users snmpv3 accessmode *user readonly/readwrite*
- config users snmpv3 authentication *user none/md5/sha*
- config users snmpv3 encryption *user none/des [key]*
- show users info

System utilities

The commands in this section allow you to fine tune your system performance and functionality.

System utilities commands

- clear config
- clear igmpsnooping
- clear lag
- clear pass
- clear stats port *port/listofports/all*
- clear stats switch
- clear transfer
- clear traplog
- clear vlan
- logout
- ping *ipaddr*
- reset system
- save config
- show history

Transfer download commands

- transfer download datatype *code/config*
- transfer download filename *name*
- transfer download path *path*
- transfer download serverip *ipaddr*
- transfer download start

Transfer upload commands

- transfer upload datatype *config/errorlog/msglog/traplog*
- transfer upload filename *name*
- transfer upload path
- transfer upload serverip *ipaddr*
- transfer upload start

Trap management

- config trapflags authentication *enable/disable*
- config trapflags dvmrp *enable/disable*
- config trapflags linkmode *enable/disable*
- config trapflags multiusers *enable/disable*
- config trapflags ospf *enable/disable*
- config trapflags pim *enable/disable*
- config trapflags stpmode *enable/disable*
- show trapflags
- show traplog

Switching configuration commands

This section lists commands you use to manage the switch and show the current management settings.

Generic Attribute Registration Protocol (GARP) commands

- config garp gmrp adminmode *enable/disable*
- config garp gmrp interfacemode *port/listofports/all enable/disable*
- config garp gvrp adminmode *enable/disable*
- config garp gvrp interfacemode *port/listoports/all enable/disable*
- config garp jointimer *port/listofports/all 10-100*
- config garp leavealltimer *port/listofports/all 200-6000*
- config garp leavetimer *port/listofports/all 20-600*
- show garp info
- show garp interface *port/listofports/all*

IGMP snooping commands

- config igmpsnooping adminmode *enable/disable*
- config igmpsnooping groupmembershipinterval *2-3600*
- config igmpsnooping interfacemode *port/listofports/all enable/disable*
- config igmpsnooping maxresponse *1-3599*
- config igmpsnooping mcrtexpiretime *0-3600*
- show igmpsnooping

Link Aggregation (LAG) commands

- config lag addport *logical_port port*
- config lag adminmode *logical_port/listofports/all enable/disable*
- config lag create *name*
- config lag deletelag *logical_port/listofports/all*
- config lag deleteport *logical_port port/listofports/all*
- config lag linktrap *logical_port/listofports/all enable/disable*
- config lag name *logical_port name*
- show lag *logical_port/listofports/all*

MAC filter commands

- config macfilter addest *macaddr vlan port/listofports/all*
- config macfilter create *macaddr vlan*
- config macfilter deldest *macaddr vlan port/listofports/all*
- config macfilter remove *macaddr vlan*
- show macfilter *all/macaddrall/vlan*

Multicast Forwarding Database (MFDB) commands

- show mfdb gmrp
- show mfdb igmpsnooping
- show mfdb staticfiltering
- show mfdb stats

- show mfdb table [macaddr/all]

Protocol - VLAN

- config protocol create *groupname*
- config protocol delete *groupname*
- config protocol interface add *groupid port/listofports/all*
- config protocol interface remove *groupid port/listofports/all*
- config protocol protocol add *groupid protocol*
- config protocol protocol remove *groupid protocol*
- config protocol vlan add *groupid vlan*
- config protocol vlan remove *groupid vlan*
- show protocol *groupid/all*

Virtual Local Area Network (VLAN) commands

- config vlan bcaststorm *1-4094 enable/disable*
- config vlan create *2-4094*
- config vlan delete *2-4094*
- config vlan makestatic *2-4094*
- config vlan mcaststorm *1-4094 enable/disable*
- config vlan name *name 2-4094*
- config vlan participation *exclude/include/auto 1-4094 port/listofports/all*
- config vlan port acceptframe *all/vlanonly port/listofports/all*
- config vlan port ingressfilter *enable/disable port/listofports/all*
- config vlan port priority *0-7 port/listofports/all*
- config vlan port pvid *1-4094 port/listofports/all*
- config vlan port tagging *enable/disable port/listofports/all*
- show vlan detailed
- show vlan port
- show vlan summary

Spanning tree commands

This section lists the commands available for the spanning tree protocol.

Spanning tree bridge commands

- config spanningtree bridge forwarddelay *4-30*
- config spanningtree bridge hellotime *1-10*
- config spanningtree bridge maxage *6-40*
- config spanningtree bridge priority *0-61440*
- show spanningtree bridge

Spanning tree Common Spanning Tree (CST) commands

- config spanningtree cst port edgeport *port true/false*
- config spanningtree cst port pathcost *port 1-20000000/auto*
- config spanningtree cst port priority *port 0-240*
- show spanningtree cst detailed

- show spanningtree cst port detailed *port*
- show spanningtree cst port summary *port/listofports/all*

Spanning tree port commands

- config spanningtree port migrationcheck *port/listofporrts/*all *enable/disable*
- config spanningtree port mode *port/listofports/all enable/disable*
- show spanningtree port *port*

Spanning tree summary commands

- config spanningtree adminmode *enable/disable*
- config spanningtree forceversion *802.1D/802.1w*
- show spanningtree summary

Routing configuration commands

The commands in this section are used to configure features and options of the Ethernet switch module, and display parameter settings, statistics, and other information.

Address resolution protocol (ARP) commands

- config arp agetime *15-3600 seconds*
- config arp cachesize *10-3072*
- config arp create *arpentry macaddr*
- config arp delete *arpentry*
- config arp resptime *1-10*
- config arp retries *1-10*
- show arp table

Internet protocol commands

- config interface encaps *port encapstype*
- config ip forwarding *enable/disable*
- config ip interface create *port ipaddr subnetmask*
- config ip interface delete *port ipaddr subnetmask*
- config interface mtu *port 576-1500*
- config ip interface netdirbcast *enable/disable*
- config routing *enable/disable*
- show ip interface *port*
- show ip interface summary
- show ip stats
- show ip summary

Open Shortest Path First (OSPF) commands

The commands in this section are used to configure and display OSPF parameters.

OSPF configuration / summary commands

- config router ospf 1583compatibility *enable/disable*
- config ospf interface cost *ipaddr port 1-65535*
- config router ospf adminmode *enable/disable*
- config router ospf area authentication *areaid none/simple/encrypt*
- config router ospf area range create *areaid ipaddr subnetmask* [enable/disable]
- config router ospf area range delete *areaid ipaddr subnetmask* [summ]
- config router ospf asbr *enable/disable*
- config router ospf area stub create *areaid*
- config router ospf area stub delete *areaid*
- config router ospf area stub metric type *areaid type*
- config router ospf area stub metric value *areaid 1-16777215*
- config router ospf area stub summarylsa *areaid enable/disable*
- config router ospf exoverflowinterval *0-2147483647*
- config router ospf extlsdblimit *-1-2147483647*
- config router ospf interface areaid *port areaid*

- config router ospf interface authentication encrypt *port key keyid*
- config router ospf interface authentication none *port*
- config router ospf interface authentication simple *port key*
- config router ospf interface iftransitdelay *port 1-3600*
- config router ospf interface interval dead *port 0-2147483647*
- config router ospf interface interval hello *port 1-65535*
- config router ospf interface interval retransmit *port 0-3600*
- config router ospf interface mode *port enable/disable*
- config router ospf interface priority *port 0-255*
- config router ospf preference *intra/inter/type1/type2 1-255*
- show router ospf area info *areaid*
- show router ospf area range *areaid*
- show router ospf info
- show router ospf interface info
- show router ospf interface stats
- show router ospf interface summary
- show router ospf lsdb summary
- show router ospf neighbor detailed
- show router ospf neighbor table

OSPF virtual interface (virtif) commands

- config router ospf virtif authentication encrypt
- config router ospf virtif authentication none
- config router ospf virtif authentication simple
- config router ospf virtif create
- config router ospf virtif delete
- config router ospf virtif interval dead
- config router ospif virtif interval hello
- config router ospf virtif interval retransmit
- config router ospf virtif transdelay
- show router ospf virtif detailed
- show router ospf virtif summary

Router BOOTP/DHCP Relay commands

- config router bootdhcprelay adminmode
- config router bootdhcprelay cidoptmode
- config router bootdhcprelay maxhopcount
- config router bootdhcprelay minwaittime *100*
- config router bootdhcprelay serverip
- show router bootdhcprelay

Router (rtr) discovery commands

- config rtrdiscovery address
- config rtrdiscovery adminmode
- config rtrdiscovery lifetime
- config rtrdiscovery maxinterval

- config rtrdiscovery mininterval *1800*
- config rtrdiscovery preference
- show rtrdiscovery

Router route commands

- config router id
- config router route create 255]
- config router route default create
- config router route default delete
- config router route delete
- config router route staticpreference
- show router route bestroutes
- show router route entry
- show router route preferences
- show router route table

Routing Information Protocol (RIP) commands

- config router rip adminmode
- config router rip interface authentication encrypt
- config router rip interface authentication none
- config router rip interface authentication simple
- config router rip autosummary
- config router rip interface defaultmetric
- config router rip hostrouteaccept
- config router rip interface mode
- config router rip interface version receive
- config router rip interface version send
- config router rip preference
- config router rip splithorizon
- show router rip info
- show router rip interface detailed
- show router rip interface summary

Virtual Local Area Network (VLAN) routing commands

- config ip vlan routing create
- config ip vlan routing delete
- show ip vlan

Virtual Router Redundancy Protocol (VRRP) commands

- config router vrrp adminmode
- config router vrrp interface adminmode
- config router vrrp interface advinterval
- config router vrrp interface authdetails
- config router vrrp interface ipaddress
- config router vrrp interface preemptmode

- config router vrrp interface priority
- config router vrrp interface routerid
- config router vrrp removedetails
- show router vrrp info
- show router vrrp interface detailed
- show router vrrp interface stats
- show router vrrp interface summary

Multicast commands

This section lists the Multicast commands available to configure features and options of the Ethernet switch, and to show parameter settings, statistics and other information..

Distance Vector Multicast Routing Protocol (DVMRP) commands

- config router dvmrp adminmode
- config router dvmrp interface metric
- config router dvmrp interface mode
- show router dvmrp info
- show router dvmrp interfaceinfo
- show router dvmrp neighborinfo
- show router dvmrp nexthopinfo
- show router dvmrp pruneinfo
- show router dvmrp routeinfo

Internet Group Management Protocol (IGMP) Commands

- config router igmp adminmode
- config router igmp interface lastmemqrycnt
- config router igmp interface lastmemqryint
- config router igmp interface maxresptime
- config router igmp interface mode
- config router igmp interface queryinterval
- config router igmp interface robustness
- config router igmp interface startupqrycnt
- config router igmp interface startupqryint
- config router igmp interface version
- show router igmp info
- show router igmp interface detail
- show router igmp interface info
- show router igmp interface membership
- show router igmp interface stats
- show router igmp interface table

Mcast commands

- clear mcast mroute all
- clear mcast mroute group
- clear mcast mroute source [groupipaddr]
- config router mcast adminmode
- config router mcast boundary add
- config router mcast boundary delete
- config router mcast mdebug mrinforun [ipaddr]
- config router mcast mdebug mstatrun
- config router mcast mdebug mtraceadminmode
- config router mcast mdebug mtracerun

- config router mcast staticroute add
- config router mcast staticroute delete
- config router mcast ttlthreshold
- show router mcast boundary
- show router mcast info
- show router mcast interfaceinfo
- show router mcast mdebug mrinforun
- show router mcast mdebug mstatrun
- show router mcast mdebug mtracerun
- show router mcast mroute detailed all
- show router mcast mroute detailed group
- show router mcast mroute detailed source
- show router mcast mroute summary all
- show router mcast mroute summary group
- show router mcast mroute summary source
- show router mcast staticroute all
- show router mcast staticroute source

Protocol Independent Multicast - Dense Mode (PIM-DM) Commands

- config router pimdm adminmode
- config router pimdm interface hellointerval
- config router pimdm interface mode
- show router pimdm info
- show router pimdm interface info
- show router pimdm interface stats
- show router pimdm neighbor

Protocol Independent Multicast - Sparse Mode (PIM-SM) Commands

- config router pimsm adminmode
- config router pimsm datathreshrate
- config router pimsm interface cbspreference
- config router pimsm interface hellointerval
- config router pimsm interfacemode
- config router pimsm joinpruneintvl
- config router pimsm regthreshrate
- show router pimsm candrptable
- show router pimsm componenttable
- show router pimsm info
- show router pimsm interface info
- show router pimsm interface stats
- show router pimsm neighbor
- show router pimsm rpsettable

Class of Service Commands

- config classofservice 802.1pmapping *7*
- show classofservice 802.1pmapping

Security Configuration Commands

The commands in this section are used to configure and manage the security features of the Ethernet switch module

Authentication Commands

- config authentication login create
- config authentication login delete
- config authentication login set [local/radius/reject]
- config users defaultlogin
- config users login
- show authentication login info
- show authentication login users
- show users authentication

IEEE 802.1X Commands

- clear dot1x port stats
- config dot1x adminmode
- config dot1x defaultlogin
- config dot1x login
- config dot1x port controlmode
- config dot1x port initialize
- config dot1x port maxrequests *10*
- config dot1x port quietperiod *65535*
- config dot1x port reauthenabled
- config dot1x port reauthenticate
- config dot1x port reauthperiod *65535*
- config dot1x port servertimeout *65535*
- config dot1x port supptimeout *65535*
- config dot1x port transmitperiod
- config dot1x port users add
- config dot1x port users remove
- show dot1x port detailed
- show dot1x port stats
- show dot1x port summary
- show dot1x port users
- show dot1x summary

Remote Authentication Dial-In User Service (RADIUS) Commands

The commands in this section are used to configure RADIUS accounting features and to configure and display RADIUS configuration parameters.

RADIUS Accounting Commands

- config radius accounting mode
- config radius accounting server add
- config radius accounting server port
- config radius accounting server remove

- config radius accounting server secret
- show radius accounting stats
- show radius accounting summary

RADIUS Configuration/Summary Commands

- clear radius stats
- config radius maxretransmit
- config radius timeout
- show radius stats
- show radius summary

RADIUS Server Commands

- config radius server add
- config radius server msgauth
- config radius server port *65535*
- config radius server primary
- config radius server remove
- config radius server secret
- show radius server stats
- show radius server summary

Secure Shell (SSH) Commands

- config ssh adminmode
- config ssh protocol
- show ssh info

Server Socket Layer (SSL) Commands

- config http secureport *65535*
- config http secureprotocol
- config http secureserver adminmode
- show http info

Quality of Service (QoS)

This section lists the commands available to configure and manage the QoS features of the Ethernet switch module.

Access Control List (ACL) commands

- config acl create
- config acl delete
- config acl interface add
- config acl interface remove
- config acl rule action
- config acl rule create *10*
- config acl rule delete
- config acl rule match dstip
- config acl rule match dstl4port keyword
- config acl rule match dstl4port number
- config acl rule match every
- config acl rule match protocol keyword
- config acl rule match protocol number
- config acl rule match protocol number
- config acl rule match srcip
- config acl rule match srcl4port keyword
- show acl detailed
- show acl summary

Bandwidth (BW) provisioning commands

The following commands are used to configure and display bandwidth information.

BW allocation commands

- config bwprovisioning bwallocation create
- config bwprovisioning bwallocation delete
- config bwprovisioning bwallocation maxbandwidth
- show bwprovisioning bwallocation detailed
- show bwprovisioning bwallocation summary

BW Traffic Class Commands

- config bwprovisioning trafficclass bwallocation
- config bwprovisioning trafficclass create
- config bwprovisioning trafficclass delete
- config bwprovisioning trafficclass port
- config bwprovisioning trafficclass vlan
- config bwprovisioning trafficclass weight
- show bwprovisioning trafficclass allocatedbw
- show bwprovisioning trafficclass detailed
- show bwprovisioning trafficclass summary

Appendix E. 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 appendix contains information about where to go for additional information about IBM and IBM products, what to do if you experience a problem with your BladeCenter T unit, 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 is 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 *Hardware Maintenance Manual and Troubleshooting Guide* on the IBM *BladeCenter T Documentation* CD or in the *Hardware Maintenance Manual* at the IBM Support Web site.
- Go to the IBM Support Web site at http://www.ibm.com/pc/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 publications that are provided with your system and software. The information that comes with your system also describes the diagnostic tests that you can perform. Most xSeries and IntelliStation® systems, operating systems, and programs come with information that contains troubleshooting procedures and explanations of error messages and error codes. If you suspect a software problem, see the information for the operating system or program.

Using the documentation

Information about your IBM BladeCenter T unit and preinstalled software, if any, is available in the documentation that comes with your system. That documentation includes printed books, online books, 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/pc/support/ and follow the instructions. Also, you can order publications through the IBM Publications Ordering System at http://www.elink.ibmlink.ibm.com/public/applications/publications/cgibin/pbi.cgi.

Getting help and information from the World Wide Web

On the World Wide Web, the IBM Web site has up-to-date information about IBM xSeries and IntelliStation products, services, and support. The address for IBM xSeries information is http://www.ibm.com/eserver/xseries/. The address for IBM IntelliStation information is http://www.ibm.com/pc/intellistation/.

You can find service information for your IBM products, including supported options, at http://www.ibm.com/pc/support/.

Software service and support

Through IBM Support Line, you can get telephone assistance, for a fee, with usage, configuration, and software problems with xSeries servers, IntelliStation workstations, and appliances. For information about which products are supported by Support Line in your country or region, go to http://www.ibm.com/services/sl/products/.

For more information about Support Line and other IBM services, go to http://www.ibm.com/services/, or go to 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 IBM Services or through your IBM reseller, if your reseller is authorized by IBM to provide warranty service. Go to http://www.ibm.com/planetwide/ for support telephone numbers, or 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.

Appendix F. Notices

This information was developed for products and services offered in the U.S.A.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.

INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the products and/or the programs described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product, and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Edition notice

Trademarks

The following terms are trademarks of International Business Machines Corporation in the United States, other countries, or both:

Active Memory
Active PCI
Active PCI-X
Alert on LAN
BladeCenter
C2T Interconnect
Chipkill
EtherJet
e-business logo
@server
FlashCopy
IBM
IBM (logo)
IntelliStation
NetBAY
Netfinity
NetView
OS/2 WARP
Predictive Failure Analysis
PS/2
ServeRAID
ServerGuide
ServerProven
TechConnect
ThinkPad
Tivoli
Tivoli Enterprise
Update Connector
Wake on LAN
XA-32
XA-64
X-Architecture
XceL4
XpandOnDemand
xSeries

Intel, MMX, and Pentium are trademarks of Intel Corporation in the United States, other countries, or both.

Microsoft, Windows, and Windows NT are trademarks of Microsoft Corporation in the United States, other countries, or both.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Java and all Java-based trademarks and logos are trademarks or registered trademarks of Sun Microsystems, Inc. in the United States, other countries, or both.

Adaptec and HostRAID are trademarks of Adaptec, Inc., in the United States, other countries, or both.

Red Hat, the Red Hat “Shadow Man” logo, and all Red Hat-based trademarks and logos are trademarks or registered trademarks of Red Hat, Inc., in the United States and other countries.

Other company, product, or service names may be trademarks or service marks of others.

Important notes

Processor speeds indicate the internal clock speed of the microprocessor; other factors also affect application performance.

CD-ROM drive speeds list the variable read rate. Actual speeds vary and are often less than the maximum possible.

When referring to processor storage, real and virtual storage, or channel volume, KB stands for approximately 1000 bytes, MB stands for approximately 1 000 000 bytes, and GB stands for approximately 1 000 000 000 bytes.

When referring to hard disk drive capacity or communications volume, MB stands for 1 000 000 bytes, and GB stands for 1 000 000 000 bytes. Total user-accessible capacity may vary depending on operating environments.

Maximum internal hard disk drive capacities assume the replacement of any standard hard disk drives and population of all hard disk drive bays with the largest currently supported drives available from IBM.

Maximum memory may require replacement of the standard memory with an optional memory module.

IBM makes no representation or warranties regarding non-IBM products and services that are ServerProven®, including but not limited to the implied warranties of merchantability and fitness for a particular purpose. These products are offered and warranted solely by third parties.

IBM makes no representations or warranties with respect to non-IBM products. Support (if any) for the non-IBM products is provided by the third party, not IBM.

Some software may differ from its retail version (if available), and may not include user manuals or all program functionality.

Product recycling and disposal

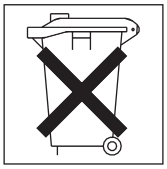
This unit contains materials such as circuit boards, cables, electromagnetic compatibility gaskets, and connectors which may contain lead and copper/beryllium alloys that require special handling and disposal at end of life. Before this unit is disposed of, these materials must be removed and recycled or discarded according to applicable regulations. IBM offers product-return programs in several countries. Information on product recycling offerings can be found on IBM's Internet site at http://www.ibm.com/ibm/environment/products/prp.shtml.

Battery return program

This product may contain a sealed lead acid, nickel cadmium, nickel metal hydride, lithium, or lithium ion battery. Consult your user manual or service manual for specific battery information. The battery must be recycled or disposed of properly. Recycling facilities may not be available in your area. For information on disposal of batteries outside the United States, go to http://www.ibm.com/ibm/environment/products/batteryrecycle.shtml or contact your local waste disposal facility.

In the United States, IBM has established a collection process for reuse, recycling, or proper disposal of used IBM sealed lead acid, nickel cadmium, nickel metal hydride, and battery packs from IBM equipment. For information on proper disposal of these batteries, contact IBM at 1-800-426-4333. Have the IBM part number listed on the battery available prior to your call.

In the Netherlands, the following applies.



Electronic emission notices

Federal Communications Commission (FCC) statement

Note: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case the user will be required to correct the interference at his own expense.

Properly shielded and grounded cables and connectors must be used in order to meet FCC emission limits. IBM is not responsible for any radio or television interference caused by using other than recommended cables and connectors or by unauthorized changes or modifications to this equipment. Unauthorized changes or modifications could void the user's authority to operate the equipment.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

Industry Canada Class A emission compliance statement

This Class A digital apparatus complies with Canadian ICES-003.

Avis de conformité à la réglementation d'Industrie Canada

Cet appareil numérique de la classe A est conforme à la norme NMB-003 du Canada.

Australia and New Zealand Class A statement

Attention: This is a Class A product. In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures.

United Kingdom telecommunications safety requirement

Notice to Customers

This apparatus is approved under approval number NS/G/1234/J/100003 for indirect connection to public telecommunication systems in the United Kingdom.

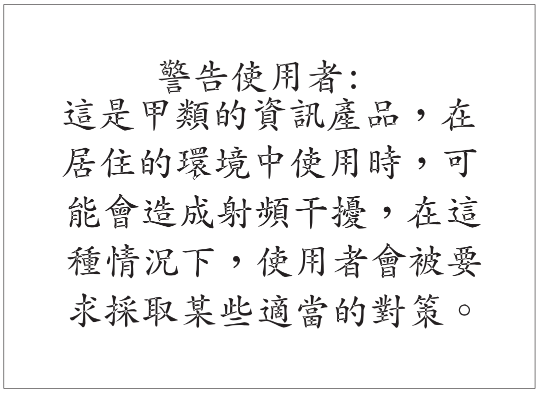
European Union EMC Directive conformance statement

This product is in conformity with the protection requirements of EU Council Directive 89/336/EEC on the approximation of the laws of the Member States relating to electromagnetic compatibility. IBM cannot accept responsibility for any failure to satisfy the protection requirements resulting from a nonrecommended modification of the product, including the fitting of non-IBM option cards.

This product has been tested and found to comply with the limits for Class A Information Technology Equipment according to CISPR 22/European Standard EN 55022. The limits for Class A equipment were derived for commercial and industrial environments to provide reasonable protection against interference with licensed communication equipment.

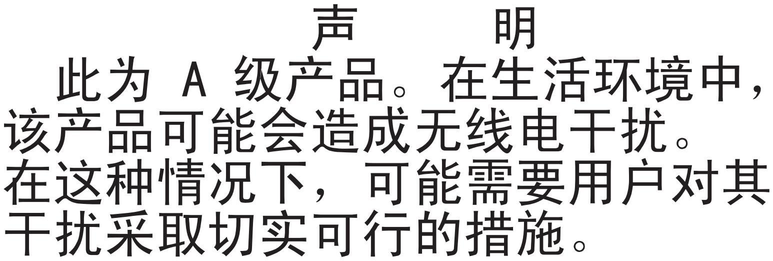
Attention: This is a Class A product. In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures.

Taiwanese Class A warning statement



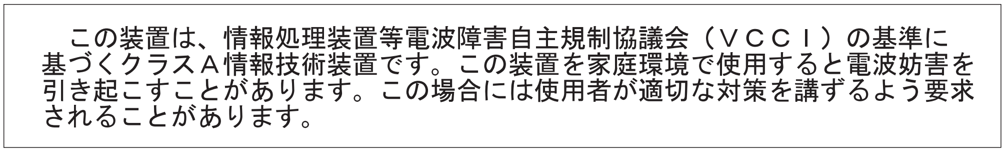
警告使用者:
這是甲類的資訊產品，在
居住的環境中使用時，可
能會造成射頻干擾，在這
種情況下，使用者會被要
求採取某些適當的對策。

Chinese Class A warning statement



声　明
此为 A 级产品。在生活环境中，
该产品可能会造成无线电干扰。
在这种情况下，可能需要用户对其
干扰采取切实可行的措施。

Japanese Voluntary Control Council for Interference (VCCI) statement



この装置は、情報処理装置等電波障害自主規制協議会（ＶＣＣＩ）の基準に
基づくクラスＡ情報技術装置です。この装置を家庭環境で使用すると電波妨害を
引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求
されることがあります。

Index

Part Number: 25K9177

Printed in USA

(1P) P/N: 25K9177