Ethernet Switch

CLI Reference Guide

Version 3.80
9/2007
Edition 1

DEFAULT LOGIN	
In-band IP Address	**http://192.168.1.1**
Out-of-band IP Address	**http://192.168.0.1**
User Name	**admin**
Password	**1234**

ZyXEL

www.zyxel.com

About This CLI Reference Guide

Intended Audience

This manual is intended for people who want to configure ZyXEL Switches via Command Line Interface (CLI). You should have at least a basic knowledge of TCP/IP networking concepts and topology.

This guide is intended as a command reference for a series of products. Therefore many commands in this guide may not be available in your product. See your User's Guide for a list of supported features and details about feature implementation.

Please refer to www.zyxel.com or your product's CD for product specific User Guides and product certifications.

How To Use This Guide

- Read the **How to Access the CLI** chapter for an overview of various ways you can get to the command interface on your Switch.
- Use the **Reference** section in this guide for command syntax, description and examples. Each chapter describes commands related to a feature.
- To find specific information in this guide, use the **Contents Overview**, the **Index of Commands**, or search the PDF file. E-mail techwriters@zyxel.com.tw if you cannot find the information you require.

CLI Reference Guide Feedback

Help us help you. Send all Reference Guide-related comments, questions or suggestions for improvement to the following address, or use e-mail instead. Thank you!

The Technical Writing Team,
ZyXEL Communications Corp.,
6 Innovation Road II,
Science-Based Industrial Park,
Hsinchu, 300, Taiwan.

E-mail: techwriters@zyxel.com.tw

Document Conventions

Warnings and Notes

These are how warnings and notes are shown in this CLI Reference Guide.

Warnings tell you about things that could harm you or your device. See your User's Guide for product specific warnings.

Notes tell you other important information (for example, other things you may need to configure or helpful tips) or recommendations.

Syntax Conventions

This manual follows these general conventions:

- ZyXEL's switches (such as the ES-2024A, ES-2108, GS-3012, and so on) may be referred to as the "Switch", the "device", the "system" or the "product" in this Reference Guide.
- Units of measurement may denote the "metric" value or the "scientific" value. For example, "k" for kilo may denote "1000" or "1024", "M" for mega may denote "1000000" or "1048576" and so on.

Command descriptions follow these conventions:

- Commands are in `courier new font`.
- Required input values are in angle brackets <>; for example, `ping <ip>` means that you must specify an IP address for this command.
- Optional fields are in square brackets []; for instance `show logins [name]`, the name field is optional.

  The following is an example of a required field within an optional field: `snmp-server [contact <system contact>]`, the `contact` field is optional. However, if you use `contact`, then you must provide the *`system contact`* information.
- Lists (such as <*`port-list`*>) consist of one or more elements separated by commas. Each element might be a single value (1, 2, 3, ...) or a range of values (1-2, 3-5, ...) separated by a dash.
- The | (bar) symbol means "or".
- *`italic`* terms represent user-defined input values; for example, in `snmp-server [contact <system contact>]`, *`system contact`* can be replaced by the administrator's name.
- A key stroke is denoted by square brackets and uppercase text, for example, [ENTER] means the "Enter" or "Return" key on your keyboard.

- <cr> means press the [ENTER] key.
- An arrow (-->) indicates that this line is a continuation of the previous line.

Command summary tables are organized as follows:

Table 1 Example: Command Summary Table

COMMAND	DESCRIPTION	M	P
show vlan	Displays the status of all VLANs.	E	3
vlan <1-4094>	Enters config-vlan mode for the specified VLAN. Creates the VLAN, if necessary.	C	13
inactive	Disables the specified VLAN.	C	13
no inactive	Enables the specified VLAN.	C	13
no vlan <1-4094>	Deletes a VLAN.	C	13

The **Table** title identifies commands or the specific feature that the commands configure.

The **COMMAND** column shows the syntax of the command.

- If a command is not indented, you run it in the enable or config mode. See Chapter 2 on page 15 for more information on command modes.
- If a command is indented, you run it in a sub-command mode.

The **DESCRIPTION** column explains what the command does. It also identifies legal input values, if necessary.

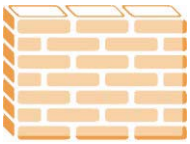
The **M** column identifies the mode in which you run the command.

- **E**: The command is available in enable mode. It is also available in user mode if the privilege level (**P**) is less than 13.
- **C**: The command is available in config (not indented) or one of the sub-command modes (indented).

The **P** column identifies the privilege level of the command. If you don't have a high enough privilege level you may not be able to view or execute some of the commands. See Chapter 2 on page 15 for more information on privilege levels.

Icons Used in Figures

Figures in this guide may use the following generic icons. The Switch icon is not an exact representation of your device.

Switch 	Computer 	Notebook computer 
Server 	DSLAM 	Firewall 
Telephone 	Switch 	Router 

Contents Overview

PART I
Introduction

1

How to Access and Use the CLI

This chapter introduces the command line interface (CLI).

1.1 Accessing the CLI

Use any of the following methods to access the CLI.

1.1.1 Console Port

1. Connect your computer to the console port on the Switch using the appropriate cable.
2. Use terminal emulation software with the following settings:

Table 2 Default Settings for the Console Port

SETTING	DEFAULT VALUE
Terminal Emulation	VT100
Baud Rate	9600 bps
Parity	None
Number of Data Bits	8
Number of Stop Bits	1
Flow Control	None

3. Press [ENTER] to open the login screen.

1.1.2 Telnet

1. Connect your computer to one of the Ethernet ports.
2. Open a Telnet session to the Switch's IP address. If this is your first login, use the default values.

Table 3 Default Management IP Address

SETTING	DEFAULT VALUE
IP Address	192.168.1.1
Subnet Mask	255.255.255.0

Make sure your computer IP address is in the same subnet, unless you are accessing the Switch through one or more routers.

1.1.3 SSH

1. Connect your computer to one of the Ethernet ports.
2. Use a SSH client program to access the Switch. If this is your first login, use the default values in Table 3 on page 11 and Table 4 on page 12. Make sure your computer IP address is in the same subnet, unless you are accessing the Switch through one or more routers.

1.2 Logging in

Use the administrator username and password. If this is your first login, use the default values.

Table 4 Default User Name and Password

SETTING	DEFAULT VALUE
User Name	admin
Password	1234

The Switch automatically logs you out of the management interface after five minutes of inactivity. If this happens to you, simply log back in again.

1.3 Using Shortcuts and Getting Help

This table identifies some shortcuts in the CLI, as well as how to get help.

Table 5 CLI Shortcuts and Help

COMMAND / KEY(S)	DESCRIPTION
`history`	Displays a list of recently-used commands.
↑↓ `(up/down arrow keys)`	Scrolls through the list of recently-used commands. You can edit any command or press `[ENTER]` to run it again.
`[CTRL]+U`	Clears the current command.
`[TAB]`	Auto-completes the keyword you are typing if possible. For example, type `config`, and press `[TAB]`. The Switch finishes the word `configure`.
`?`	Displays the keywords and/or input values that are allowed in place of the `?`.
`help`	Displays the (full) commands that are allowed in place of `help`.

1.4 Saving Your Configuration

When you run a command, the Switch saves any changes to its run-time memory. The Switch loses these changes if it is turned off or loses power. Use the `write memory` command in enable mode to save the current configuration permanently to non-volatile memory.

```
sysname# write memory
```

You should save your changes after each CLI session. All unsaved configuration changes are lost once you restart the Switch.

1.5 Logging Out

Enter `logout` to log out of the CLI. You have to be in user, enable, or config mode. See Chapter 2 on page 15 for more information about modes.

2

Privilege Level and Command Mode

This chapter introduces the CLI privilege levels and command modes.

- The privilege level determines whether or not a user can run a particular command.
- If a user can run a particular command, the user has to run it in the correct mode.

2.1 Privilege Levels

Every command has a privilege level (0-14). Users can run a command if the session's privilege level is greater than or equal to the command's privilege level. The session's privilege level initially comes from the login account's privilege level, though it is possible to change the session's privilege level after logging in.

2.1.1 Privilege Levels for Commands

The privilege level of each command is listed in the Reference A-G chapters on page 25.

At the time of writing, commands have a privilege level of 0, 3, 13, or 14. The following table summarizes the types of commands at each of these privilege levels.

Table 6 Types of Commands at Different Privilege Levels

PRIVILEGE LEVEL	TYPES OF COMMANDS AT THIS PRIVILEGE LEVEL
0	Display basic system information.
3	Display configuration or status.
13	Configure features except for login accounts, the authentication method sequence, multiple logins, and administrator and enable passwords.
14	Configure login accounts, the authentication method sequence, multiple logins, and administrator and enable passwords.

2.1.2 Privilege Levels for Login Accounts

You can manage the privilege levels for login accounts in the following ways:

- Using commands. Login accounts can be configured by the **admin** account or any login account with a privilege level of 14. See Chapter 29 on page 111.
- Using vendor-specific attributes in an external authentication server. See the User's Guide for more information.

The **admin** account has a privilege level of 14, so the administrator can run every command. You cannot change the privilege level of the **admin** account.

2.1.3 Privilege Levels for Sessions

The session's privilege level initially comes from the privilege level of the login account the user used to log in to the Switch. After logging in, the user can use the following commands to change the session's privilege level.

2.1.3.1 enable Command

This command raises the session's privilege level to 14. It also changes the session to enable mode (if not already in enable mode). This command is available in user mode or enable mode, and users have to know the enable password.

In the following example, the login account **user0** has a privilege level of 0 but knows that the enable password is **123456**. Afterwards, the session's privilege level is 14, instead of 0, and the session changes to enable mode.

```
sysname> enable
Password: 123456
sysname#
```

The default enable password is **1234**. Use this command to set the enable password.

```
password <password>
```

<password> consists of 1-32 alphanumeric characters. For example, the following command sets the enable password to **123456**. See Chapter 68 on page 215 for more information about this command.

```
sysname(config)# password 123456
```

2.1.3.2 enable <0-14> Command

This command raises the session's privilege level to the specified level. It also changes the session to enable mode, if the specified level is 13 or 14. This command is available in user mode or enable mode, and users have to know the password for the specified privilege level.

In the following example, the login account **user0** has a privilege level of 0 but knows that the password for privilege level 13 is **pswd13**. Afterwards, the session's privilege level is 13, instead of 0, and the session changes to enable mode.

```
sysname> enable 13
Password: pswd13
sysname#
```

Users cannot use this command until you create passwords for specific privilege levels. Use the following command to create passwords for specific privilege levels.

```
password <password> privilege <0-14>
```

<*password*> consists of 1-32 alphanumeric characters. For example, the following command sets the password for privilege level 13 to **pswd13**. See Chapter 68 on page 215 for more information about this command.

```
sysname(config)# password pswd13 privilege 13
```

2.1.3.3 disable Command

This command reduces the session's privilege level to 0. It also changes the session to user mode. This command is available in enable mode.

2.2 Command Modes

The CLI is divided into several modes. If a user has enough privilege to run a particular command, the user has to run the command in the correct mode. The modes that are available depend on the session's privilege level.

2.2.1 Command Modes for Privilege Levels 0-12

If the session's privilege level is 0-12, the user and all of the allowed commands are in user mode. Users do not have to change modes to run any allowed commands.

2.2.2 Command Modes for Privilege Levels 13-14

If the session's privilege level is 13-14, the allowed commands are in one of several modes.

Table 7 Command Modes for Privilege Levels 13-14 and the Types of Commands in Each One

MODE	PROMPT	COMMAND FUNCTIONS IN THIS MODE
enable	`sysname#`	Display current configuration, diagnostics, maintenance.
config	`sysname(config)#`	Configure features other than those below.
config-interface	`sysname(config-interface)#`	Configure ports.
config-interface	`sysname(config-interface)#`	Configure ports.
config-mvr	`sysname(config-mvr)#`	Configure multicast VLAN.
config-route-domain	`sysname(config-if)#`	Enable and enter configuration mode for an IP routing domain.
config-dvmrp	`sysname(config-dvmrp)#`	Configure Distance Vector Multicast Routing Protocol (DVRMP).
config-igmp	`sysname(config-igmp)#`	Configure Internet Group Management Protocol (IGMP).
config-ospf	`sysname(config-ospf)#`	Configure Open Shortest Path First (OSPF) protocol.
config-rip	`sysname(config-rip)#`	Configure Routing Information Protocol (RIP).
config-vrrp	`sysname(config-vrrp)#`	Configure Virtual Router Redundancy Protocol (VRRP).

Each command is usually in one and only one mode. If a user wants to run a particular command, the user has to change to the appropriate mode. The command modes are organized like a tree, and users start in enable mode. The following table explains how to change from one mode to another.

Table 8 Changing Between Command Modes for Privilege Levels 13-14

MODE	ENTER MODE	LEAVE MODE
enable	--	--
config	`configure`	exit
config-interface	`interface port-channel <port-list>`	exit
config-mvr	`mvr <1-4094>`	exit
config-vlan	`vlan <1-4094>`	exit
config-route-domain	`interface route domain <ip-address>/<mask-bits>`	exit
config-dvmrp	`router dvmrp`	exit
config-igmp	`router igmp`	exit
config-ospf	`router ospf <router-id>`	exit
config-rip	`router rip`	exit
config-vrrp	`router vrrp network <ip-address>/<mask-bits> vr-id <1~7> uplink-gateway <ip-address>`	exit

2.3 Listing Available Commands

Use the `help` command to view the executable commands on the Switch. You must have the highest privilege level in order to view all the commands. Follow these steps to create a list of supported commands:

1. Log into the CLI. This takes you to the enable mode.
2. Type `help` and press [ENTER]. A list comes up which shows all the commands available in enable mode. The example shown next has been edited for brevity's sake.

```
sysname# help
  Commands available:

  help
  logout
  exit
  history
  enable <0-14>
  enable <cr>  traceroute <ip|host-name> [vlan <vlan-id>][..]
  .
  .
  traceroute help
  ssh <1|2> <[user@]dest-ip> <cr>
  ssh <1|2> <[user@]dest-ip> [command </>]
sysname#
```

3. Copy and paste the results into a text editor of your choice. This creates a list of all the executable commands in the user and enable modes.
4. Type `configure` and press [ENTER]. This takes you to the config mode.
5. Type `help` and press [ENTER]. A list is displayed which shows all the commands available in config mode and all the sub-commands. The sub-commands are preceded by the command necessary to enter that sub-command mode. For example, the command `name <name-str>` as shown next, is preceded by the command used to enter the config-vlan sub-mode: `vlan <1-4094>`.

```
sysname# help
 .
 .
 no arp inspection log-buffer logs
 no arp inspection filter-aging-time
 no arp inspection <cr>
 vlan <1-4094>
 vlan <1-4094> name <name-str>
 vlan <1-4094> normal <port-list>
 vlan <1-4094> fixed <port-list>
```

6. Copy and paste the results into a text editor of your choice. This creates a list of all the executable commands in config and the other submodes, for example, the config-vlan mode.

3

Initial Setup

This chapter identifies tasks you might want to do when you first configure the Switch.

3.1 Changing the Administrator Password

It is recommended you change the default administrator password.

Use this command to change the administrator password.

`admin-password <pw-string> <Confirm-string>`

where <*pw-string*> may be 1-32 alphanumeric characters long.

```
sysname# configure
sysname(config)# admin-password t1g2y7i9 t1g2y7i9
```

3.2 Changing the Enable Password

It is recommended you change the default enable password.

Use this command to change the enable password.

`password <password>`

where <*password*> may be 1-32 alphanumeric characters long.

```
sysname# configure
sysname(config)# password k8s8s3dl0
```

3.3 Prohibiting Concurrent Logins

By default, multiple CLI sessions are allowed via the console port or Telnet. See the User's Guide for the maximum number of concurrent sessions for your Switch. Use this command to prohibit concurrent logins.

```
no multi-login
```

Console port has higher priority than Telnet. See Chapter 38 on page 131 for more `multi-login` commands.

```
sysname# configure
sysname(config)# no multi-login
```

3.4 Changing the Management IP Address

The Switch has a different IP address in each VLAN. By default, the Switch has VLAN 1 with IP address 192.168.1.1 and subnet mask 255.255.255.0. Use this command in config-vlan mode to change the management IP address in a specific VLAN.

```
ip address <ip> <mask>
```

This example shows you how to change the management IP address in VLAN 1 to 172.16.0.1 with subnet mask 255.255.255.0.

```
sysname# configure
sysname(config)# vlan 1
sysname(config-vlan)# ip address 172.16.0.1 255.255.255.0
```

Afterwards, you have to use the new IP address to access the Switch.

3.5 Changing the Out-of-band Management IP Address

If your Switch has a **MGMT** port (also referred to as the out-of-band management port), then the Switch can also be managed via this interface. By default, the **MGMT** port IP address is 192.168.0.1 and the subnet mask is 255.255.255.0. Use this command in config mode to change the out-of-band management IP address.

```
ip address <ip> <mask>
```

This example shows you how to change the out-of-band management IP address to 10.10.10.1 with subnet mask 255.255.255.0 and the default gateway 10.10.10.254

```
sysname# configure
sysname(config)# ip address 10.10.10.1 255.255.255.0
sysname(config)# ip address default-gateway 10.10.10.254
```

3.6 Looking at Basic System Information

Use this command to look at general system information about the Switch.

```
show system-information
```

This is illustrated in the following example.

```
sysname# show system-information

System Name              : sysname
System Contact           :
System Location          :
Ethernet Address         : 00:13:49:ae:fb:7a
ZyNOS F/W Version        : V3.80(AII.0)b0 | 04/18/2007
RomRasSize               : 1746416
System up Time           :   280:32:52 (605186d ticks)
Bootbase Version         : V1.00 | 05/17/2006
ZyNOS CODE               : RAS Apr 18 2007 19:59:49
Product Model            : ES-2024PWR
```

See Chapter 68 on page 215 for more information about these attributes.

3.7 Looking at the Operating Configuration

Use this command to look at the current operating configuration.

```
show running-config
```

This is illustrated in the following example.

```
sysname# show running-config
  Building configuration...

  Current configuration:

vlan 1
  name 1
  normal ""
  fixed 1-9
  forbidden ""
  untagged 1-9
  ip address default-management 172.16.37.206 255.255.255.0
  ip address default-gateway 172.16.37.254
exit
```

PART II
Reference A-G

4

AAA Commands

Use these commands to configure authentication and accounting on the Switch.

4.1 Command Summary

The following section lists the commands for this feature.

Table 9 aaa authentication Command Summary

COMMAND	DESCRIPTION	M	P
`show aaa authentication`	Displays what methods are used for authentication.	E	3
`show aaa authentication enable`	Displays the authentication method(s) for checking privilege level of administrators.	E	3
`aaa authentication enable <method1> [<method2> ...]`	Specifies which method should be used first, second, and third for checking privileges. *method*: `enable`, `radius`, or `tacacs+`.	C	14
`no aaa authentication enable`	Resets the method list for checking privileges to its default value.	C	14
`show aaa authentication login`	Displays the authentication methods for administrator login accounts.	E	3
`aaa authentication login <method1> [<method2> ...]`	Specifies which method should be used first, second, and third for the authentication of login accounts. *method*: `local`, `radius`, or `tacacs+`.	C	14
`no aaa authentication login`	Resets the method list for the authentication of login accounts to its default value.	C	14

Table 10 Command Summary: aaa accounting

COMMAND	DESCRIPTION	M	P
`show aaa accounting`	Displays accounting settings configured on the Switch.	E	3
`show aaa accounting update`	Display the update period setting on the Switch for accounting sessions.	E	3
`aaa accounting update periodic <1-2147483647>`	Sets the update period (in minutes) for accounting sessions. This is the time the Switch waits to send an update to an accounting server after a session starts.	C	13
`no aaa accounting update`	Resets the accounting update interval to the default value.	C	13
`show aaa accounting commands`	Displays accounting settings for recording command events.	E	3
`aaa accounting commands <privilege> stop-only tacacs+ [broadcast]`	Enables accounting of command sessions and specifies the minimum privilege level (0-14) for the command sessions that should be recorded. Optionally, sends accounting information for command sessions to all configured accounting servers at the same time.	C	13

Table 10 Command Summary: aaa accounting (continued)

COMMAND	DESCRIPTION	M	P
`no aaa accounting commands`	Disables accounting of command sessions on the Switch.	C	13
`show aaa accounting dot1x`	Displays accounting settings for recording IEEE 802.1x session events.	E	3
`aaa accounting dot1x <start-stop|stop-only> <radius|tacacs+> [broadcast]`	Enables accounting of IEEE 802.1x authentication sessions and specifies the mode and protocol method. Optionally, sends accounting information for IEEE 802.1x authentication sessions to all configured accounting servers at the same time.	C	13
`no aaa accounting dot1x`	Disables accounting of IEEE 802.1x authentication sessions on the Switch.	C	13
`show aaa accounting exec`	Displays accounting settings for recording administrative sessions via SSH, Telnet or the console port.	E	3
`aaa accounting exec <start-stop|stop-only> <radius|tacacs+> [broadcast]`	Enables accounting of administrative sessions via SSH, Telnet and console port and specifies the mode and protocol method. Optionally, sends accounting information for administrative sessions via SSH, Telnet and console port to all configured accounting servers at the same time.	C	13
`no aaa accounting exec`	Disables accounting of administrative sessions via SSH, Telnet or console on the Switch.	C	13
`show aaa accounting system`	Displays accounting settings for recording system events, for example system shut down, start up, accounting enabled or accounting disabled.	E	3
`aaa accounting system <radius|tacacs+> [broadcast]`	Enables accounting of system events and specifies the protocol method. Optionally, sends accounting information for system events to all configured accounting servers at the same time.	C	13
`no aaa accounting system`	Disables accounting of system events on the Switch.	C	13

5

ARP Commands

Use these commands to look at IP-to-MAC address mapping(s).

5.1 Command Summary

The following section lists the commands for this feature.

Table 11 arp Command Summary

COMMAND	DESCRIPTION	M	P
`show ip arp`	Displays the ARP table.	E	3
`no arp`	Flushes the ARP table entries.	E	13

5.2 Command Examples

This example shows the ARP table.

```
sysname# show ip arp
  Index    IP               MAC                VLAN  Age(s)  Type
     1     172.16.37.254    00:04:80:9b:78:00     1   300     dynamic
```

The following table describes the labels in this screen.

Table 12 show ip arp

LABEL	DESCRIPTION
Index	This field displays the index number.
IP	This field displays the learned IP address of the device.
MAC	This field displays the MAC address of the device.
VLAN	This field displays the VLAN to which the device belongs.
Age(s)	This field displays how long the entry remains valid.
Type	This field displays how the entry was learned. **dynamic**: The Switch learned this entry from ARP packets.

6

ARP Inspection Commands

Use these commands to filter unauthorized ARP packets in your network.

6.1 Command Summary

The following section lists the commands for this feature.

Table 13 arp inspection Command Summary

COMMAND	DESCRIPTION	M	P
`show arp inspection`	Displays ARP inspection configuration details.	E	3
`arp inspection`	Enables ARP inspection on the Switch. You still have to enable ARP inspection on specific VLAN and specify trusted ports.	C	13
`no arp inspection`	Disables ARP inspection on the Switch.	C	13

Table 14 Command Summary: arp inspection filter

COMMAND	DESCRIPTION	M	P
`show arp inspection filter [<mac-addr>] [vlan <vlan-id>]`	Displays the current list of MAC address filters that were created because the Switch identified an unauthorized ARP packet. Optionally, lists MAC address filters based on the MAC address or VLAN ID in the filter.	E	3
`no arp inspection filter <mac-addr> vlan <vlan-id>`	Specifies the ARP inspection record you want to delete from the Switch. The ARP inspection record is identified by the MAC address and VLAN ID pair.	E	13
`clear arp inspection filter`	Delete all ARP inspection filters from the Switch.	E	13
`arp inspection filter-aging-time <1-2147483647>`	Specifies how long (1-2147483647 seconds) MAC address filters remain in the Switch after the Switch identifies an unauthorized ARP packet. The Switch automatically deletes the MAC address filter afterwards.	C	13
`arp inspection filter-aging-time none`	Specifies the MAC address filter to be permanent.	C	13
`no arp inspection filter-aging-time`	Resets how long (1-2147483647 seconds) the MAC address filter remains in the Switch after the Switch identifies an unauthorized ARP packet to the default value.	C	13

Table 15 Command Summary: arp inspection log

COMMAND	DESCRIPTION	M	P
`show arp inspection log`	Displays the log settings configured on the Switch. It also displays the log entries recorded on the Switch.	E	3
`clear arp inspection log`	Delete all ARP inspection log entries from the Switch.	E	13

Table 15 Command Summary: arp inspection log (continued)

COMMAND	DESCRIPTION	M	P
`arp inspection log-buffer entries <0-1024>`	Specifies the maximum number (1-1024) of log messages that can be generated by ARP packets and not sent to the syslog server. If the number of log messages in the Switch exceeds this number, the Switch stops recording log messages and simply starts counting the number of entries that were dropped due to unavailable buffer.	C	13
`arp inspection log-buffer logs <0-1024> interval <0-86400>`	Specifies the number of syslog messages that can be sent to the syslog server in one batch and how often (1-86400 seconds) the Switch sends a batch of syslog messages to the syslog server.	C	13
`no arp inspection log-buffer entries`	Resets the maximum number (1-1024) of log messages that can be generated by ARP packets and not sent to the syslog server to the default value.	C	13
`no arp inspection log-buffer logs`	Resets the maximum number of syslog messages the Switch can send to the syslog server in one batch to the default value.	C	13

Table 16 Command Summary: interface arp inspection

COMMAND	DESCRIPTION	M	P
`show arp inspection interface port-channel <port-list>`	Displays the ARP inspection settings for the specified port(s).	E	3
`interface port-channel <port-list>`	Enters config-interface mode for the specified port(s).	C	13
`arp inspection trust`	Sets the port to be a trusted port for arp inspection. The Switch does not discard ARP packets on trusted ports for any reason.	C	13
`no arp inspection trust`	Disables this port from being a trusted port for ARP inspection.	C	13

Table 17 Command Summary: arp inspection vlan

COMMAND	DESCRIPTION	M	P
`show arp inspection vlan <vlan-list>`	Displays ARP inspection settings for the specified VLAN(s).	E	3
`arp inspection vlan <vlan-list>`	Enables ARP inspection on the specified VLAN(s).	C	13
`no arp inspection vlan <vlan-list>`	Disables ARP inspection on the specified VLAN(s).	C	13
`arp inspection vlan <vlan-list> logging [all|none|permit|deny]`	Enables logging of ARP inspection events on the specified VLAN(s). Optionally specifies which types of events to log.	C	13
`no arp inspection vlan <vlan-list> logging`	Disables logging of messages generated by ARP inspection for the specified VLAN(s).	C	13

6.2 Command Examples

This example looks at the current list of MAC address filters that were created because the Switch identified an unauthorized ARP packet. When the Switch identifies an unauthorized ARP packet, it automatically creates a MAC address filter to block traffic from the source MAC address and source VLAN ID of the unauthorized ARP packet.

```
sysname# show arp inspection filter
  Filtering aging timeout : 300

         MacAddress  VLAN   Port  Expiry (sec)          Reason
  -----------------  ----  -----  ------------  --------------
  Total number of bindings: 0
```

The following table describes the labels in this screen.

Table 18 show arp inspection filter

LABEL	DESCRIPTION
Filtering aging timeout	This field displays how long the MAC address filters remain in the Switch after the Switch identifies an unauthorized ARP packet. The Switch automatically deletes the MAC address filter afterwards.
MacAddress	This field displays the source MAC address in the MAC address filter.
VLAN	This field displays the source VLAN ID in the MAC address filter.
Port	This field displays the source port of the discarded ARP packet.
Expiry (sec)	This field displays how long (in seconds) the MAC address filter remains in the Switch. You can also delete the record manually (**Delete**).
Reason	This field displays the reason the ARP packet was discarded. **MAC+VLAN**: The MAC address and VLAN ID were not in the binding table. **IP**: The MAC address and VLAN ID were in the binding table, but the IP address was not valid. **Port**: The MAC address, VLAN ID, and IP address were in the binding table, but the port number was not valid.

This example looks at log messages that were generated by ARP packets and that have not been sent to the syslog server yet.

```
sysname# show arp inspection log
  Total Log Buffer Size : 32
  Syslog rate : 5 entries per 1 seconds

  Port  Vlan         Sender MAC        Sender IP  Pkts      Reason
         Time
  ----  ----  -----------------  ---------------  ----  ----------  ----
---------------------
  Total number of logs: 0
```

The following table describes the labels in this screen.

Table 19 show arp inspection log

LABEL	DESCRIPTION
Total Log Buffer Size	This field displays the maximum number (1-1024) of log messages that were generated by ARP packets and have not been sent to the syslog server yet. If the number of log messages in the Switch exceeds this number, the Switch stops recording log messages and simply starts counting the number of entries that were dropped due to unavailable buffer.
Syslog rate	This field displays the maximum number of syslog messages the Switch can send to the syslog server in one batch. This number is expressed as a rate because the batch frequency is determined by the **Log Interval**.
Port	This field displays the source port of the ARP packet.
Vlan	This field displays the source VLAN ID of the ARP packet.
Sender MAC	This field displays the source MAC address of the ARP packet.
Sender IP	This field displays the source IP address of the ARP packet.
Pkts	This field displays the number of ARP packets that were consolidated into this log message. The Switch consolidates identical log messages generated by ARP packets in the log consolidation interval into one log message.
Reason	This field displays the reason the log message was generated. **static deny**: An ARP packet was discarded because it violated a static binding with the same MAC address and VLAN ID. **deny**: An ARP packet was discarded because there were no bindings with the same MAC address and VLAN ID. **static permit**: An ARP packet was forwarded because it matched a static binding.
Time	This field displays when the log message was generated.
Total number of logs	This field displays the number of log messages that were generated by ARP packets and that have not been sent to the syslog server yet. If one or more log messages are dropped due to unavailable buffer, there is an entry called **overflow** with the current number of dropped log messages.

This example displays whether ports are trusted or untrusted ports for ARP inspection.

```
sysname# show arp inspection interface port-channel 1
Interface  Trusted State  Rate (pps)  Burst Interval
---------  -------------  ----------  --------------
        1      Untrusted          15               1
```

The following table describes the labels in this screen.

Table 20 show arp inspection interface port-channel

LABEL	DESCRIPTION
Interface	This field displays the port number. If you configure the * port, the settings are applied to all of the ports.
Trusted State	This field displays whether this port is a trusted port (**Trusted**) or an untrusted port (**Untrusted**). Trusted ports are connected to DHCP servers or other switches, and the switch discards DHCP packets from trusted ports only if the rate at which DHCP packets arrive is too high.

Table 20 show arp inspection interface port-channel (continued)

LABEL	DESCRIPTION
Rate (pps)	This field displays the maximum number for DHCP packets that the switch receives from each port each second. The switch discards any additional DHCP packets.
Burst Interval	This field displays the length of time over which the rate of ARP packets is monitored for each port. For example, if the Rate is 15 pps and the burst interval is 1 second, then the switch accepts a maximum of 15 ARP packets in every one-second interval. If the burst interval is 5 seconds, then the switch accepts a maximum of 75 ARP packets in every five-second interval.

7

Bandwidth Commands

Use these commands to configure the maximum allowable bandwidth for incoming or outgoing traffic flows on a port.

Bandwidth management implementation differs across Switch models.

- Some models use a single command (`bandwidth-limit ingress`) to control the incoming rate of traffic on a port.
- Other models use two separate commands (`bandwidth-limit cir` and `bandwidth-limit pir`) to control the Committed Information Rate (CIR) and the Peak Information Rate (PIR) allowed on a port.

  The CIR and PIR should be set for all ports that use the same uplink bandwidth. If the CIR is reached, packets are sent at the rate up to the PIR. When network congestion occurs, packets through the ingress port exceeding the CIR will be marked for drop.

The CIR should be less than the PIR.

See Section 7.2 on page 38 and Section 7.3 on page 39 for examples.

See also Chapter 61 on page 197 for information on how to use trTCM (Two Rate Three Color Marker) to control traffic flow.

7.1 Command Summary

The following table describes user-input values available in multiple commands for this feature.

Table 21 User-input Values: running-config

COMMAND	DESCRIPTION
port-list	The port number or a range of port numbers that you want to configure.
rate	The rate represents a bandwidth limit. Different models support different rate limiting incremental steps. See your User's Guide for more information.

The following section lists the commands for this feature.

Table 22 Command Summary: bandwidth-control & bandwidth-limit

COMMAND	DESCRIPTION	M	P
`show interfaces config <port-list> bandwidth-control`	Displays the current settings for interface bandwidth control.	E	3
`bandwidth-control`	Enables bandwidth control on the Switch.	C	13
`no bandwidth-control`	Disables bandwidth control on the Switch.	C	13
`interface port-channel <port-list>`	Enters subcommand mode for configuring the specified ports.	C	13
`bandwidth-limit ingress`	Enables bandwidth limits for incoming traffic on the port(s).	C	13
`bandwidth-limit ingress <rate>`	Sets the maximum bandwidth allowed for incoming traffic on the port(s).	C	13
`bandwidth-limit egress`	Enables bandwidth limits for outgoing traffic on the port(s).	C	13
`bandwidth-limit egress <rate>`	Sets the maximum bandwidth allowed for outgoing traffic on the port(s).	C	13
`no bandwidth-limit ingress`	Disables ingress bandwidth limits on the specified port(s).	C	13
`no bandwidth-limit egress`	Disables egress bandwidth limits on the specified port(s).	C	13
`bandwidth-limit cir`	Enables commit rate limits on the specified port(s).	C	13
`bandwidth-limit cir <rate>`	Sets the guaranteed bandwidth allowed for the incoming traffic flow on a port. The commit rate should be less than the peak rate. The sum of commit rates cannot be greater than or equal to the uplink bandwidth. Note: The sum of CIRs cannot be greater than or equal to the uplink bandwidth.	C	13
`bandwidth-limit pir`	Enables peak rate limits on the specified port(s).	C	13
`bandwidth-limit pir <rate>`	Sets the maximum bandwidth allowed for the incoming traffic flow on the specified port(s).	C	13
`no bandwidth-limit cir`	Disables commit rate limits on the specified port(s).	C	13
`no bandwidth-limit pir`	Disables peak rate limits on the specified port(s).	C	13

7.2 Command Examples: ingress

This example sets the outgoing traffic bandwidth limit to 5000 Kbps and the incoming traffic bandwidth limit to 4000 Kbps for port 1.

```
sysname# configure
sysname(config)# bandwidth-control
sysname(config)# interface port-channel 1
sysname(config-interface)# bandwidth-limit egress 5000
sysname(config-interface)# bandwidth-limit ingress 4000
sysname(config-interface)# exit
sysname(config)# exit
```

This example deactivates the outgoing bandwidth limit on port 1.

```
sysname# configure
sysname(config)# interface port-channel 1
sysname(config-interface)# no bandwidth-limit egress
sysname(config-interface)# exit
sysname(config)# exit
```

7.3 Command Examples: cir & pir

This example sets the guaranteed traffic bandwidth limit on port 1 to 4000 Kbps and the maximum traffic bandwidth limit to 5000 Kbps for port 1.

```
sysname# configure
sysname(config)# bandwidth-control
sysname(config)# interface port-channel 1
sysname(config-interface)# bandwidth-limit cir
sysname(config-interface)# bandwidth-limit cir 4000
sysname(config-interface)# bandwidth-limit pir
sysname(config-interface)# bandwidth-limit pir 5000
sysname(config-interface)# exit
sysname(config)# exit
```

This example displays the bandwidth limits configured on port 1.

```
sysname# show running-config interface port-channel 1 bandwidth-limit
  Building configuration...

  Current configuration:

interface port-channel 1
  bandwidth-limit cir 4000
  bandwidth-limit cir
  bandwidth-limit pir 5000
  bandwidth-limit pir
```

8

Broadcast Storm Commands

Use these commands to limit the number of broadcast, multicast and destination lookup failure (DLF) packets the Switch receives per second on the ports.

Broadcast storm control implementation differs across Switch models.

- Some models use a single command (`bmstorm-limit`) to control the combined rate of broadcast, multicast and DLF packets accepted on Switch ports.
- Other models use three separate commands (`broadcast-limit`, `multicast-limit`, `dlf-limit`) to control the number of individual types of packets accepted on Switch ports.

See Section 8.2 on page 42 and Section 8.3 on page 42 for examples.

8.1 Command Summary

The following table describes user-input values available in multiple commands for this feature.

Table 23 User-input Values: broadcast-limit, multicast-limit & dlf-limit

COMMAND	DESCRIPTION
pkt/s	Specifies the maximum number of packets per second accepted by a Switch port.

The following section lists the commands for this feature.

Table 24 Command Summary: storm-control, bmstorm-limit, and bstorm-control

COMMAND	DESCRIPTION	M	P
`show interfaces config <port-list> bstorm-control`	Displays the current settings for broadcast storm control.	E	3
`storm-control`	Enables broadcast storm control on the Switch.	C	13
`no storm-control`	Disables broadcast storm control on the Switch.	C	13
`interface port-channel <port-list>`	Enters subcommand mode for configuring the specified ports.	C	13
`bmstorm-limit`	Enables broadcast storm control on the specified port(s).	C	13

Table 24 Command Summary: storm-control, bmstorm-limit, and bstorm-control (continued)

COMMAND	DESCRIPTION	M	P
bmstorm-limit <*rate*>	Specifies the maximum rate at which the Switch receives broadcast, multicast, and destination lookup failure (DLF) packets on the specified port(s). Different models support different rate limiting incremental steps. See your User's Guide for more information.	C	13
no bmstorm-limit	Disables broadcast storm control on the specified port(s).	C	13
broadcast-limit	Enables the broadcast packet limit on the specified port(s).	C	13
broadcast-limit <*pkt/s*>	Specifies the maximum number of broadcast packets the Switch accepts per second on the specified port(s).	C	13
no broadcast-limit	Disables broadcast packet limit no the specified port(s).	C	13
multicast-limit	Enables the multicast packet limit on the specified port(s).	C	13
multicast-limit <*pkt/s*>	Specifies the maximum number of multicast packets the Switch accepts per second on the specified port(s).	C	13
no multicast-limit	Disables multicast packet limit on the specified port(s).	C	13
dlf-limit	Enables the DLF packet limit on the specified port(s).	C	13
dlf-limit <*pkt/s*>	Specifies the maximum number of DLF packets the Switch accepts per second on the specified port(s).	C	13
no dlf-limit	Disables DLF packet limits no the specified port(s).	C	13

8.2 Command Example: bmstorm-limit

This example enables broadcast storm control on port **1** and limits the combined maximum rate of broadcast, multicast and DLF packets to **128** Kbps.

```
sysname# configure
sysname(config)# storm-control
sysname(config)# interface port-channel 1
sysname(config-interface)# bmstorm-limit
sysname(config-interface)# bmstorm-limit 128
sysname(config-interface)# exit
sysname(config)# exit
```

8.3 Command Example: broadcast-limit, multicast-limit & dlf-limit

This example enables broadcast storm control on the Switch, and configures port **1** to accept up to:

- **128** broadcast packets per second,
- **256** multicast packets per second,

- **64** DLF packets per second.

```
sysname# configure
sysname(config)# storm-control
sysname(config)# interface port-channel 1
sysname(config-interface)# broadcast-limit
sysname(config-interface)# broadcast-limit 128
sysname(config-interface)# multicast-limit
sysname(config-interface)# multicast-limit 256
sysname(config-interface)# dlf-limit
sysname(config-interface)# dlf-limit 64
sysname(config)# exit
sysname# show interfaces config 1 bstorm-control
  Broadcast Storm Control Enabled: Yes

  Port    Broadcast|Enabled     Multicast|Enabled     DLF-Limit|Enabled
     1    128 pkt/s|Yes         256 pkt/s|Yes           64 pkt/s|Yes
```

9

Classifier Commands

Use these commands to classify packets into traffic flows. After classifying traffic, `policy` commands (Chapter 43 on page 147) can be used to ensure that a traffic flow gets the requested treatment in the network.

9.1 Command Summary

The following section lists the commands for this feature.

Table 25 Command Summary: classifier

COMMAND	DESCRIPTION	M	P
`show classifier [<name>]`	Displays classifier configuration details.	E	3
`classifier <name> <[packet-format <802.3untag|802.3tag| EtherIIuntag| EtherIItag>] [priority <0-7>] [vlan <vlan-id>][ethernet-type <ether-num|ip|ipx|arp|rarp| appletalk|decnet| sna|netbios|dlc>] [source-mac <src-mac-addr>] [source-port <port-num>] [destination-mac <dest-mac-addr>] [dscp <0-63>] [ip-protocol <protocol-num|tcp|udp|icmp|egp| ospf|rsvp|igmp|igp|pim|ipsec> [establish-only]] [source-ip <SRC-IP-ADDR> [mask-bits <mask-bits>]] [source-socket <socket-num>] [destination-ip <dest-ip-addr> [mask-bits <mask-bits>]] [destination-socket <socket-num>] [inactive]>`	Configures a classifier. Specify the parameters to identify the traffic flow: `ethernet-type` - enter one of the Ethernet types or type the hexadecimal number that identifies an Ethernet type (see Table 26 on page 46) `ip-protocol` - enter one of the protocols or type the port number that identifies the protocol (see Table 27 on page 46) `establish-only` - enter this to identify only TCP packets used to establish TCP connections. `source-socket` - (for UDP or TCP protocols only) specify the protocol port number (see Table 28 on page 46). `destination-socket` - (for UDP or TCP protocols only) specify the protocol port number (see Table 28 on page 46). `inactive` - disables this classifier.	C	13
`no classifier <name>`	Deletes the classifier. If you delete a classifier you cannot use policy rule related information.	C	13
`no classifier <name> inactive`	Enables a classifier.	C	13

The following table shows some other common Ethernet types and the corresponding protocol number.

Table 26 Common Ethernet Types and Protocol Number

ETHERNET TYPE	PROTOCOL NUMBER
IP ETHII	0800
X.75 Internet	0801
NBS Internet	0802
ECMA Internet	0803
Chaosnet	0804
X.25 Level 3	0805
XNS Compat	0807
Banyan Systems	0BAD
BBN Simnet	5208
IBM SNA	80D5
AppleTalk AARP	80F3

In the Internet Protocol there is a field, called “Protocol”, to identify the next level protocol. The following table shows some common protocol types and the corresponding protocol number. Refer to http://www.iana.org/assignments/protocol-numbers for a complete list.

Table 27 Common IP Protocol Types and Protocol Numbers

PROTOCOL TYPE	PROTOCOL NUMBER
ICMP	1
TCP	6
UDP	17
EGP	8
L2TP	115

Some of the most common TCP and UDP port numbers are:

Table 28 Common TCP and UDP Port Numbers

PROTOCOL NAME	TCP/UDP PORT NUMBER
FTP	21
Telnet	23
SMTP	25
DNS	53
HTTP	80
POP3	110

9.2 Command Examples

This example creates a classifier for packets with a VLAN ID of 3. The resulting traffic flow is identified by the name **VLAN3**. The `policy` command can use the name **VLAN3** to apply policy rules to this traffic flow.

```
sysname# config
sysname(config)# classifier VLAN3 vlan 3
sysname(config)# exit
sysname# show classifier
Index Active Name                                Rule
    1 Yes    VLAN3                               VLAN = 3;
```

10

Cluster Commands

Use these commands to configure cluster management.

10.1 Command Summary

The following section lists the commands for this feature.

Table 29 cluster Command Summary

COMMAND	DESCRIPTION	M	P
`show cluster`	Displays cluster management status.	E	3
`cluster <vlan-id>`	Enables clustering in the specified VLAN group.	C	13
`no cluster`	Disables cluster management on the Switch.	C	13
`cluster name <cluster name>`	Sets a descriptive name for the cluster. `<cluster name>`: You may use up to 32 printable characters (spaces are allowed).	C	13
`show cluster candidates`	Displays candidates in the specified VLAN group.	E	3
`cluster member <mac> password <password>`	Adds the specified device to the cluster. You have to specify the password of the device too.	C	13
`show cluster member`	Displays the cluster member(s) and their running status.	E	3
`show cluster member config`	Displays the current cluster member(s).	E	3
`show cluster member mac <mac>`	Displays the running status of the cluster member(s).	E	3
`cluster rcommand <mac>`	Logs into the CLI of the specified cluster member.	C	13
`no cluster member <mac>`	Removes the cluster member.	C	13

10.2 Command Examples

This example creates the cluster CManage in VLAN 1. Then, it looks at the current list of candidates for membership in this cluster and adds two switches to cluster.

```
sysname# configure
sysname(config)# cluster 1
sysname(config)# cluster name CManage
sysname(config)# exit
sysname# show cluster candidates
  Clustering Candidates:
  Index Candidates(MAC/HostName/Model)
      0 00:13:49:00:00:01/ES-2108PWR/ES-2108PWR
      1 00:13:49:00:00:02/GS-3012/GS-3012
      2 00:19:cb:00:00:02/ES-3124/ES-3124
sysname# configure
sysname(config)# cluster member 00:13:49:00:00:01 password 1234
sysname(config)# cluster member 00:13:49:00:00:02 password 1234
sysname(config)# exit
sysname# show cluster member
  Clustering member status:
  Index MACAddr           Name                            Status
      1 00:13:49:00:00:01 ES-2108PWR                      Online
      2 00:13:49:00:00:02 GS-3012                         Online
```

The following table describes the labels in this screen.

Table 30 show cluster member

LABEL	DESCRIPTION
Index	This field displays an entry number for each member.
MACAddr	This field displays the member's MAC address.
Name	This field displays the member's system name.
Status	This field displays the current status of the member in the cluster. **Online**: The member is accessible. **Error**: The member is connected but not accessible. For example, the member's password has changed, or the member was set as the manager and so left the member list. This status also appears while the Switch finishes adding a new member to the cluster. **Offline**: The member is disconnected. It takes approximately 1.5 minutes after the link goes down for this status to appear.

This example logs in to the CLI of member 00:13:49:00:00:01, looks at the current firmware version on the member switch, logs out of the member's CLI, and returns to the CLI of the manager.

```
sysname# configure
sysname(config)# cluster rcommand 00:13:49:00:00:01
Connected to 127.0.0.2
Escape character is '^]'.

User name: admin

Password: ****
Copyright (c) 1994 - 2007 ZyXEL Communications Corp.


ES-2108PWR# show version
  Current ZyNOS version: V3.80(ABS.0)b2 | 05/28/2007
ES-2108PWR# exit
Telnet session with remote host terminated.

Closed
sysname(config)#
```

This example looks at the current status of the Switch's cluster.

```
sysname# show cluster
  Cluster Status: Manager
  VID: 1
  Manager: 00:13:49:ae:fb:7a
```

The following table describes the labels in this screen.

Table 31 show cluster

LABEL	DESCRIPTION
Cluster Status	This field displays the role of this Switch within the cluster. **Manager**: This Switch is the device through which you manage the cluster member switches. **Member**: This Switch is managed by the specified manager. **None**: This Switch is not in a cluster.
VID	This field displays the VLAN ID used by the cluster.
Manager	This field displays the cluster manager's MAC address.

11

Date and Time Commands

Use these commands to configure the date and time on the Switch.

11.1 Command Summary

The following table describes user-input values available in multiple commands for this feature.

Table 32 time User-input Values

COMMAND	DESCRIPTION
week	Possible values (`daylight-saving-time` commands only): `first`, `second`, `third`, `fourth`, `last`.
day	Possible values (`daylight-saving-time` commands only): `Sunday`, `Monday`, `Tuesday`, ...
month	Possible values (`daylight-saving-time` commands only): `January`, `February`, `March`, ...
o'clock	Possible values (`daylight-saving-time` commands only): 0-23

The following section lists the commands for this feature.

Table 33 time Command Summary

COMMAND	DESCRIPTION	M	P
`show time`	Displays current system time and date.	E	3
`time <hour:min:sec>`	Sets the current time on the Switch. *hour*: 0-23 *min*: 0-59 *sec*: 0-59 Note: If you configure Daylight Saving Time after you configure the time, the Switch will apply Daylight Saving Time.	C	13
`time date <month/day/year>`	Sets the current date on the Switch. *month*: 1-12 *day*: 1-31 *year*: 1970-2037	C	13
`time timezone <-1200|...|1200>`	Selects the time difference between UTC (formerly known as GMT) and your time zone.	C	13
`time daylight-saving-time`	Enables daylight saving time. The current time is updated if daylight saving time has started.	C	13

Table 33 time Command Summary (continued)

COMMAND	DESCRIPTION	M	P
`time daylight-saving-time start-date <week> <day> <month> <o'clock>`	Sets the day and time when Daylight Saving Time starts. In most parts of the United States, Daylight Saving Time starts on the second Sunday of March at 2 A.M. local time. In the European Union, Daylight Saving Time starts on the last Sunday of March at 1 A.M. GMT or UTC, so the *o'clock* field depends on your time zone.	C	13
`time daylight-saving-time end-date <week> <day> <month> <o'clock>`	Sets the day and time when Daylight Saving Time ends. In most parts of the United States, Daylight Saving Time ends on the first Sunday of November at 2 A.M. local time. In the European Union, Daylight Saving Time ends on the last Sunday of October at 1 A.M. GMT or UTC, so the *o'clock* field depends on your time zone.	C	13
`no time daylight-saving-time`	Disables daylight saving on the Switch.	C	13
`time daylight-saving-time help`	Provides more information about the specified command.	C	13

Table 34 timesync Command Summary

COMMAND	DESCRIPTION	M	P
`show timesync`	Displays time server information.	E	3
`timesync server <ip>`	Sets the IP address of your time server. The Switch synchronizes with the time server in the following situations: • When the Switch starts up. • Every 24 hours after the Switch starts up. • When the time server IP address or protocol is updated.	C	13
`timesync <daytime|time|ntp>`	Sets the time server protocol. You have to configure a time server before you can specify the protocol.	C	13
`no timesync`	Disables timeserver settings.	C	13

11.2 Command Examples

This example sets the current date, current time, time zone, and daylight savings time.

```
sysname# configure
sysname(config)# time date 06/04/2007
sysname(config)# time timezone -600
sysname(config)# time daylight-saving-time
sysname(config)# time daylight-saving-time start-date second Sunday
--> March 2
sysname(config)# time daylight-saving-time end-date first Sunday
--> November 2
sysname(config)# time 13:24:00
sysname(config)# exit
sysname# show time
Current Time  13:24:03 (UTC-05:00 DST)
Current Date  2007-06-04
```

This example looks at the current time server settings.

```
sysname# show timesync


  Time Configuration
  ------------------------------
  Time Zone              :UTC -600
  Time Sync Mode         :USE_DAYTIME
  Time Server IP Address :172.16.37.10

  Time Server Sync Status:CONNECTING
```

The following table describes the labels in this screen.

Table 35 show timesync

LABEL	DESCRIPTION
Time Zone	This field displays the time zone.
Time Sync Mode	This field displays the time server protocol the Switch uses. It displays **NO_TIMESERVICE** if the time server is disabled.
Time Server IP Address	This field displays the IP address of the time server.
Time Server Sync Status	This field displays the status of the connection with the time server. **NONE**: The time server is disabled. **CONNECTING**: The Switch is trying to connect with the specified time server. **OK**: Synchronize with time server done. **FAIL**: Synchronize with time server fail.

12

DHCP Commands

Use these commands to configure DHCP features on the Switch.

- Use the `dhcp relay` commands to configure DHCP relay for specific VLAN.
- Use the `dhcp smart-relay` commands to configure DHCP relay for all broadcast domains.
- Use the `dhcp server` commands to configure the Switch as a DHCP server.

12.1 Command Summary

The following section lists the commands for this feature.

Table 36 dhcp smart-relay Command Summary

COMMAND	DESCRIPTION	M	P
`show dhcp smart-relay`	Displays global DHCP relay settings.	E	3
`dhcp smart-relay`	Enables DHCP relay for all broadcast domains on the Switch. Note: You have to disable `dhcp relay` before you can enable `dhcp smart-relay`.	C	13
`no dhcp smart-relay`	Disables global DHCP relay settings.	C	13
`dhcp smart-relay helper-address <remote-dhcp-server1> [<remote-dhcp-server2>] [<remote-dhcp-server3>]`	Sets the IP addresses of up to 3 DHCP servers.	C	13
`dhcp smart-relay information`	Allows the Switch to add system name to agent information.	C	13
`no dhcp smart-relay information`	System name is not appended to option 82 information field for global dhcp settings.	C	13
`dhcp smart-relay option`	Allows the Switch to add DHCP relay agent information.	C	13
`no dhcp smart-relay option`	Disables the relay agent information option 82 for global dhcp settings.	C	13

Table 37 dhcp relay Command Summary

COMMAND	DESCRIPTION	M	P
`show dhcp relay <vlan-id>`	Displays DHCP relay settings for the specified VLAN.	E	3
`dhcp relay <vlan-id> helper-address <remote-dhcp-server1> [<remote-dhcp-server2>] [<remote-dhcp-server3>] [option] [information]`	Enables DHCP relay on the specified VLAN and sets the IP address of up to 3 DHCP servers. Optionally, sets the Switch to add relay agent information and system name. Note: You have to configure the VLAN before you configure a DHCP relay for the VLAN. You have to disable `dhcp smart-relay` before you can enable `dhcp relay`.	C	13
`no dhcp relay <vlan-id>`	Disables DHCP relay.	C	13
`no dhcp relay <vlan-id> information`	System name is not appended to option 82 information field.	C	13
`no dhcp relay <vlan-id> option`	Disables the relay agent information option 82.	C	13

Table 38 dhcp relay-broadcast Command Summary

COMMAND	DESCRIPTION	M	P
`dhcp relay-broadcast`	The broadcast behavior of DHCP packets will not be terminated by the Switch.	C	13
`no dhcp relay-broadcast`	The Switch terminates the broadcast behavior of DHCP packets.	C	13

Table 39 dhcp relay Command Summary

COMMAND	DESCRIPTION	M	P
`show dhcp relay <vlan-id>`	Displays DHCP relay settings for the specified VLAN.	E	3
`dhcp relay <vlan-id> helper-address <remote-dhcp-server1> [<remote-dhcp-server2>] [<remote-dhcp-server3>] [option] [information]`	Enables DHCP relay on the specified VLAN and sets the IP address of up to 3 DHCP servers. Optionally, sets the Switch to add relay agent information and system name. Note: You have to configure the VLAN before you configure a DHCP relay for the VLAN. You have to disable `dhcp smart-relay` before you can enable `dhcp relay`.	C	13
`no dhcp relay <vlan-id>`	Disables DHCP relay.	C	13
`no dhcp relay <vlan-id> information`	Disables the relay agent information option 82.	C	13
`no dhcp relay <vlan-id> option`	System name is not appended to option 82 information field.	C	13

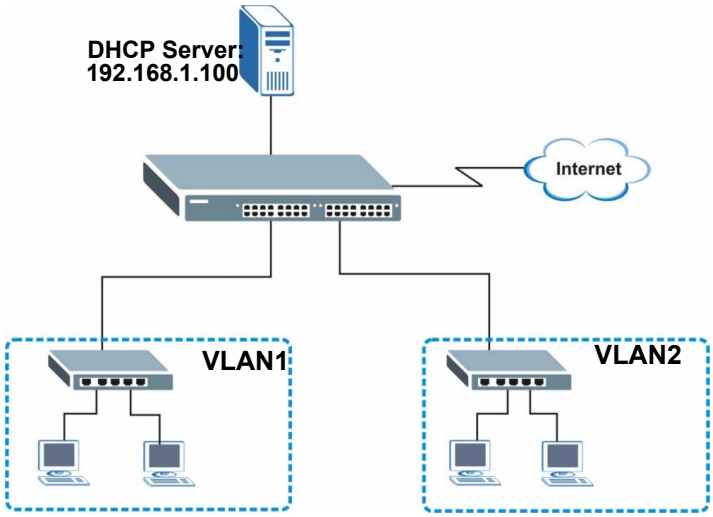
Table 40 dhcp server Command Summary

COMMAND	DESCRIPTION	M	P
`dhcp server <vlan-id> starting-address <ip-addr> <subnet-mask> size-of-client-ip-pool <1-253>`	Enables DHCP server for the specified VLAN and specifies the TCP/IP configuration details to send to DHCP clients.	C	13
`dhcp server <vlan-id> starting-address <ip-addr> <subnet-mask> size-of-client-ip-pool <1-253> [default-gateway <ip-addr>] [primary-dns <ip-addr>] [secondary-dns <ip-addr>]`	Enables DHCP server for the specified VLAN and specifies the TCP/IP configuration details to send to DHCP clients. Including default gateway IP address and DNS server information.	C	13
`no dhcp server <vlan-id>`	Disables DHCP server for the specified VLAN.	C	13
`no dhcp server <vlan-id> default-gateway`	Disables DHCP server default gateway settings.	C	13
`no dhcp server <vlan-id> primary-dns`	Disables DHCP primary DNS server settings.	C	13
`no dhcp server <vlan-id> secondary-dns`	Disables DHCP server secondary DNS settings.	C	13

12.2 Command Examples

In this example, the Switch relays DHCP requests for the **VLAN1** and **VLAN2** domains. There is only one DHCP server for DHCP clients in both domains.

Figure 1 Example: Global DHCP Relay

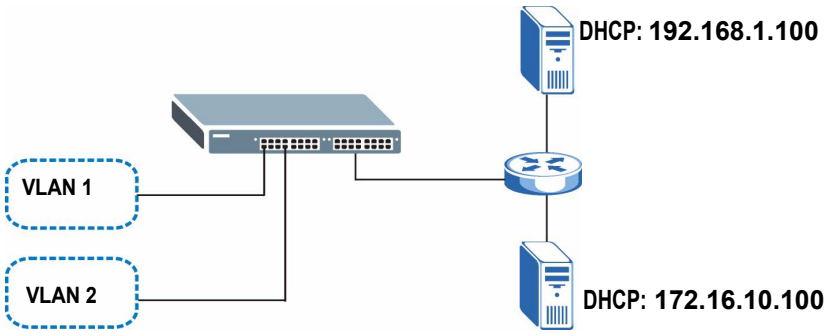


This example shows how to configure the Switch for this configuration. DHCP relay agent information option 82 is also enabled.

```
sysname# configure
sysname(config)# dhcp smart-relay
sysname(config)# dhcp smart-relay helper-address 192.168.1.100
sysname(config)# dhcp smart-relay option
sysname(config)# exit
sysname# show dhcp smart-relay
  DHCP Relay Agent Configuration
  Active:       Yes
  Remote DHCP Server 1:192.168.1.100
  Remote DHCP Server 2:   0.0.0.0
  Remote DHCP Server 3:   0.0.0.0
  Option82:  Enable     Option82Inf: Disable
```

In this example, there are two VLANs (VIDs 1 and 2) in a campus network. Two DHCP servers are installed to serve each VLAN. The Switch forwards DHCP requests from the dormitory rooms (VLAN 1) to the DHCP server with IP address 192.168.1.100. DHCP requests from the academic buildings (VLAN 2) are sent to the other DHCP server with IP address 172.16.10.100.

Figure 2 Example: DHCP Relay for Two VLANs

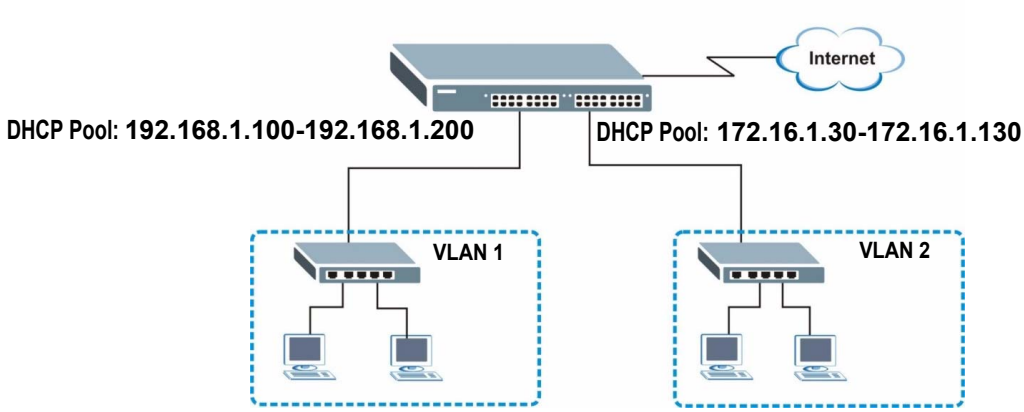


This example shows how to configure these DHCP servers. The VLANs are already configured.

```
sysname# configure
sysname(config)# dhcp relay 1 helper-address 192.168.1.100
sysname(config)# dhcp relay 2 helper-address 172.16.10.100
sysname(config)# exit
```

In this example, the Switch is a DHCP server for clients on VLAN 1 and VLAN 2. The DHCP clients in VLAN 1 are assigned IP addresses in the range 192.168.1.100 to 192.168.1.200 and clients on VLAN 2 are assigned IP addresses in the range 172.16.1.30 to 172.16.1.130.

Figure 3 Example: DHCP Relay for Two VLANs



This example shows how to configure the DHCP server for VLAN 1 with the configuration shown in Figure 3 on page 61. It also provides the DHCP clients with the IP address of the default gateway and the DNS server.

```
sysname# configure
sysname(config)# dhcp server 1 starting-address 192.168.1.100
255.255.255.0 size-of-client-ip-pool 100 default-gateway 192.168.1.1
primary-dns 192.168.5.1
```

13

DHCP Snooping & DHCP VLAN Commands

Use the `dhcp snooping` commands to configure the DHCP snooping on the Switch and the `dhcp vlan` commands to specify a DHCP VLAN on your network. DHCP snooping filters unauthorized DHCP packets on the network and builds the binding table dynamically.

13.1 Command Summary

The following section lists the commands for this feature.

Table 41 dhcp snooping Command Summary

COMMAND	DESCRIPTION	M	P
`show dhcp snooping`	Displays DHCP snooping configuration on the Switch.	E	3
`show dhcp snooping binding`	Displays the DHCP binding table.	E	3
`show dhcp snooping database`	Displays DHCP snooping database update statistics and settings.	E	3
`show dhcp snooping database detail`	Displays DHCP snooping database update statistics in full detail form.	E	3
`dhcp snooping`	Enables DHCP Snooping on the Switch.	C	13
`no dhcp snooping`	Disables DHCP Snooping on the Switch.	C	13
`dhcp snooping database <tftp://host/filename>`	Specifies the location of the DHCP snooping database. The location should be expressed like this: **tftp://{domain name or IP address}/directory, if applicable/file name**; for example, **tftp://192.168.10.1/database.txt**.	C	13
`no dhcp snooping database`	Removes the location of the DHCP snooping database.	C	13
`dhcp snooping database timeout <seconds>`	Specifies how long (10-65535 seconds) the Switch tries to complete a specific update in the DHCP snooping database before it gives up.	C	13
`no dhcp snooping database timeout <seconds>`	Resets how long (10-65535 seconds) the Switch tries to complete a specific update in the DHCP snooping database before it gives up to the default value (300).	C	13
`dhcp snooping database write-delay <seconds>`	Specifies how long (10-65535 seconds) the Switch waits to update the DHCP snooping database the first time the current bindings change after an update.	C	13
`no dhcp snooping database write-delay <seconds>`	Resets how long (10-65535 seconds) the Switch waits to update the DHCP snooping database the first time the current bindings change after an update to the default value (300).	C	13

Table 41 dhcp snooping Command Summary (continued)

COMMAND	DESCRIPTION	M	P
`dhcp snooping vlan <vlan-list>`	Specifies the VLAN IDs for VLANs you want to enable DHCP snooping on.	C	13
`no dhcp snooping vlan <vlan-list>`	Specifies the VLAN IDs for VLANs you want to disable DHCP snooping on.	C	13
`dhcp snooping vlan <vlan-list> information`	Sets the Switch to add the system name to DHCP requests that it broadcasts to the DHCP VLAN, if specified, or VLAN.	C	13
`no dhcp snooping vlan <vlan-list> information`	Sets the Switch to not add the system name to DHCP requests that it broadcasts to the DHCP VLAN, if specified, or VLAN.	C	13
`dhcp snooping vlan <vlan-list> option`	Sets the Switch to add the slot number, port number and VLAN ID to DHCP requests that it broadcasts to the DHCP VLAN, if specified, or VLAN.	C	13
`no dhcp snooping vlan <vlan-list> option`	Sets the Switch to not add the slot number, port number and VLAN ID to DHCP requests that it broadcasts to the DHCP VLAN, if specified, or VLAN.	C	13
`clear dhcp snooping database statistics`	Delete all statistics records of DHCP requests going through the Switch.	E	13
`renew dhcp snooping database`	Loads dynamic bindings from the default DHCP snooping database.	E	13
`renew dhcp snooping database <tftp://host/filename>`	Loads dynamic bindings from the specified DHCP snooping database.	E	13
`interface port-channel <port-list>`	Enables a port or a list of ports for configuration.	C	13
`dhcp snooping trust`	Sets this port as a trusted DHCP snooping port. Trusted ports are connected to DHCP servers or other switches, and the Switch discards DHCP packets from trusted ports only if the rate at which DHCP packets arrive is too high.	C	13
`dhcp snooping limit rate <pps>`	Sets the maximum rate in packets per second (pps) that DHCP packets are allowed to arrive at a trusted DHCP snooping port.	C	13
`no dhcp snooping trust`	Disables this port from being a trusted port for DHCP snooping.	C	13
`no dhcp snooping limit rate`	Resets the DHCP snooping rate to the default (0).	C	13

The following table describes the `dhcp-vlan` commands.

Table 42 dhcp-vlan Command Summary

COMMAND	DESCRIPTION	M	P
`dhcp dhcp-vlan <vlan-id>`	Specifies the VLAN ID of the DHCP VLAN.	C	13
`no dhcp dhcp-vlan`	Disables DHCP VLAN on the Switch.	C	13

13.2 Command Examples

This example:

- Enables DHCP snooping Switch.
- Sets up an external DHCP snooping database on a network server with IP address 172.16.37.17.

- Enables DHCP snooping on VLANs 1,2,3,200 and 300.
- Sets the Switch to add the slot number, port number and VLAN ID to DHCP requests that it broadcasts to the DHCP VLAN.
- Sets ports 1 - 5 as DHCP snooping trusted ports.
- Sets the maximum number of DHCP packets that can be received on ports 1 - 5 to 100 packets per second.
- Configures a DHCP VLAN with a VLAN ID 300.
- Displays DHCP snooping configuration details.

```
sysname(config)# dhcp snooping
sysname(config)# dhcp snooping database tftp://172.16.37.17/
snoopdata.txt
sysname(config)# dhcp snooping vlan 1,2,3,200,300
sysname(config)# dhcp snooping vlan 1,2,3,200,300 option
sysname(config)# interface port-channel 1-5
sysname(config-interface)# dhcp snooping trust
sysname(config-interface)# dhcp snooping limit rate 100
sysname(config-interface)# exit
sysname(config)# dhcp dhcp-vlan 300
sysname(config)# exit
sysname# show dhcp snooping
  Switch DHCP snooping is enabled
  DHCP Snooping is configured on the following VLANs:
    1-3,200,300
  Option 82 is configured on the following VLANs:
    1-3,200,300
  Appending system name is configured on the following VLANs:

  DHCP VLAN is enabled on VLAN 300
Interface  Trusted  Rate Limit (pps)
---------  -------  ----------------
        1      yes               100
        2      yes               100
        3      yes               100
        4      yes               100
        5      yes               100
        6       no         unlimited
        7       no         unlimited
        8       no         unlimited
```

14

DiffServ Commands

Use these commands to configure Differentiated Services (DiffServ) on the Switch.

14.1 Command Summary

The following section lists the commands for this feature.

Table 43 diffserv Command Summary

COMMAND	DESCRIPTION	M	P
`show diffserv`	Displays general DiffServ settings.	E	3
`diffserv`	Enables DiffServ on the Switch.	C	13
`no diffserv`	Disables DiffServ on the Switch.	C	13
`diffserv dscp <0-63> priority <0-7>`	Sets the DSCP-to-IEEE 802.1q mappings.	C	13
`interface port-channel <port-list>`	Enters config-interface mode for the specified port(s).	C	13
`diffserv`	Enables DiffServ on the port(s).	C	13
`no diffserv`	Disables DiffServ on the port(s).	C	13

15

DVMRP Commands

This chapter explains how to use commands to activate the Distance Vector Multicast Routing Protocol (DVMRP) on the Switch.

15.1 DVMRP Overview

DVMRP (Distance Vector Multicast Routing Protocol) is a protocol used for routing multicast data. DVMRP is used when a router receives multicast traffic and it wants to find out if other multicast routers it is connected to need to receive the data. DVMRP sends the data to all attached routers and waits for a reply. Routers which do not need to receive the data (do not have multicast group member connected) return a "prune" message, which stops further multicast traffic for that group from reaching the router.

15.2 Command Summary

The following section lists the commands for this feature.

Table 44 Command Summary: DVMRP

COMMAND	DESCRIPTION	M	P
`show ip dvmrp group`	Displays DVMRP group information.	E	3
`show ip dvmrp interface`	Displays DVMRP interface information.	E	3
`show ip dvmrp neighbor`	Displays DVMRP neighbor information.	E	3
`show ip dvmrp prune`	Displays the DVMRP prune information.	E	3
`show ip dvmrp route`	Displays the DVMRP routes.	E	3
`show router dvmrp`	Displays DVMRP settings.	E	3
`router dvmrp`	Enables and enters the DVMRP configuration mode.	C	13
`exit`	Leaves the DVMRP configuration mode.	C	13
`threshold <ttl-value>`	Sets the DVMRP threshold value. Multicast packets with TTL (Time-To-Live) value lower than the threshold are not forwarded by the Switch.	C	13
`no router dvmrp`	Disables DVMRP on the Switch.	C	13
`interface route-domain <ip-address>/<mask-bits>`	Enters the configuration mode for this routing domain.	C	13

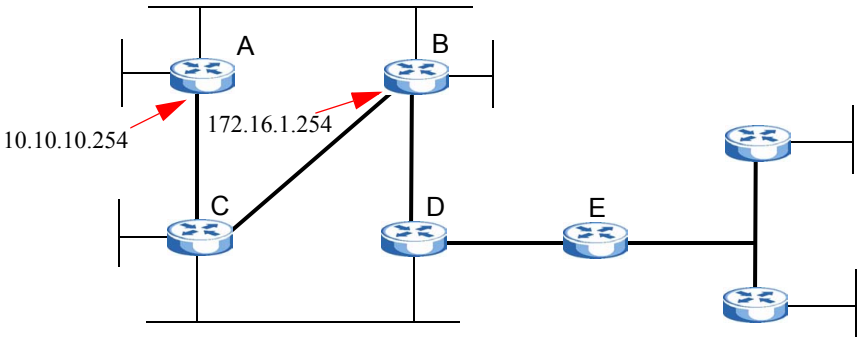
Table 44 Command Summary: DVMRP (continued)

COMMAND	DESCRIPTION	M	P
ip dvmrp	Activates this routing domain in participating in DVMRP.	C	13
no ip dvmrp	Disables this routing domain from participating in DVMRP.	C	13

15.3 Command Examples

In this example, the Switch is configured to exchange DVMRP information with other DVMRP enabled routers as shown next. The Switch is a DVMRP router (**C**). DVMRP is activated on IP routing domains **10.10.10.1/24** and **172.16.1.1/24** so that it can exchange DVMRP information with routers **A** and **B**.

Figure 4 DVMRP Network Example



- Enables IGMP and DVMRP on the Switch.
- Enables DVMRP on the following routing domains: 10.10.10.1/24, 172.16.1.1/24.
- Displays DVMRP settings configured on the Switch.

```
sysname(config)# router igmp
sysname(config-igmp)# exit
sysname(config)# router dvmrp
sysname(config-dvmrp)# exit
sysname(config)# interface route-domain 10.10.10.1/24
sysname(config-if)# ip dvmrp
sysname(config-if)# exit
sysname(config)# interface route-domain 172.16.1.1/24
sysname(config-if)# ip dvmrp
sysname(config-if)# exit
sysname(config)# exit
sysname# show router dvmrp
  TTL threshold: 50

  IP Address       Subnet Mask     Active
  ----------------------------------------
  10.10.10.1       255.255.255.0   Yes
  172.16.1.1   255.255.255.0   Yes
  192.168.1.1      255.255.255.0   No
```

16

Ethernet OAM Commands

Use these commands to use the link monitoring protocol IEEE 802.3ah Link Layer Ethernet OAM (Operations, Administration and Maintenance).

16.1 IEEE 802.3ah Link Layer Ethernet OAM Implementation

Link layer Ethernet OAM (Operations, Administration and Maintenance) as described in IEEE 802.3ah is a link monitoring protocol. It utilizes OAM Protocol Data Units or OAM PDU's to transmit link status information between directly connected Ethernet devices. Both devices must support IEEE 802.3ah. Because link layer Ethernet OAM operates at layer two of the OSI (Open Systems Interconnection Basic Reference) model, neither IP or SNMP are necessary to monitor or troubleshoot network connection problems.

The Switch supports the following IEEE 802.3ah features:

- **Discovery** - this identifies the devices on each end of the Ethernet link and their OAM configuration.
- **Remote Loopback** - this can initiate a loopback test between Ethernet devices.

16.2 Command Summary

The following section lists the commands for this feature.

Table 45 ethernet oam Command Summary

COMMAND	DESCRIPTION	M	P
`show ethernet oam discovery <port-list>`	Displays OAM configuration details and operational status of the specified ports.	E	3
`show ethernet oam statistics <port-list>`	Displays the number of OAM packets transferred for the specified ports.	E	3
`show ethernet oam summary`	Displays the configuration details of each OAM activated port.	E	3
`remote-loopback test <port-list>`	Initiates a remote-loopback test from the specified port(s).	E	3
`ethernet oam`	Enables Ethernet OAM on the Switch.	C	13
`no ethernet oam`	Disables Ethernet OAM on the Switch.	C	13
`interface port-channel <port-list>`	Enters config-interface mode for the specified port(s).	C	13
`ethernet oam`	Enables Ethernet OAM on the port(s).	C	13
`no ethernet oam`	Disables Ethernet OAM on the port(s).	C	13

Table 45 ethernet oam Command Summary (continued)

COMMAND	DESCRIPTION	M	P
ethernet oam mode <active|passive>	Specifies the OAM mode on the ports. active: Allows the port to issue and respond to Ethernet OAM commands. passive: Allows the port to respond to Ethernet OAM commands.	C	13
ethernet oam remote-loopback supported	Enables the remote loopback feature on the ports.	C	13
no ethernet oam remote-loopback supported	Disables the remote loopback feature on the ports.	C	13
no ethernet oam mode	Resets the OAM mode to the default value.	C	13

16.3 Command Examples

This example enables Ethernet OAM on port 7 and sets the mode to active.

```
sysname# configure
sysname(config)# ethernet oam
sysname(config)# interface port-channel 7
sysname(config-interface)# ethernet oam
sysname(config-interface)# ethernet oam mode active
sysname(config-interface)# exit
sysname(config)# exit
```

This example performs Ethernet OAM discovery from port 7.

```
sysname# show ethernet oam discovery 7
Port 7
Local client
------------
  OAM configurations:
    Mode              : Active
    Unidirectional    : Not supported
    Remote loopback   : Not supported
    Link events       : Not supported
    Variable retrieval: Not supported
    Max. OAMPDU size  : 1518

  Operational status:
    Link status       : Down
    Info. revision    : 3
    Parser state      : Forward
    Discovery state   : Active Send Local
```

The following table describes the labels in this screen.

Table 46 show ethernet oam discovery

LABEL	DESCRIPTION
OAM configurations	The remote device uses this information to determine what functions are supported.
Mode	This field displays the OAM mode. The device in active mode (typically the service provider's device) controls the device in passive mode (typically the subscriber's device). **Active**: The Switch initiates OAM discovery; sends information PDUs; and may send event notification PDUs, variable request/response PDUs, or loopback control PDUs. **Passive**: The Switch waits for the remote device to initiate OAM discovery; sends information PDUs; may send event notification PDUs; and may respond to variable request PDUs or loopback control PDUs. The Switch might not support some types of PDUs, as indicated in the fields below.
Unidirectional	This field indicates whether or not the Switch can send information PDUs to transmit fault information when the receive path is non-operational.
Remote loopback	This field indicates whether or not the Switch can use loopback control PDUs to put the remote device into loopback mode.
Link events	This field indicates whether or not the Switch can interpret link events, such as link fault and dying gasp. Link events are sent in event notification PDUs and indicate when the number of errors in a given interval (time, number of frames, number of symbols, or number of errored frame seconds) exceeds a specified threshold. Organizations may create organization-specific link event TLVs as well.
Variable retrieval	This field indicates whether or not the Switch can respond to requests for more information, such as requests for Ethernet counters and statistics, about link events.
Max. OAMPDU size	This field displays the maximum size of PDU for receipt and delivery.
Operational status	
Link status	This field indicates that the link is up or down.
Info. revision	This field displays the current version of local state and configuration. This two-octet value starts at zero and increments every time the local state or configuration changes.

Table 46 show ethernet oam discovery (continued)

LABEL	DESCRIPTION
Parser state	This field indicates the current state of the parser. **Forward**: The packet is forwarding packets normally. **Loopback**: The Switch is in loopback mode. **Discard**: The Switch is discarding non-OAMPDUs because it is trying to or has put the remote device into loopback mode.
Discovery state	This field indicates the state in the OAM discovery process. OAM-enabled devices use this process to detect each other and to exchange information about their OAM configuration and capabilities. OAM discovery is a handshake protocol. **Fault**: One of the devices is transmitting OAM PDUs with link fault information, or the interface is not operational. **Active Send Local**: The Switch is in active mode and is trying to see if the remote device supports OAM. **Passive Wait**: The Switch is in passive mode and is waiting for the remote device to begin OAM discovery. **Send Local Remote**: This state occurs in the following circumstances. • The Switch has discovered the remote device but has not accepted or rejected the connection yet. • The Switch has discovered the remote device and rejected the connection. **Send Local Remote OK**: The Switch has discovered the remote device and has accepted the connection. In addition, the remote device has not accepted or rejected the connection yet, or the remote device has rejected the connected. **Send Any**: The Switch and the remote device have accepted the connection. This is the operating state for OAM links that are fully operational.

This example looks at the number of OAM packets transferred on port 1.

```
sysname# show ethernet oam statistics 1
Port 1
Statistics:
-----------
  Information OAMPDU Tx         : 0
  Information OAMPDU Rx         : 0
  Event Notification OAMPDU Tx  : 0
  Event Notification OAMPDU Rx  : 0
  Loopback Control OAMPDU Tx    : 0
  Loopback Control OAMPDU Rx    : 0
  Variable Request OAMPDU Tx    : 0
  Variable Request OAMPDU Rx    : 0
  Variable Response OAMPDU Tx   : 0
  Variable Response OAMPDU Rx   : 0
  Unsupported OAMPDU Tx         : 0
  Unsupported OAMPDU Rx         : 0
```

The following table describes the labels in this screen.

Table 47 show ethernet oam statistics

LABEL	DESCRIPTION
Information OAMPDU Tx	This field displays the number of OAM PDUs sent on the port.
Information OAMPDU Rx	This field displays the number of OAM PDUs received on the port.

Table 47 show ethernet oam statistics (continued)

LABEL	DESCRIPTION
Event Notification OAMPDU Tx	This field displays the number of unique or duplicate OAM event notification PDUs sent on the port.
Event Notification OAMPDU Rx	This field displays the number of unique or duplicate OAM event notification PDUs received on the port.
Loopback Control OAMPDU Tx	This field displays the number of loopback control OAM PDUs sent on the port.
Loopback Control OAMPDU Rx	This field displays the number of loopback control OAM PDUs received on the port.
Variable Request OAMPDU Tx	This field displays the number of OAM PDUs sent to request MIB objects on the remote device.
Variable Request OAMPDU Rx	This field displays the number of OAM PDUs received requesting MIB objects on the Switch.
Variable Response OAMPDU Tx	This field displays the number of OAM PDUs sent by the Switch in response to requests.
Variable Response OAMPDU Rx	This field displays the number of OAM PDUs sent by the remote device in response to requests.
Unsupported OAMPDU Tx	This field displays the number of unsupported OAM PDUs sent on the port.
Unsupported OAMPDU Rx	This field displays the number of unsupported OAM PDUs received on the port.

This example looks at the configuration of ports on which OAM is enabled.

```
sysname# show ethernet oam summary

OAM Config: U : Unidirection, R : Remote Loopback
            L : Link Events , V : Variable Retrieval

    Local          Remote
------------- ----------------------------------------
Port  Mode    MAC Addr          OUI    Mode    Config
----- ------- ----------------- ------ ------- --------
1     Active
```

The following table describes the labels in this screen.

Table 48 show ethernet oam summary

LABEL	DESCRIPTION
Local	This section displays information about the ports on the Switch.
Port	This field displays the port number.
Mode	This field displays the operational state of the port.
Remote	This section displays information about the remote device.
MAC Addr	This field displays the MAC address of the remote device.
OUI	This field displays the OUI (first three bytes of the MAC address) of the remote device.

Table 48 show ethernet oam summary (continued)

LABEL	DESCRIPTION
Mode	This field displays the operational state of the remote device.
Config	This field displays the capabilities of the Switch and remote device. THe capabilities are identified in the **OAM Config** section.

17

GARP Commands

Use these commands to configure GARP.

17.1 GARP Overview

Switches join VLANs by making a declaration. A declaration is made by issuing a Join message using GARP. Declarations are withdrawn by issuing a Leave message. A Leave All message terminates all registrations. GARP timers set declaration timeout values.

17.2 Command Summary

The following section lists the commands for this feature.

Table 49 garp Command Summary

COMMAND	DESCRIPTION	M	P
`show garp`	Displays GARP information.	E	3
`garp join <100-65535> leave <200-65535> leaveall <200-65535>`	Configures GARP time settings (in milliseconds), including the join, leave and leave all timers for each port. Leave Time must be at least two times larger than Join Timer, and Leave All Timer must be larger than Leave Timer.	C	13

17.3 Command Examples

In this example, the administrator looks at the Switch's GARP timer settings and decides to change them. The administrator sets the Join Timer to 300 milliseconds, the Leave Timer to 800 milliseconds, and the Leave All Timer to 11000 milliseconds.

```
sysname# show garp

GARP Timer
------------------------
Join  Timer      :200
Leave Timer      :600
Leave All Timer  :10000
sysname# configure
sysname(config)# garp join 300 leave 800 leaveall 11000
sysname(config)# exit
sysname# show garp

GARP Timer
------------------------
Join  Timer      :300
Leave Timer      :800
Leave All Timer  :11000
```

18

GVRP Commands

Use these commands to configure GVRP.

18.1 Command Summary

The following section lists the commands for this feature.

Table 50 gvrp Command Summary

COMMAND	DESCRIPTION	M	P
`show vlan1q gvrp`	Displays GVRP settings.	E	13
`vlan1q gvrp`	Enables GVRP.	C	13
`no vlan1q gvrp`	Disables GVRP on the Switch.	C	13
`interface port-channel <port-list>`	Enters config-interface mode for the specified port(s).	C	13
`gvrp`	Enables this function to permit VLAN groups beyond the local Switch.	C	13
`no gvrp`	Disable GVRP on the port(s).	C	13

18.2 Command Examples

This example shows the Switch's GVRP settings.

```
sysname# show vlan1q gvrp

GVRP Support
-----------------------
gvrpEnable = YES
gvrpPortEnable:
```

This example turns off GVRP on ports 1-5.

```
sysname# configure
sysname(config)# interface port-channel 1-5
sysname(config-interface)# no gvrp
sysname(config-interface)# exit
sysname(config)# exit
```

PART III
Reference H-M

19

HTTPS Server Commands

Use these commands to configure the HTTPS server on the Switch.

19.1 Command Summary

The following section lists the commands for this feature.

Table 51 https Command Summary

COMMAND	DESCRIPTION	M	P
`show https`	Displays the HTTPS settings, statistics, and sessions.	E	3
`show https certificate`	Displays the HTTPS certificates.	E	3
`show https key <rsa|dsa>`	Displays the HTTPS key.	E	3
`show https session`	Displays current HTTPS session(s).	E	3
`https cert-regeneration <rsa|dsa>`	Re-generates a certificate.	C	13

19.2 Command Examples

This example shows the current HTTPS settings, statistics, and sessions.

```
sysname# show https
Configuration
    Version               : SSLv3, TLSv1
    Maximum session number:    64 sessions
    Maximum cache number  :   128 caches
    Cache timeout         :   300 seconds
    Support ciphers       :
        DHE-RSA-AES256-SHA DHE-DSS-AES256-SHA AES256-SHA EDH-RSA-DES-
CBC3-SHA
       EDH-DSS-DES-CBC3-SHA DES-CBC3-SHA DES-CBC3-MD5 DHE-RSA-AES128-SHA
        DHE-DSS-AES128-SHA AES128-SHA DHE-DSS-RC4-SHA IDEA-CBC-SHA RC4-
SHA
        RC4-MD5 IDEA-CBC-MD5 RC2-CBC-MD5 RC4-MD5

Statistics:
    Total connects        :     0
    Current connects      :     0
    Connects that finished:     0
    Renegotiate requested :     0
    Session cache items   :     0
    Session cache hits    :     0
    Session cache misses  :     0
    Session cache timeouts:     0

Sessions:
    Remote IP        Port   Local IP         Port   SSL bytes  Sock bytes
```

The following table describes the labels in this screen.

Table 52 show https

LABEL	DESCRIPTION
Configuration	
Version	This field displays the current version of SSL (Secure Sockets Layer) and TLS (Transport Layer Security).
Maximum session number	This field displays the maximum number of HTTPS sessions the Switch supports.
Maximum cache number	This field displays the maximum number of entries in the cache table the Switch supports for HTTPS sessions.
Cache timeout	This field displays how long entries remain in the cache table before they expire.
Support ciphers	This field displays the SSL or TLS cipher suites the Switch supports for HTTPS sessions. The cipher suites are identified by their OpenSSL equivalent names. If the name does not include the authentication used, assume RSA authentication. See SSL v2.0, SSL v3.0, TLS v1.0, and RFC 3268 for more information.
Statistics	
Total connects	This field displays the total number of HTTPS connections since the Switch started up.
Current connects	This field displays the current number of HTTPS connections.

Table 52 show https (continued)

LABEL	DESCRIPTION
Connects that finished	This field displays the number of HTTPS connections that have finished.
Renegotiate requested	This field displays the number of times the Switch requested clients to renegotiate the SSL connection parameters.
Session cache items	This field displays the current number of items in cache.
Session cache hits	This field displays the number of times the Switch used cache to satisfy a request.
Session cache misses	This field displays the number of times the Switch could not use cache to satisfy a request.
Session cache timeouts	This field displays the number of items that have expired in the cache.
Sessions	
Remote IP	This field displays the client's IP address in this session.
Port	This field displays the client's port number in this session.
Local IP	This field displays the Switch's IP address in this session.
Port	This field displays the Switch's port number in this session.
SSL bytes	This field displays the number of bytes encrypted or decrypted by the Secure Socket Layer (SSL).
Sock bytes	This field displays the number of bytes encrypted or decrypted by the socket.

This example shows the current HTTPS sessions.

```
sysname# show https session
SSL-Session:
    Protocol  : SSLv3
    Cipher    : RC4-MD5
    Session-ID:
68BFB25BFAFEE3F0F15AB7B038EAB6BACE4AB7A4A6A5280E55943B7191057C96
    Session-ID-ctx: 7374756E6E656C20534944
    Master-Key:
65C110D9BD9BB0EE36CE0C76408C121DAFD1E5E3209614EB0AC5509CDB60D0904937DA4B
A5BA058B57FD7169ACDD4ACF
    Key-Arg   : None
    Start Time: 2252
    Timeout   : 300 (sec)
    Verify return code: 0 (ok)
```

The following table describes the labels in this screen.

Table 53 show https session

LABEL	DESCRIPTION
Protocol	This field displays the SSL version used in the session.
Cipher	This field displays the encryption algorithms used in the session.
Session-ID	This field displays the session identifier.
Session-ID-ctx	This field displays the session ID context, which is used to label the data and cache in the sessions and to ensure sessions are only reused in the appropriate context.
Master-Key	This field displays the SSL session master key.

Table 53 show https session (continued)

LABEL	DESCRIPTION
Key-Arg	This field displays the key argument that is used in SSLv2.
Start Time	This field displays the start time (in seconds, represented as an integer in standard UNIX format) of the session.
Timeout	This field displays the timeout for the session. If the session is idle longer than this, the Switch automatically disconnects.
Verify return code	This field displays the return code when an SSL client certificate is verified.

20

IEEE 802.1x Authentication Commands

Use these commands to configure IEEE 802.1x authentication.

Do not forget to configure the authentication server.

20.1 Command Summary

The following section lists the commands for this feature.

Table 54 port-access-authenticator Command Summary

COMMAND	DESCRIPTION	M	P
`show port-access-authenticator`	Displays all port authentication settings.	E	3
`show port-access-authenticator <port-list>`	Displays port authentication settings on the specified port(s).	E	3
`port-access-authenticator`	Enables 802.1x authentication on the Switch.	C	13
`no port-access-authenticator`	Disables port authentication on the Switch.	C	13
`port-access-authenticator <port-list>`	Enables 802.1x authentication on the specified port(s).	C	13
`no port-access-authenticator <port-list>`	Disables authentication on the listed ports.	C	13
`port-access-authenticator <port-list> reauthenticate`	Sets a subscriber to periodically re-enter his or her username and password to stay connected to a specified port.	C	13
`no port-access-authenticator <port-list> reauthenticate`	Disables the re-authentication mechanism on the listed port(s).	C	13
`port-access-authenticator <port-list> reauth-period <1-65535>`	Specifies how often (in seconds) a client has to re-enter the username and password to stay connected to the specified port(s).	C	13

20.2 Command Examples

This example configures the Switch in the following ways:

1. Specifies RADIUS server 1 with IP address 10.10.10.1, port 1890 and the string **secretKey** as the password.
2. Specifies the timeout period of 30 seconds that the Switch will wait for a response from the RADIUS server.
3. Enables port authentication on the Switch.
4. Enables port authentication on ports 4 to 8.
5. Activates reauthentication on ports 4-8.
6. Specifies 1800 seconds as the interval for client reauthentication on ports 4-8.

```
sysname(config)# radius-server host 1 10.10.10.1 auth-port 1890 key
--> secretKey
sysname(config)# radius-server timeout 30
sysname(config)# port-access-authenticator
sysname(config)# port-access-authenticator 4-8
sysname(config)# port-access-authenticator 4-8 reauthenticate
sysname(config)# port-access-authenticator 4-8 reauth-period 1800
```

This example configures the Switch in the following ways:

1. Disables authentication on the Switch.
2. Disables re-authentication on ports 1, 3, 4, and 5.
3. Disables authentication on ports 1, 6, and 7.

```
sysname(config)# no port-access-authenticator
sysname(config)# no port-access-authenticator 1,3-5 reauthenticate
sysname(config)# no port-access-authenticator 1,6-7
```

21

IGMP and Multicasting Commands

This chapter explains how to use commands to configure the Internet Group Membership Protocol (IGMP) on the Switch. It also covers configuring the ports to remove the VLAN tag from outgoing multicast packets on the Switch.

21.1 IGMP Overview

The Switch supports IGMP version 1 (**IGMP-v1**), version 2 (**IGMP-v2**) and IGMP version 3 (**IGMP-v3**). Refer to RFC 1112, RFC 2236 and RFC 3376 for information on IGMP versions 1, 2 and 3 respectively. At start up, the Switch queries all directly connected networks to gather group membership. After that, the Switch periodically updates this information.

21.2 Command Summary

The following section lists the commands for this feature.

Table 55 IGMP Command Summary

COMMAND	DESCRIPTION	M	P
`router igmp`	Enables and enters the IGMP configuration mode.	C	13
`exit`	Leaves the IGMP configuration mode.	C	13
`non-querier`	Sets the Switch to Non-Querier mode. (If the Switch discovers a multicast router with a lower IP address, it will stop sending Query messages on that network.)	C	13
`no non-querier`	Disables non-querier mode on the Switch, (the multicast router always sends Query messages).	C	13
`unknown-multicast-frame <drop|flooding>`	Specifies the action the Switch should perform when it receives unknown multicast frames.	C	13
`no router igmp`	Disables IGMP on the Switch.	C	13
`interface route-domain <`*`ip-address`*`>/<`*`mask-bits`*`>`	Enters the configuration mode for the specified routing domain.	C	13

Table 55 IGMP Command Summary (continued)

COMMAND	DESCRIPTION	M	P
ip igmp <v1|v2|v3>	Enables IGMP in this routing domain and specifies the version of the IGMP packets that the Switch should use.	C	13
ip igmp robustness-variable <2-255>	Sets the IGMP robustness variable on the Switch. This variable specifies how susceptible the subnet is to lost packets.	C	13
ip igmp query-interval	Sets the igmp query interval on the Switch. This variable specifies the amount of time in seconds between general query messages sent by the router.	C	13
ip igmp query-max-response-time <1-25>	Sets the maximum time that the router waits for a response to a general query message.	C	13
ip igmp last-member-query-interval <1-25>	Sets the amount of time in seconds that the router waits for a response to a group specific query message.	C	13
no ip igmp	Disables IP IGMP in this routing domain.	C	13

Table 56 IPMC Command Summary

COMMAND	DESCRIPTION	M	P
interface port-channel <*port-list*>	Enters config-interface mode for the specified port(s).	C	13
ipmc egress-untag-vlan <*vlan-id*>	Sets the Switch to remove the VLAN tag from IP multicast packets belonging to the specified VLAN before transmission on this port. Enter a VLAN group ID in this field. Enter 0 to set the Switch not to remove any VLAN tags from the packets.	C	13
no ipmc egress-untag-vlan	Disables the ports from removing the VLAN tags from outgoing IP multicast packets.	C	13

21.3 Command Examples

This example configures IGMP on the Switch with the following settings:

- Sets the Switch to flood unknown multicast frames.
- Sets the Switch to non-querier mode.
- Configures the IP interface **172.16.1.1** with subnet mask **255.255.255.0** to route IGMP version **3** packets.

```
sysname(config)# router igmp
sysname(config-igmp)# non-querier
sysname(config-igmp)# unknown-multicast-frame flooding
sysname(config-igmp)# exit
sysname(config)# interface route-domain 172.16.1.1/24
sysname(config-if)# ip igmp v3
```

22

IGMP Snooping Commands

Use these commands to configure IGMP snooping on the Switch.

See Chapter 23 on page 95 for IGMP filtering commands.

22.1 Command Summary

The following section lists the commands for this feature.

Table 57 igmp-flush Command Summary

COMMAND	DESCRIPTION	M	P
`igmp-flush`	Removes all multicast group information.	E	13

Table 58 igmp-snooping Command Summary

COMMAND	DESCRIPTION	M	P
`show igmp-snooping`	Displays global IGMP snooping settings.	E	3
`show multicast [vlan]`	Displays multicast status, including the port number, VLAN ID and multicast group members on the Switch. Optionally, displays the type of each multicast VLAN.	E	3
`igmp-snooping`	Enables IGMP snooping.	C	13
`no igmp-snooping`	Disables IGMP snooping.	C	13
`igmp-snooping 8021p-priority <0-7>`	Sets the 802.1p priority for outgoing igmp snooping packets.	C	13
`no igmp-snooping 8021p-priority`	Disables changing the priority of outgoing IGMP control packets.	C	13
`igmp-snooping host-timeout <1-16711450>`	Sets the host timeout value.	C	13
`igmp-snooping leave-timeout <1-16711450>`	Sets the leave timeout value	C	13
`igmp-snooping reserved-multicast-frame <drop|flooding>`	Sets how to treat traffic with a reserved multicast address. Reserved multicast addresses are in the range 224.0.0.0 to 224.0.0.255.	C	13
`igmp-snooping unknown-multicast-frame <drop|flooding>`	Sets how to treat traffic from unknown multicast groups.	C	13
`show igmp-snooping querier`	Displays the IGMP query mode for the specified port(s).	E	3

Table 58 igmp-snooping Command Summary (continued)

COMMAND	DESCRIPTION	M	P
`igmp-snooping querier`	Enables the IGMP snooping querier on the Switch.	C	13
`no igmp-snooping querier`	Disables the IGMP snooping querier on the Switch.	C	13

Table 59 igmp-snooping vlan Command Summary

COMMAND	DESCRIPTION	M	P
`show igmp-snooping vlan`	Displays the VLANs on which IGMP snooping is enabled.	E	3
`igmp-snooping vlan mode <auto|fixed>`	Specifies how the VLANs on which the Switch snoops IGMP packets are selected. `auto`: The Switch learns multicast group membership on any VLAN. See the User's Guide for the maximum number of VLANs the switch supports for IGMP snooping. The Switch drops any IGMP control messages on other VLANs after it reaches this maximum number (`auto` mode). `fixed`: The Switch only learns multicast group membership on specified VLAN(s). The Switch drops any IGMP control messages for any unspecified VLANs (`fixed` mode). See the User's Guide for the maximum number of VLANs the switch supports for IGMP snooping.	C	13
`igmp-snooping vlan <vlan-id> [name <name>]`	Specifies which VLANs to perform IGMP snooping on if the mode is `fixed`. Optionally, sets a name for the multicast VLAN. *name*: 1-32 printable characters; spaces are allowed if you put the string in double quotation marks (“).	C	13
`no igmp-snooping vlan <vlan-id>`	Removes IGMP snooping configuration on the specified VLAN if the mode is `fixed`.	C	13

Table 60 interface igmp Command Summary

COMMAND	DESCRIPTION	M	P
`show interfaces config <port-list> igmp-group-limited`	Displays the group limits for IGMP snooping.	E	3
`show interfaces config <port-list> igmp-immediate-leave`	Displays the immediate leave settings for IGMP snooping.	E	3
`show interfaces config <port-list> igmp-query-mode`	Displays the IGMP query mode for the specified port(s).	E	3
`interface port-channel <port-list>`	Enters config-interface mode for the specified port(s).	C	13
`igmp-group-limited`	Enables the group limiting feature for IGMP snooping. You must enable IGMP snooping as well.	C	13
`igmp-group-limited number <number>`	Sets the maximum number of multicast groups allowed. *number*: 0-255	C	13
`no igmp-group-limited`	Disables multicast group limits.	C	13
`igmp-immediate-leave`	Enables the immediate leave function for IGMP snooping. You must enable IGMP snooping as well.	C	13

Table 60 interface igmp Command Summary (continued)

COMMAND	DESCRIPTION	M	P
`no igmp-immediate-leave`	Disables the immediate leave function for IGMP snooping.	C	13
`igmp-querier-mode <auto|fixed|edge>`	Specifies whether or not and under what conditions the port(s) is (are) IGMP query port(s). The Switch forwards IGMP join or leave packets to an IGMP query port, treating the port as being connected to an IGMP multicast router (or server). You must enable IGMP snooping as well. `fixed`: The Switch always treats the port(s) as IGMP query port(s). Select this when you connect an IGMP multicast server to the port(s). `auto`: The Switch uses the port as an IGMP query port if the port receives IGMP query packets. `edge`: The Switch does not use the port as an IGMP query port. The Switch does not keep any record of an IGMP router being connected to this port. The Switch does not forward IGMP join or leave packets to this port.	C	13

22.2 Command Examples

This example enables IGMP snooping on the Switch, sets the `host-timeout` and `leave-timeout` values to 30 seconds, and sets the Switch to drop packets from unknown multicast groups.

```
sysname(config)# igmp-snooping
sysname(config)# igmp-snooping host-timeout 30
sysname(config)# igmp-snooping leave-timeout 30
sysname(config)# igmp-snooping unknown-multicast-frame drop
```

This example limits the number of multicast groups on port 1 to 5.

```
sysname# configure
sysname(config)# igmp-snooping
sysname(config)# interface port-channel 1
sysname(config-interface)# igmp-group-limited
sysname(config-interface)# igmp-group-limited number 5
sysname(config-interface)# exit
sysname(config)# exit
sysname# show interfaces config 1 igmp-group-limited
  Port          Enable          Max Multicast Group
   1              YES                5
```

This example shows the current multicast groups on the Switch.

```
sysname# show multicast
  Multicast Status

  Index   VID    Port   Multicast Group    Timeout
  -----   ----   ----   ----------------   -------
```

The following table describes the labels in this screen.

Table 61 show multicast

LABEL	DESCRIPTION
Index	This field displays an entry number for the VLAN.
VID	This field displays the multicast VLAN ID.
Port	This field displays the port number that belongs to the multicast group.
Multicast Group	This field displays the IP multicast group addresses.
Timeout	This field displays how long the port will belong to the multicast group.

This example shows the current multicast VLAN on the Switch.

```
sysname# show multicast vlan
  Multicast Vlan Status

  Index   VID    Type
  -----   ----   ----------
      1   3      MVR
```

23

IGMP Filtering Commands

Use these commands to configure IGMP filters and IGMP filtering on the Switch.

23.1 Command Summary

The following section lists the commands for this feature.

Table 62 igmp-filtering Command Summary

COMMAND	DESCRIPTION	M	P
`show igmp-filtering profile`	Displays IGMP filtering profile settings.	E	3
`igmp-filtering`	Enables IGMP filtering on the Switch. Ports can only join multicast groups specified in their IGMP filtering profile.	C	13
`no igmp-filtering`	Disables IGMP filtering on the Switch.	C	13
`igmp-filtering profile <name> start-address <ip> end-address <ip>`	Sets the range of multicast address(es) in a profile. *name*: 1-32 alphanumeric characters	C	13
`no igmp-filtering profile <name>`	Removes the specified IGMP filtering profile. You cannot delete an IGMP filtering profile that is assigned to any ports.	C	13
`no igmp-filtering profile <name> start-address <ip> end-address <ip>`	Clears the specified rule of the specified IGMP filtering profile.	C	13
`show interfaces config <port-list> igmp-filtering`	Displays IGMP filtering settings.	E	3
`interface port-channel <port-list>`	Enters config-interface mode for the specified port(s).	C	13
`igmp-filtering profile <name>`	Assigns the specified IGMP filtering profile to the port(s). If IGMP filtering is enabled on the Switch, the port(s) can only join the multicast groups in the specified profile.	C	13
`no igmp-filtering profile`	Prohibits the port(s) from joining any multicast groups if IGMP filtering is enabled on the Switch.	C	13

23.2 Command Examples

This example restricts ports 1-4 to multicast IP addresses 224.255.255.0 through 225.255.255.255.

```
sysname# configure
sysname(config)# igmp-filtering
sysname(config)# igmp-filtering profile example1 start-address
--> 224.255.255.0 end-address 225.255.255.255
sysname(config)# interface port-channel 1-4
sysname(config-interface)# igmp-filtering profile example1
sysname(config-interface)# exit
sysname(config)# exit
```

24

Interface Commands

Use these commands to configure basic port settings.

24.1 Command Summary

The following section lists the commands for this feature.

Table 63 interface Command Summary

COMMAND	DESCRIPTION	M	P
`show interfaces <port-list>`	Displays the current interface status.	E	3
`no interface <port-number>`	Clears all statistics for the specified port.	E	13
`show interfaces config <port-list>`	Displays current interface configuration.	E	3
`interface port-channel <port-list>`	Enters config-interface mode for the specified port(s).	C	13
`inactive`	Disables the specified port(s) on the Switch.	C	13
`no inactive`	Enables the port(s) on the Switch.	C	13
`name <port-name-string>`	Sets a name for the port(s). *port-name-string*: up to 64 English keyboard characters	C	13
`speed-duplex <auto|10-half|10-full|100-half|100-full|1000-full>`	Sets the duplex mode (`half` or `full`) and speed (`10`, `100` or `1000` Mbps) of the connection on the interface. Select `auto` (auto-negotiation) to let the specified port(s) negotiate with a peer to obtain the connection speed and duplex mode.	C	13
`flow-control`	Enables interface flow control. Flow control regulates transmissions to match the bandwidth of the receiving port.	C	13
`no flow-control`	Disables flow control on the port(s).	C	13
`qos priority <0-7>`	Sets the quality of service priority for an interface.	C	13
`frame-type <all|tagged|untagged>`	Choose to accept both tagged and untagged incoming frames (`all`), just tagged incoming frames (`tagged`) or just untagged incoming frames on a port (`untagged`). Note: Not all switch models support accepting untagged frames on a port.	C	13
`pvid <1-4094>`	The default PVID is VLAN 1 for all ports. Sets a PVID in the range 1 to 4094 for the specified interface.	C	13

Table 63 interface Command Summary (continued)

COMMAND	DESCRIPTION	M	P
intrusion-lock	Enables intrusion lock on the port(s) and a port cannot be connected again after you disconnected the cable.	C	13
no intrusion-lock	Disables intrusion-lock on a port so that a port can be connected again after you disconnected the cable.	C	13

24.2 Command Examples

This example looks at the current status of port 1.

```
sysname# show interfaces 1
  Port Info     Port NO.                :1
                Link                    :100M/F
                Status                  :FORWARDING
                LACP                    :Disabled
                TxPkts                  :7214
                RxPkts                  :395454
                Errors                  :0
                Tx KBs/s                :0.0
                Rx KBs/s                :0.0
                Up Time                 :127:26:26
  TX Packet     Tx Packets              :7214
                Multicast               :0
                Broadcast               :163
                Pause                   :0
  RX Packet     Rx Packets              :395454
                Multicast               :186495
                Broadcast               :200177
                Pause                   :0
  TX Collison   Single                  :0
                Multiple                :0
                Excessive               :0
                Late                    :0
  Error Packet  RX CRC                  :0
                Runt                    :0
  Distribution  64                      :285034
                65 to 127               :31914
                128 to 255              :22277
                256 to 511              :50546
                512 to 1023             :1420
                1024 to 1518            :4268
                Giant                   :0
```

The following table describes the labels in this screen.

Table 64 show interfaces

LABEL	DESCRIPTION
Port Info	
Port NO.	This field displays the port number you are viewing.

Table 64 show interfaces (continued)

LABEL	DESCRIPTION
Link	This field displays the speed (either **10M** for 10 Mbps, **100M** for 100 Mbps or **1000M** for 1000 Mbps) and the duplex (**F** for full duplex or **H** for half duplex). It also shows the cable type (**Copper** or **Fiber**). This field displays **Down** if the port is not connected to any device.
Status	If STP (Spanning Tree Protocol) is enabled, this field displays the STP state of the port. If STP is disabled, this field displays FORWARDING if the link is up, otherwise, it displays STOP.
LACP	This field shows if LACP is enabled on this port or not.
TxPkts	This field shows the number of transmitted frames on this port
RxPkts	This field shows the number of received frames on this port
Errors	This field shows the number of received errors on this port.
Tx KBs/s	This field shows the number kilobytes per second transmitted on this port.
Rx KBs/s	This field shows the number of kilobytes per second received on this port.
Up Time	This field shows the total amount of time the connection has been up.
Tx Packet The following fields display detailed information about packets transmitted.	
TX Packets	This field shows the number of good packets (unicast, multicast and broadcast) transmitted.
Multicast	This field shows the number of good multicast packets transmitted.
Broadcast	This field shows the number of good broadcast packets transmitted.
Pause	This field shows the number of 802.3x Pause packets transmitted.
Rx Packet The following fields display detailed information about packets received.	
RX Packets	This field shows the number of good packets (unicast, multicast and broadcast) received.
Multicast	This field shows the number of good multicast packets received.
Broadcast	This field shows the number of good broadcast packets received.
Pause	This field shows the number of 802.3x Pause packets received.
TX Collision The following fields display information on collisions while transmitting.	
Single	This is a count of successfully transmitted packets for which transmission is inhibited by exactly one collision.
Multiple	This is a count of successfully transmitted packets for which transmission was inhibited by more than one collision.
Excessive	This is a count of packets for which transmission failed due to excessive collisions. Excessive collision is defined as the number of maximum collisions before the retransmission count is reset.
Late	This is the number of times a late collision is detected, that is, after 512 bits of the packets have already been transmitted.
Error Packet	The following fields display detailed information about packets received that were in error.
RX CRC	This field shows the number of packets received with CRC (Cyclic Redundant Check) error(s).
Runt	This field shows the number of packets received that were too short (shorter than 64 octets), including the ones with CRC errors.

Table 64 show interfaces (continued)

LABEL	DESCRIPTION
Distribution	
64	This field shows the number of packets (including bad packets) received that were 64 octets in length.
65-127	This field shows the number of packets (including bad packets) received that were between 65 and 127 octets in length.
128-255	This field shows the number of packets (including bad packets) received that were between 128 and 255 octets in length.
256-511	This field shows the number of packets (including bad packets) received that were between 256 and 511 octets in length.
512-1023	This field shows the number of packets (including bad packets) received that were between 512 and 1023 octets in length.
1024-1518	This field shows the number of packets (including bad packets) received that were between 1024 and 1518 octets in length.
Giant	This field shows the number of packets dropped because they were bigger than the maximum frame size.

This example configures ports 1, 3, 4, and 5 in the following ways:

1. Sets the IEEE 802.1p quality of service priority to four (4).
2. Sets the name “Test”.
3. Sets the speed to 100 Mbps in half duplex mode.

```
sysname(config)# interface port-channel 1,3-5
sysname(config-interface)# qos priority 4
sysname(config-interface)# name Test
sysname(config-interface)# speed-duplex 100-half
```

This example configures ports 1-5 in the following ways:

1. Sets the default port VID to 200.
2. Sets these ports to accept only tagged frames.

```
sysname (config)# interface port-channel 1-5
sysname (config-interface)# pvid 200
sysname (config-interface)# frame-type tagged
```

25

Interface Route-domain Mode

In order to configure layer 3 routing features on the Switch, you must enter the interface routing domain mode in the CLI.

25.1 Command Summary

The following section lists the commands for this feature.

Table 65 Interface Route Domain Command Summary:

COMMAND	DESCRIPTION	M	P
`interface route-domain <ip-address>/<mask-bits>`	Enters the configuration mode for this routing domain. The mask-bits are defined as the number of bits in the subnet mask. Enter the subnet mask number preceded with a "/". To find the bit number, convert the subnet mask to binary and add all of the 1's together. Take "255.255.255.0" for example. 255 converts to eight 1's in binary. There are three 255's, so add three eights together and you get the bit number (24).	C	13
`exit`	Exits from the interface routing-domain configuration mode.	C	13

25.2 Command Examples

Use this command to enable/create the specified routing domain for configuration.

- Enter the configuration mode.
- Enable default routing domain (the 192.168.1.1 subnet) for configuration.
- Begin configuring for this domain.

```
sysname# config
sysname(config)# interface route-domain 192.168.1.1/24
sysname(config-if)#
```

26

IP Commands

Use these commands to configure the management port IP address, default domain name server and to look at IP domains.

See Chapter 55 on page 179 for static route commands.

See Chapter 27 on page 107 for IP source binding commands.

26.1 Command Summary

The following section lists the commands for this feature.

Table 66 ip Command Summary

COMMAND	DESCRIPTION	M	P
`show ip`	Displays current IP interfaces.	E	0
`ip name-server <ip>`	Sets the IP address of the domain name server.	C	13
`ip address <ip> <mask>`	Sets the IP address of the **MGMT** port (for out-of-band management) on the Switch.	E	0
`ip address default-gateway <ip>`	Sets the default gateway for the out-of-band management interface on the Switch.	C	13
`show ip iptable all [IP|VID|PORT]`	Displays the IP address table. You can sort the table based on the IP address, VLAN ID or the port number.	E	3
`show ip iptable count`	Displays the number of IP interfaces configured on the Switch.	E	3
`show ip iptable static`	Displays the static IP address table.	E	3

Table 67 tcp and udp Command Summary

COMMAND	DESCRIPTION	M	P
`show ip tcp`	Displays IP TCP information.	E	3

Table 67 tcp and udp Command Summary (continued)

COMMAND	DESCRIPTION	M	P
`show ip udp`	Displays IP UDP information.	E	3
`kick tcp <session id>`	Disconnects the specified TCP session. *session id*: Display the session id by running the `show ip tcp` command. See Section 26.2 on page 104 for an example.	E	13

26.2 Command Examples

This example shows the TCP statistics and listener ports. See RFC 1213 for more information.

```
sysname# show ip tcp
( 1)tcpRtoAlgorithm              4     ( 2)tcpRtoMin                    0
( 3)tcpRtoMax           4294967295     ( 4)tcpMaxConn          4294967295
( 5)tcpActiveOpens               2     ( 6)tcpPassiveOpens            188
( 7)tcpAttemptFails              3     ( 8)tcpEstabResets              25
( 9)tcpCurrEstab                 1     (10)tcpInSegs                 4025
(11)tcpOutSegs                5453     (12)tcpRetransSegs              64
(14)tcpInErrs                    0     (15)tcpOutRsts                   0
    &TCB Rcv-Q Snd-Q Rcv-Wnd Snd-Wnd Local socket           Remote socket
   State
80d60868     0   620     128   63907  172.16.37.206:23       172.16.5.15:1510
    Estab
80d535a0     0     0     128       1  0.0.0.0:23              0.0.0.0:0
    Listen (S)
80d536bc     0     0   16384       1  0.0.0.0:80              0.0.0.0:0
    Listen (S)
80d5f6a8     0     0   22400       1  0.0.0.0:21              0.0.0.0:0
    Listen
80d5440c     0     0     128       1  0.0.0.0:22              0.0.0.0:0
    Listen
80d541d4     0     0   22400       1  0.0.0.0:443             0.0.0.0:0
    Listen (S)
```

The following table describes the labels in this screen.

Table 68 show ip tcp

LABEL	DESCRIPTION
tcpRtoAlgorithm	This field displays the algorithm used to determine the timeout value that is used for retransmitting unacknowledged octets.
tcpRtoMin	This field displays the minimum timeout (in milliseconds) permitted by a TCP implementation for the retransmission timeout. More refined semantics for objects of this type depend upon the algorithm used to determine the retransmission timeout. In particular, when the timeout algorithm is rsre(3), an object of this type has the semantics of the LBOUND quantity described in RFC 793.
tcpRtoMax	This field displays the maximum timeout (in milliseconds) permitted by a TCP implementation for the retransmission timeout. More refined semantics for objects of this type depend upon the algorithm used to determine the retransmission timeout. In particular, when the timeout algorithm is rsre(3), an object of this type has the semantics of the UBOUND quantity described in RFC 793.

Table 68 show ip tcp (continued)

LABEL	DESCRIPTION
tcpMaxConn	This field displays the maximum number of TCP connections the Switch can support. If the maximum number is dynamic, this field displays -1.
tcpActiveOpens	This field displays the number of times TCP connections have made a direct transition to the SYN-SENT state from the CLOSED state.
tcpPassiveOpens	This field displays the number of times TCP connections have made a direct transition to the SYN-RCVD state from the LISTEN state.
tcpAttemptFails	This field displays the number of times TCP connections have made a direct transition to the CLOSED state from either the SYN-SENT state or the SYN-RCVD state, plus the number of times TCP connections have made a direct transition to the LISTEN state from the SYN-RCVD state.
tcpEstabResets	This field displays the number of times TCP connections have made a direct transition to the CLOSED state from either the ESTABLISHED state or the CLOSE-WAIT state.
tcpCurrEstab	This field displays the number of TCP connections for which the current state is either ESTABLISHED or CLOSE-WAIT.
tcpInSegs	This field displays the total number of segments received, including those received in error. This count includes segments received on currently established connections.
tcpOutSegs	This field displays the total number of segments sent, including those on current connections but excluding those containing only retransmitted octets.
tcpRetransSegs	This field displays the total number of TCP segments transmitted containing one or more previously transmitted octets.
tcpInErrs	This field displays the total number of segments received with error (for example, bad TCP checksums).
tcpOutRsts	This field displays the number of TCP segments sent containing the RST flag.
	This section displays the current TCP listeners.
&TCB	This field displays the session ID.
Rcv-Q	This field displays the items on the receive queue in this connection.
Snd-Q	This field displays the sequence number of the first unacknowledged segment on the send queue in this connection.
Rcv-Wnd	This field displays the receiving window size in this connection. It determines the amount of received data that can be buffered.
Snd-Wnd	This field displays the sending window size in this connection. It is offered by the remote device.
Local socket	This field displays the local IP address and port number in this TCP connection. In the case of a connection in the LISTEN state that is willing to accept connections for any IP interface associated with the node, the value is 0.0.0.0.

Table 68 show ip tcp (continued)

LABEL	DESCRIPTION
Remote socket	This field displays the remote IP address and port number in this TCP connection.
State	This field displays the state of this TCP connection. The only value which may be set by a management station is deleteTCB(12). Accordingly, it is appropriate for an agent to return a `badValue' response if a management station attempts to set this object to any other value. If a management station sets this object to the value deleteTCB(12), then this has the effect of deleting the TCB (as defined in RFC 793) of the corresponding connection on the managed node, resulting in immediate termination of the connection. As an implementation-specific option, a RST segment may be sent from the managed node to the other TCP endpoint (note however that RST segments are not sent reliably).

This example shows the UDP statistics and listener ports. See RFC 1213 for more information.

```
sysname# show ip udp
( 1)udpInDatagrams           10198     ( 2)udpNoPorts               81558
( 3)udpInErrors                  0     ( 4)udpOutDatagrams             13
    &UCB Rcv-Q  Local socket
80bfdac0     0  0.0.0.0:53
80bfd9ac     0  0.0.0.0:520
80c78888     0  0.0.0.0:161
80c79184     0  0.0.0.0:162
80c3188c     0  0.0.0.0:1027
80c31830     0  0.0.0.0:1026
80bfdb78     0  0.0.0.0:1025
80bfdb1c     0  0.0.0.0:1024
80bfda64     0  0.0.0.0:69
80bfda08     0  0.0.0.0:263
```

The following table describes the labels in this screen.

Table 69 show ip udp

LABEL	DESCRIPTION
udpInDatagrams	This field displays the total number of UDP datagrams delivered to UDP users.
udpNoPorts	This field displays the total number of received UDP datagrams for which there was no application at the destination port.
udpInErrors	This field displays the number of received UDP datagrams that could not be delivered for reasons other than the lack of an application at the destination port.
udpOutDatagrams	This field displays the total number of UDP datagrams sent by the Switch.
&UCB	This field displays the process ID.
Rcv-Q	This field displays the queue number of pending datagrams in this connection.
Local socket	This field displays the local IP address and port number for this UDP listener. In the case of a UDP listener that is willing to accept datagrams for any IP interface associated with the node, the value is 0.0.0.0.

27

IP Source Binding Commands

Use these commands to manage the bindings table for IP source guard.

27.1 Command Summary

The following section lists the commands for this feature.

Table 70 ip source binding Command Summary

COMMAND	DESCRIPTION	M	P
`show ip source binding [<mac-addr>] [...]`	Displays the bindings configured on the Switch, optionally based on the specified parameters.	E	3
`show ip source binding help`	Provides more information about the specified command.	E	3
`ip source binding <mac-addr> vlan <vlan-id> <ip> [interface port-channel <interface-id>]`	Creates a static binding for ARP inspection.	C	13
`no ip source binding <mac-addr> vlan <vlan-id>`	Removes the specified static binding.	C	13

27.2 Command Examples

This example shows the current binding table.

```
sysname# show ip source binding
        MacAddress        IpAddress         Lease           Type  VLAN   Port
  -----------------  ---------------  ------------  -------------  ----  ---
  Total number of bindings: 0
```

The following table describes the labels in this screen.

Table 71 show ip source binding

LABEL	DESCRIPTION
MacAddress	This field displays the source MAC address in the binding.
IpAddress	This field displays the IP address assigned to the MAC address in the binding.
Lease	This field displays how many days, hours, minutes, and seconds the binding is valid; for example, **2d3h4m5s** means the binding is still valid for 2 days, 3 hours, 4 minutes, and 5 seconds. This field displays **infinity** if the binding is always valid (for example, a static binding).

Table 71 show ip source binding (continued)

LABEL	DESCRIPTION
Type	This field displays how the switch learned the binding. **static**: This binding was learned from information provided manually by an administrator.
VLAN	This field displays the source VLAN ID in the binding.
Port	This field displays the port number in the binding. If this field is blank, the binding applies to all ports.

28

Logging Commands

Use these commands to manage system logs.

28.1 Command Summary

The following section lists the commands for this feature.

Table 72 logging Command Summary

COMMAND	DESCRIPTION	M	P
`show logging`	Displays system logs.	E	3
`no logging`	Clears system logs.	E	13

28.2 Command Examples

This example displays the system logs.

```
sysname# show logging
   1 Thu Jan  1 00:02:08 1970 PP05 -WARN  SNMP TRAP 3: link up
   2 Thu Jan  1 00:03:14 1970       INFO  adjtime task pause 1 day
   3 Thu Jan  1 00:03:16 1970 PP0f -WARN  SNMP TRAP 26: Event On Trap
   4 Thu Jan  1 00:03:16 1970 PINI -WARN  SNMP TRAP 1: warm start
   5 Thu Jan  1 00:03:16 1970 PINI -WARN  SNMP TRAP 3: link up
   6 Thu Jan  1 00:03:16 1970 PINI  INFO  main: init completed
   7 Thu Jan  1 00:00:13 1970 PP26  INFO  adjtime task pause 1 day
   8 Thu Jan  1 00:00:14 1970 PP0f -WARN  SNMP TRAP 26: Event On Trap
   9 Thu Jan  1 00:00:14 1970 PINI -WARN  SNMP TRAP 0: cold start
  10 Thu Jan  1 00:00:14 1970 PINI  INFO  main: init completed
  11 Thu Jan  1 00:00:04 1970 PP05 -WARN  SNMP TRAP 3: link up
  11 Thu Jan  1 00:00:04 1970 PP05 -WARN  SNMP TRAP 3: link up
Clear Error Log (y/n):
```

29

Login Account Commands

Use these commands to configure login accounts on the Switch.

29.1 Command Summary

The following section lists the commands for this feature.

Table 73 logins Command Summary

COMMAND	DESCRIPTION	M	P
`show logins`	Displays login account information.	E	3
`logins username <name> password <password>`	Creates account with the specified user name and sets the password. *name*: 1-32 alphanumeric characters *password*: 1-32 alphanumeric characters	C	14
`no logins username <name>`	Removes specified account.	C	14
`logins username <name> privilege <0-14>`	Assigns a privilege level to the specified account. The privilege level is applied the next time the user logs in.	C	14

29.2 Command Examples

This example creates a new user **user2** with privilege 13.

```
sysname# configure
sysname(config)# logins username user2 password 1234
sysname(config)# logins username user2 privilege 13
sysname(config)# exit
sysname# show logins
Login   Username                                  Privilege
1       user2                                    13
2                                                 0
3                                                 0
4                                                 0
```

30

Loopguard Commands

Use these commands to configure the Switch to guard against loops on the edge of your network. The Switch shuts down a port if the Switch detects that packets sent out on the port loop back to the Switch.

30.1 Command Summary

The following section lists the commands for this feature.

Table 74 loopguard Command Summary

COMMAND	DESCRIPTION	M	P
`show loopguard`	Displays which ports have loopguard enabled as well as their status.	E	3
`loopguard`	Enables loopguard on the Switch.	C	13
`no loopguard`	Disables loopguard on the Switch.	C	13
`interface port-channel <port-list>`	Enters config-interface mode for the specified port(s).	C	13
`loopguard`	Enables the loopguard feature on the port(s). You have to enable loopguard on the Switch as well. The Switch shuts down a port if the Switch detects that packets sent out on the port loop back to the Switch.	C	13
`no loopguard`	Disables the loopguard feature on the port(s).	C	13
`clear loopguard`	Clears loopguard counters.	E	13

30.2 Command Examples

This example enables loopguard on ports 1-3.

```
sysname# configure
sysname(config)# loopguard
sysname(config)# interface port-channel 1-3
sysname(config-interface)# loopguard
sysname(config-interface)# exit
sysname(config)# exit
sysname# show loopguard
  LoopGuard Status: Enable

  Port  Port      LoopGuard  Total     Total     Bad   Shutdown
  No    Status    Status     TxPkts    RxPkts    Pkts  Time
  ----  --------  ---------  --------  --------  ----  ------------------
     1    Active     Enable         0         0     0   00:00:00 UTC Jan
1 1970
     2    Active     Enable         0         0     0   00:00:00 UTC Jan
1 1970
     3    Active     Enable         0         0     0   00:00:00 UTC Jan
1 1970
     4    Active    Disable         0         0     0   00:00:00 UTC Jan
1 1970
--------------------------------- SNIP ---------------------------------
```

The following table describes the labels in this screen.

Table 75 show loopguard

LABEL	DESCRIPTION
LoopGuard Status	This field displays whether or not loopguard is enabled on the Switch.
Port No	This field displays the port number.
Port Status	This field displays whether or not the port is active.
LoopGuard Status	This field displays whether or not loopguard is enabled on the port.
Total TxPkts	This field displays the number of packets that have been sent on this port since loopguard was enabled on the port.
Total RxPkts	This field displays the number of packets that have been received on this port since loopguard was enabled on the port.
Bad Pkts	This field displays the number of invalid probe packets that were received on this port.
Shutdown Time	This field displays the last time the port was shut down because a loop state was detected.

31

MAC Address Commands

Use these commands to look at the MAC address table and to configure MAC address learning. The Switch uses the MAC address table to determine how to forward frames.

31.1 Command Summary

The following section lists the commands for this feature.

Table 76 mac, mac-aging-time, and mac-flush Command Summary

COMMAND	DESCRIPTION	M	P
`show mac-aging-time`	Displays MAC learning aging time.	E	3
`mac-aging-time <10-3000>`	Sets learned MAC aging time in seconds.	C	13
`show mac address-table all [<sort>]`	Displays MAC address table. You can sort by MAC address, VID or port. *sort*: MAC, VID, or PORT.	E	3
`show mac address-table count`	Displays the total number of MAC addresses in the MAC address table.	E	3
`show mac address-table port <port-list> [<sort>]`	Displays the MAC address table for the specified port(s). Sorted by MAC, Port or VID. *sort*: MAC, VID, or PORT.	E	3
`show mac address-table static`	Displays the static MAC address table.	E	3
`show mac address-table vlan <vlan-id> [<sort>]`	Displays the MAC address table for the specified VLAN. Optionally, sorted by MAC or port. *sort*: MAC or PORT.	E	3
`mac-flush [<port-num>]`	Clears the MAC address table. Optionally, removes all learned MAC address on the specified port.	E	13

31.2 Command Examples

This example shows the current MAC address table.

```
sysname# show mac address-table all
Port      VLAN ID        MAC Address         Type
2         1              00:00:e8:7c:14:80   Dynamic
2         1              00:04:80:9b:78:00   Dynamic
2         1              00:0f:fe:ad:58:ab   Dynamic
2         1              00:13:49:6b:10:55   Dynamic
2         1              00:13:d3:f0:7e:f0   Dynamic
2         1              00:18:f8:04:f5:67   Dynamic
2         1              00:80:c8:ef:81:d3   Dynamic
2         1              00:a0:c5:00:00:01   Dynamic
```

The following table describes the labels in this screen.

Table 77 show mac address-table

LABEL	DESCRIPTION
Port	This is the port from which the above MAC address was learned. **Drop**: The entry is created from a filtering rule.
VLAN ID	This is the VLAN group to which this frame belongs.
MAC Address	This is the MAC address of the device from which this frame came.
Type	This shows whether the MAC address is **dynamic** (learned by the Switch) or **static** (manually entered using `mac-forward` commands, see Chapter 34 on page 121).

32

MAC Authentication Commands

Use these commands to configure MAC authentication on the Switch.

32.1 MAC Authentication Overview

MAC authentication allows you to validate access to a port based on the MAC address and password of the client.

You also need to configure a RADIUS server (see Chapter 48 on page 161).

See also Chapter 20 on page 87 for IEEE 802.1x port authentication commands and Chapter 44 on page 151 for port security commands.

32.2 Command Summary

The following section lists the commands for this feature.

Table 78 mac-authentication Command Summary

COMMAND	DESCRIPTION	M	P
`show mac-authentication`	Displays MAC authentication settings for the Switch.	E	3
`show mac-authentication config`	Displays MAC authentication settings on a port by port basis with authentication statistics for each port.	E	3
`mac-authentication`	Enables MAC authentication on the Switch.	C	13
`mac-authentication nameprefix <name-string>`	Sets the prefix appended to the MAC address before it is sent to the RADIUS server for authentication. The prefix can be up to 32 printable ASCII characters.	C	13
`mac-authentication password <name-string>`	Sets the password sent to the RADIUS server for clients using MAC authentication. The password can be up to 32 printable ASCII characters.	C	13
`mac-authentication timeout <1-3000>`	Specifies the amount of time before the Switch allows a client MAC address that fails authentication to try and authenticate again. This settings is superseded by the `mac-aging-time` command.	C	13
`no mac-authentication`	Disables MAC authentication on the Switch.	C	13

Table 78 mac-authentication Command Summary (continued)

COMMAND	DESCRIPTION	M	P
`no mac-authentication timeout`	Sets the MAC address entries learned via MAC authentication to never age out.	C	13
`interface port-channel <port-list>`	Enables a port or a list of ports for configuration.	C	13
`mac-authentication`	Enables MAC authentication via a RADIUS server on the port(s).	C	13
`no mac-authentication`	Disables MAC authentication via a RADIUS server on the port(s).	C	13

32.3 Command Examples

This example enables MAC authentication on the Switch. Specifies the name prefix **clientName** and the MAC authentication password **Lech89**. Next, MAC authentication is activated on ports 1 - 5 and configuration details are displayed.

```
sysname(config)# mac-authentication
sysname(config)# mac-authentication nameprefix clientName
sysname(config)# mac-authentication password Lech89
sysname(config)# interface port-channel 1-5
sysname(config-interface)# mac-authentication
sysname(config-interface)# exit
sysname(config)# exit
sysname# show mac-authentication
NamePrefix:     clientName
Password:       Lech89
Update Time:    None
Deny Number:    0
```

33

MAC Filter Commands

Use these commands to filter traffic going through the Switch based on the MAC addresses and VLAN group (ID).

Use the running configuration commands to look at the current MAC filter settings. See Chapter 51 on page 167.

MAC filtering implementation differs across Switch models.

- Some models allow you to specify a filter rule and discard all packets with the specified MAC address (source or destination) and VID.
- Other models allow you to choose whether you want to discard traffic originating from the specified MAC address and VID (src), sent to the specified MAC address (dst) or both.

See Section 33.2 on page 120 and Section 33.3 on page 120 for examples.

33.1 Command Summary

The following section lists the commands for this feature.

Table 79 mac-filter Command Summary

COMMAND	DESCRIPTION	M	P
`mac-filter name <name> mac <mac-addr> vlan <vlan-id>`	Configures a static MAC address port filtering rule. *name*: 1-32 alphanumeric characters	C	13
`no mac-filter mac <mac-addr> vlan <vlan-id>`	Deletes the specified MAC filter rule.	C	13
`mac-filter name <name> mac <mac-addr> vlan <vlan-id> inactive`	Disables a static MAC address port filtering rule. *name*: 1-32 alphanumeric characters	C	13
`no mac-filter mac <mac-addr> vlan <vlan-id> inactive`	Enables the specified MAC-filter rule.	C	13
`mac-filter name sourcefilter mac <mac-addr> vlan <vlan-id> drop <src|dst|both>`	Specifies the source and or destination filter parameters.	C	13

33.2 Command Example

This example creates a MAC filter called “filter1” that drops packets coming from or going to the MAC address 00:12:00:12:00:12 on VLAN 1.

```
sysname(config)# mac-filter name filter1 mac 00:12:00:12:00:12 vlan 1
```

33.3 Command Example: Filter Source

The next example is for Switches that support the filtering of frames based on the source or destination MAC address only. This example creates a filter “sourcefilter” that drops packets originating from the MAC address af:af:01:01:ff:02 on VLAN 2.

```
sysname(config)# mac-filter name sourcefilter mac af:af:01:01:ff:02 vlan 2
drop src
```

34

MAC Forward Commands

Use these commands to configure static MAC address forwarding.

Use the `mac` commands to look at the current `mac-forward` settings. See Chapter 31 on page 115.

34.1 Command Summary

The following table describes user-input values available in multiple commands for this feature.

Table 80 mac-forward User-input Values

COMMAND	DESCRIPTION
name	1-32 alphanumeric characters

The following section lists the commands for this feature.

Table 81 mac-forward Command Summary

COMMAND	DESCRIPTION	M	P
`mac-forward name <name> mac <mac-addr> vlan <vlan-id> interface <interface-id>`	Configures a static MAC address forwarding rule.	C	13
`no mac-forward mac <mac-addr> vlan <vlan-id> interface <interface-id>`	Removes the specified MAC forwarding entry, belonging to a VLAN group forwarded through an interface.	C	13
`mac-forward name <name> mac <mac-addr> vlan <vlan-id> interface <interface-id> inactive`	Disables a static MAC address forwarding rule.	C	13
`no mac-forward mac <mac-addr> vlan <vlan-id> interface <interface-id> inactive`	Enables the specified MAC address, belonging to a VLAN group forwarded through an interface.	C	13

35

Mirror Commands

Use these commands to copy a traffic flow for one or more ports to a monitor port so that you can examine the traffic on the monitor port without interference.

Use the running configuration commands to look at the current mirror settings. See Chapter 51 on page 167.

`mirror-filter` commands are not supported on all Switch models.

35.1 Command Summary

The following section lists the commands for this feature.

Table 82 mirror Command Summary

COMMAND	DESCRIPTION	M	P
`mirror-port`	Enables port mirroring on the Switch.	C	13
`mirror-port <port-num>`	Specifies the monitor port (the port to which traffic flow is copied) for port mirroring.	C	13
`no mirror-port`	Disables port mirroring on the Switch.	C	13
`interface port-channel <port-list>`	Enters config-interface mode for the specified port(s).	C	13
`mirror`	Enables port mirroring in the interface.	C	13
`mirror dir <ingress|egress|both>`	Enables port mirroring for incoming (`ingress`), outgoing (`egress`) or both incoming and outgoing (`both`) traffic.	C	13
`no mirror`	Disables port mirroring on the port(s).	C	13

Table 83 mirror-filter Command Summary

COMMAND	DESCRIPTION	M	P
`mirror-filter egress mac <mac-addr>`	Specifies the source or destination MAC address that the Switch uses to decide whether or not to copy outgoing traffic to mirrored ports to the monitor port.	C	13
`mirror-filter egress type <all|dest|src>`	`all`: Specifies that the Switch should copy all outgoing traffic from mirrored ports. `dest`: Specifies that the Switch should copy all outgoing traffic from mirrored ports to the specified destination MAC address. `src`: Specifies that the Switch should copy all outgoing traffic from mirrored ports from the specified source MAC address.	C	13
`mirror-filter ingress mac <mac-addr>`	Specifies the source or destination MAC address that the Switch uses to decide whether or not to copy incoming traffic from mirrored ports to the monitor port.	C	13
`mirror-filter ingress type <all|dest|src>`	`all`: Specifies that the Switch should copy all incoming traffic from mirrored ports. `dest`: Specifies that the Switch should copy all incoming traffic from mirrored ports to the specified destination MAC address. `src`: Specifies that the Switch should copy all incoming traffic from mirrored ports from the specified source MAC address.	C	13

35.2 Command Examples

This example enables port mirroring and copies outgoing traffic from ports 1, 4, 5, and 6 to port 3.

```
sysname(config)# mirror-port
sysname(config)# mirror-port 3
sysname(config)# interface port-channel 1,4-6
sysname(config-interface)# mirror
sysname(config-interface)# mirror dir egress
```

36

MRSTP Commands

Use these commands to configure MRSTP on the Switch.

36.1 MRSTP Overview

The Switch allows you to configure multiple instances of Rapid Spanning Tree Protocol (RSTP) as defined in the following standard.

- IEEE 802.1w Rapid Spanning Tree Protocol

See Chapter 53 on page 173 for information on RSTP commands and Chapter 37 on page 127 for information on MSTP commands.

36.2 Command Summary

The following section lists the commands for this feature.

Table 84 Command Summary: mrstp

COMMAND	DESCRIPTION	M	P
`show mrstp <tree-index>`	Displays multiple rapid spanning tree configuration for the specified tree. *tree-index*: this is a number identifying the RSTP tree configuration. Note: The number of RSTP tree configurations supported differs by model. Refer to your User's Guide for details.	E	3
`spanning-tree mode <RSTP|MRSTP|MSTP>`	Specifies the STP mode you want to implement on the Switch.	C	13
`mrstp <tree-index>`	Activates the specified RSTP configuration.	C	13
`mrstp <tree-index> priority <0-61440>`	Sets the bridge priority of the Switch for the specified RSTP configuration.		
`mrstp <tree-index> hello-time <1-10> maximum-age <6-40> forward-delay <4-30>`	Sets the Hello Time, Maximum Age and Forward Delay values on the Switch for the specified RSTP configuration.		
`mrstp interface <port-list>`	Activates RSTP on the specified ports.	C	13
`mrstp interface <port-list> path-cost <1-65535>`	Sets a path cost to the specified ports.	C	13

Table 84 Command Summary: mrstp

COMMAND	DESCRIPTION	M	P
`mrstp interface <port-list> priority <0-255>`	Sets the priority value to the specified ports for RSTP.	C	13
`mrstp interface <port-list> tree-index <tree-index>`	Assigns the specified port list to a specific RSTP configuration.	C	13
`no mrstp <tree-index>`	Disables the specified RSTP configuration.	C	13
`no mrstp interface <port-list>`	Disables the STP assignment from the specified port(s).	C	13

36.3 Command Examples

This example configures MRSTP in the following way:

- Enables MRSTP on the Switch.
- Activates tree **1** and sets the bridge priority, Hello Time, Maximum Age and Forward Values for this RSTP configuration.
- Activates MRSTP for ports **1-5** and sets path cost on these ports to **127**.
- Adds ports **1-5** to tree index **1**.

```
sysname(config)# spanning-tree mode mrstp
sysname(config)# mrstp 1
sysname(config)# mrstp 1 priority 16384
sysname(config)# mrstp 1 hello-time 2 maximum-age 15 forward-delay 30
sysname(config)# mrstp interface 1-5
sysname(config)# mrstp interface 1-5 path-cost 127
sysname(config)# mrstp interface 1-5 tree-index 1
```

37

MSTP Commands

Use these commands to configure Multiple Spanning Tree Protocol (MSTP) as defined in IEEE 802.1s.

37.1 Command Summary

The following section lists the commands for this feature.

Table 85 mstp Command Summary

COMMAND	DESCRIPTION	M	P
`show mstp`	Displays MSTP configuration for the Switch.	E	3
`spanning-tree mode <RSTP|MRSTP|MSTP>`	Specifies the STP mode you want to implement on the Switch.	C	13
`mstp`	Activates MSTP on the Switch.	C	13
`no mstp`	Disables MSTP on the Switch.	C	13
`mstp configuration-name <`*`name`*`>`	Sets a name for an MSTP region. *`name`*: 1-32 printable characters	C	13
`mstp revision <0-65535>`	Sets the revision number for this MST Region configuration.	C	13
`mstp hello-time <1-10> maximum-age <6-40> forward-delay <4-30>`	Sets Hello Time, Maximum Age and Forward Delay. `hello-time`: The time interval in seconds between BPDU (Bridge Protocol Data Units) configuration message generations by the root switch. `maximum-age`: The maximum time (in seconds) the Switch can wait without receiving a BPDU before attempting to reconfigure. `forward-delay`: The maximum time (in seconds) the Switch will wait before changing states.	C	13
`mstp max-hop <1-255>`	Sets the maximum hop value before BPDUs are discarded in the MST Region.	C	13

Table 86 mstp instance Command Summary

COMMAND	DESCRIPTION	M	P
`show mstp instance <0-16>`	Displays MSTP instance configuration.	E	3
`no mstp instance <0-16>`	Disables the specified MST instance on the Switch.	C	13
`mstp instance <0-16> priority <0-61440>`	Specifies the bridge priority of the instance. `priority`: Must be a multiple of 4096.	C	13
`mstp instance <0-16> vlan <`*`vlan-list`*`>`	Specifies the VLANs that belongs to the instance.	C	13

Table 86 mstp instance Command Summary (continued)

COMMAND	DESCRIPTION	M	P
no mstp instance <0-16> vlan <1-4094>	Disables the assignment of specific VLANs from an MST instance.	C	13
mstp instance <0-16> interface port-channel <*port-list*>	Specifies the ports you want to participate in this MST instance.	C	13
no mstp instance <0-16> interface port-channel <*port-list*>	Disables the assignment of specific ports from an MST instance.	C	13
mstp instance <0-16> interface port-channel <*port-list*> path-cost <1-65535>	Specifies the cost of transmitting a frame to a LAN through the port(s). It is recommended you assign it according to the speed of the bridge.	C	13
mstp instance <0-16> interface port-channel <*port-list*> priority <1-255>	Sets the priority for the specified ports. Priority decides which port should be disabled when more than one port forms a loop in a Switch. Ports with a higher priority numeric value are disabled first.	C	13

37.2 Command Examples

This example shows the current MSTP configuration.

```
sysname# show mstp
  (a)BridgeMaxAge:              20      (seconds)
  (b)BridgeHelloTime:           2       (seconds)
  (c)BridgeForwardDelay:        15      (seconds)
  (d)BridgeMaxHops:             128     (seconds)
  (e)TransmissionLimit:         3
  (f)ForceVersion:              3
  (g)MST Configuration ID
     Format Selector:           0
     Configuration Name:        001349aefb7a
     Reveision Number:          0
     Configuration Digest:      0xAC36177F50283CD4B83821D8AB26DE62
     msti       vlans mapped
     ----------------------------
      0         1-4094
     ----------------------------
```

The following table describes the labels in this screen.

Table 87 show mstp

LABEL	DESCRIPTION
BridgeMaxAge	This field displays the maximum time (in seconds) the Switch can wait without receiving a configuration message before attempting to reconfigure.
BridgeHelloTime	This field displays the time interval (in seconds) at which the Switch transmits a configuration message.
BridgeForwardDelay	This field displays the time (in seconds) the Switch will wait before changing states (that is, listening to learning to forwarding).
BridgeMaxHops	This field displays the number of hops (in seconds) in an MSTP region before the BPDU is discarded and the port information is aged.

Table 87 show mstp (continued)

LABEL	DESCRIPTION
TransmissionLimit	This field displays the maximum number of BPDUs that can be transmitted in the interval specified by **BridgeHelloTime**.
ForceVersion	This field indicates whether BPDUs are RSTP (a value less than 3) or MSTP (a value greater than or equal to 3).
MST Configuration ID	
Format Selector	This field displays zero, which indicates the use of the fields below.
Configuration Name	This field displays the configuration name for this MST region.
Revision Number	This field displays the revision number for this MST region.
Configuration Digest	A configuration digest is generated from the VLAN-MSTI mapping information. This field displays the 16-octet signature that is included in an MSTP BPDU. This field displays the digest when MSTP is activated on the system.
msti	This field displays the MSTI ID.
vlans mapped	This field displays which VLANs are mapped to an MSTI.

This example shows the current CIST configuration (MSTP instance 0).

```
sysname# show mstp instance 0
Bridge Info: MSTID: 0
  (a)BridgeID:                  8000-001349aefb7a
  (b)TimeSinceTopoChange:       756003
  (c)TopoChangeCount:           0
  (d)TopoChange:                0
  (e)DesignatedRoot:            8000-001349aefb7a
  (f)RootPathCost:              0
  (g)RootPort:                  0x0000
  (h)RootMaxAge:                20      (seconds)
  (i)RootHelloTime:             2       (seconds)
  (j)RootForwardDelay:          15      (seconds)
  (k)BridgeMaxAge:              20      (seconds)
  (l)BridgeHelloTime:           2       (seconds)
  (m)BridgeForwardDelay:        15      (seconds)
  (n)ForceVersion:              mstp
  (o)TransmissionLimit:         3

  (p)CIST_RRootID:              8000-001349aefb7a
  (q)CIST_RRootPathCost:        0
```

The following table describes the labels in this screen.

Table 88 show mstp instance

LABEL	DESCRIPTION
MSTID	This field displays the MSTI ID.
BridgeID	This field displays the unique identifier for this bridge, consisting of bridge priority plus MAC address.
TimeSinceTopoChange	This field displays the time since the spanning tree was last reconfigured.
TopoChangeCount	This field displays the number of times the spanning tree has been reconfigured.

Table 88 show mstp instance (continued)

LABEL	DESCRIPTION
TopoChange	This field indicates whether or not the current topology is stable. **0**: The current topology is stable. **1**: The current topology is changing.
DesignatedRoot	This field displays the unique identifier for the root bridge, consisting of bridge priority plus MAC address.
RootPathCost	This field displays the path cost from the root port on this Switch to the root switch.
RootPort	This field displays the priority and number of the port on the Switch through which this Switch must communicate with the root of the Spanning Tree.
RootMaxAge	This field displays the maximum time (in seconds) the root switch can wait without receiving a configuration message before attempting to reconfigure.
RootHelloTime	This field displays the time interval (in seconds) at which the root switch transmits a configuration message.
RootForwardDelay	This field displays the time (in seconds) the root switch will wait before changing states (that is, listening to learning to forwarding).
BridgeMaxAge	This field displays the maximum time (in seconds) the Switch can wait without receiving a configuration message before attempting to reconfigure.
BridgeHelloTime	This field displays the time interval (in seconds) at which the Switch transmits a configuration message.
BridgeForwardDelay	This field displays the time (in seconds) the Switch will wait before changing states (that is, listening to learning to forwarding).
ForceVersion	This field indicates whether BPDUs are RSTP (a value less than 3) or MSTP (a value greater than or equal to 3).
TransmissionLimit	This field displays the maximum number of BPDUs that can be transmitted in the interval specified by **BridgeHelloTime**.
CIST_RRootID	This field displays the unique identifier for the CIST regional root bridge, consisting of bridge priority plus MAC address.
CIST_RRootPathCost	This field displays the path cost from the root port on this Switch to the CIST regional root switch.

This example adds the Switch to the MST region **MSTRegionNorth**. **MSTRegionNorth** is on revision number 1. In **MSTRegionNorth**, VLAN 2 is in MST instance 1, and VLAN 3 is in MST instance 2.

```
sysname# configure
sysname(config)# mstp
sysname(config)# mstp configuration-name MSTRegionNorth
sysname(config)# mstp revision 1
sysname(config)# mstp instance 1 vlan 2
sysname(config)# mstp instance 2 vlan 3
sysname(config)# exit
```

38

Multiple Login Commands

Use these commands to configure multiple administrator logins on the Switch.

38.1 Command Summary

The following section lists the commands for this feature.

Table 89 multi-login Command Summary

COMMAND	DESCRIPTION	M	P
`show multi-login`	Displays multi-login information.	E	3
`multi-login`	Enables multi-login.	C	14
`no multi-login`	Disables another administrator from logging into Telnet or SSH.	C	14

38.2 Command Examples

This example shows the current administrator logins.

```
sysname# show multi-login
[session info ('*' denotes your session)]
index session    remote ip
----- ---------- ---------------
    1 telnet-d   172.16.5.15
 *  2 telnet-d   172.16.5.15
```

The following table describes the labels in this screen.

Table 90 show multi-login

LABEL	DESCRIPTION
index	This field displays a sequential number for this entry. If there is an asterisk (*) next to the index number, this entry is your session.
session	This field displays the service the administrator used to log in.
remote ip	This field displays the IP address of the administrator's computer.

39

MVR Commands

Use these commands to configure Multicast VLAN Registration (MVR).

39.1 Command Summary

The following section lists the commands for this feature.

Table 91 mvr Command Summary

COMMAND	DESCRIPTION	M	P
`show mvr`	Shows the MVR status.	E	3
`show mvr <vlan-id>`	Shows the detailed MVR status and MVR group configuration for a VLAN.	E	3
`mvr <vlan-id>`	Enters config-mvr mode for the specified MVR (multicast VLAN registration). Creates the MVR, if necessary.	C	13
`8021p-priority <0-7>`	Sets the IEEE 802.1p priority of outgoing MVR packets.	C	13
`inactive`	Disables these MVR settings.	C	13
`no inactive`	Enables these MVR settings.	C	13
`mode <dynamic|compatible>`	Sets the MVR mode (dynamic or compatible).	C	13
`name <name>`	Sets the MVR name for identification purposes. *name*: 1-32 English keyboard characters	C	13
`receiver-port <port-list>`	Sets the receiver port(s).An MVR receiver port can only receive multicast traffic in a multicast VLAN.	C	13
`no receiver-port <port-list>`	Disables the receiver port(s).An MVR receiver port can only receive multicast traffic in a multicast VLAN.	C	13
`source-port <port-list>`	Sets the source port(s).An MVR source port can send and receive multicast traffic in a multicast VLAN.	C	13
`no source-port <port-list>`	Disables the source port(s).An MVR source port can send and receive multicast traffic in a multicast VLAN.	C	13
`tagged <port-list>`	Sets the port(s) to tag VLAN tags.	C	13
`no tagged <port-list>`	Sets the port(s) to untag VLAN tags.	C	13
`group <name> start-address <ip> end-address <ip>`	Sets the multicast group range for the MVR. *name*: 1-32 English keyboard characters	C	13
`no group`	Disables all MVR group settings.	C	13
`no group <name-str>`	Disables the specified MVR group setting.	C	13
`no mvr <vlan-id>`	Removes an MVR configuration of the specified VLAN from the Switch.	C	13

39.2 Command Examples

This example configures MVR in the following ways:

1. Enters MVR mode. This creates a multicast VLAN with the name `multivlan` and the VLAN ID of 3.
2. Specifies source ports 2, 3, 5 for the multicast group.
3. Specifies receiver ports 6-8 for the multicast group.
4. Specifies dynamic mode for the multicast group.
5. Configures MVR multicast group addresses 224.0.0.1 through 224.0.0.255 by the name of `ipgroup`.
6. Exits MVR mode.

```
sysname(config)# mvr 3
sysname(config-mvr)# name multivlan
sysname(config-mvr)# source-port 2,3,5
sysname(config-mvr)# receiver-port 6-8
sysname(config-mvr)# mode dynamic
sysname(config-mvr)# group ipgroup start-address 224.0.0.1 end-address
--> 224.0.0.255
sysname(config-mvr)# exit
```

PART IV
Reference N-S

40

OSPF Commands

This chapter explains how to use commands to configure the Open Shortest Path First (OSPF) routing protocol on the Switch.

40.1 OSPF Overview

OSPF (Open Shortest Path First) is a link-state protocol designed to distribute routing information within an autonomous system (AS). An autonomous system is a collection of networks using a common routing protocol to exchange routing information.

40.2 Command Summary

The following section lists the commands for this feature.

Table 92 OSPF Command Summary

COMMAND	DESCRIPTION	M	P
`show ip ospf database`	Displays OSPF link state database information.	E	3
`show ip ospf interface`	Displays OSPF interface settings.	E	3
`show ip ospf neighbor`	Displays OSPF neighbor information.	E	3
`show router ospf`	Displays OSPF settings.	E	3
`show router ospf area`	Displays OSPF area settings.	E	3
`show router ospf network`	Displays OSPF network (or interface) settings.	E	3
`show router ospf redistribute`	Displays OSPF redistribution settings.	E	3
`show router ospf virtual-link`	Displays OSPF virtual link settings.	E	3
`interface route-domain <ip-address>/<mask-bits>`	Enters the configuration mode for this routing domain.	C	13
`ip ospf authentication-key <key>`	Specifies the authentication key for OSPF.	C	13
`no ip ospf authentication-key <key>`	Disables OSPF authentication in this routing domain.	C	13
`ip ospf authentication-same-aa`	Sets the same OSPF authentication settings in the routing domain as the associated area.	C	13
`no ip ospf authentication-same-aa`	Sets the routing domain not to use the same OSPF authentication settings as the area.	C	13

Table 92 OSPF Command Summary (continued)

COMMAND	DESCRIPTION	M	P
ip ospf cost <1-65535>	Sets the OSPF cost in this routing domain.	C	13
no ip ospf cost <1-65535>	Resets the OSPF cost in the routing domain to default.	C	13
ip ospf message-digest-key <*key*>	Sets the OSPF authentication key in this routing domain.	C	13
no ip ospf message-digest-key <*key*>	Disables the routing domain from using a security key in OSPF.	C	13
ip ospf priority <0-255>	Sets the OSPF priority for the interface. Setting this value to 0 means that this router will not participate in router elections.	C	13
no ip ospf priority <0-255>	Resets the OSPF priority for the interface.	C	13
router ospf <*router-id*>	Enables and enters the OSPF configuration mode.	C	13
area <*area-id*>	Enables and sets the area ID.	C	13
no area <*area-id*>	Removes the specified area.	C	13
area <*area-id*> authentication	Enables simple authentication for the area.	C	13
area <*area-id*> authentication message-digest	Enables MD5 authentication for the area.	C	13
no area <*area-id*> authentication	Sets the area to use no authentication (None).	C	13
area <*area-iD*> default-cost <0-16777214>	Sets the cost to the area.	C	13
no area <*area-id*> default-cost	Sets the area to use the default cost (15).	C	13
area <*area-id*> name <*name*>	Sets a descriptive name for the area for identification purposes.	C	13
area <*area-id*> stub	Enables and sets the area as a stub area.	C	13
no area <*area-id*> stub	Disables stub network settings in the area.	C	13
area <*area-id*> stub no-summary	Sets the stub area not to send any LSA (Link State Advertisement).	C	13
no area <*area-id*> stub no-summary	Sets the area to send LSAs (Link State Advertisements).	C	13
area <*area-id*> virtual-link <*router-id*>	Sets the virtual link ID information for the area.	C	13
no area <*area-id*> virtual-link <*router-id*>	Deletes the virtual link from the area.	C	13
area <*area-id*> virtual-link <*router-id*> authentication-key <*key*>	Enables simple authentication and sets the authentication key for the specified virtual link in the area.	C	13
no area <*area-id*> virtual-link <*router-id*> authentication-key	Resets the authentication settings on this virtual link.	C	13
area <*area-id*> virtual-link <*router*-ID> authentication-same-as-area	Sets the virtual link to use the same authentication method as the area.	C	13
no area <*area-id*> virtual-link <*router-id*> authentication-same-as-area	Resets the authentication settings on this virtual area.	C	13

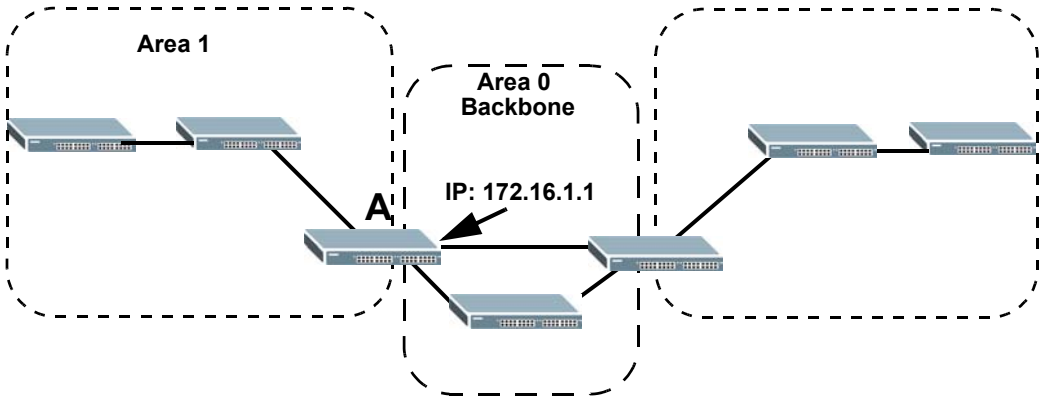
Table 92 OSPF Command Summary (continued)

COMMAND	DESCRIPTION	M	P
area <*area-id*> virtual-link <*router-id*> message-digest-key <*keyid*> md5 <*key*>	Enables MD5 authentication and sets the key ID and key for the virtual link in the area.	C	13
no area <*area-id*> virtual-link <*router-id*> message-digest-key	Resets the authentication settings on this virtual link.	C	13
area <*area-id*> virtual-link <*router-id*> name <*name*>	Sets a descriptive name for the virtual link for identification purposes.	C	13
exit	Leaves the router OSPF configuration mode.	C	13
network <*ip-addr/bits*> area <*area-id*>	Creates an OSPF area.	C	13
no network <*ip-addr/bits*>	Deletes the OSPF network.	C	13
redistribute rip metric-type <1|2> metric <0-65535>	Sets the Switch to learn RIP routing information which will use the specified metric information.	C	13
no redistribute rip	Sets the Switch not to learn RIP routing information.	C	13
redistribute static metric-type <1|2> metric <0-65535>	Sets the Switch to learn static routing information which will use the specified metric information.	C	13
no redistribute static	Sets the Switch not to learn static routing information.	C	13
passive-iface <*ip-addr/bits*>	Sets the interface to be passive. A passive interface does not send or receive OSPF traffic.	C	13
no router ospf	Disables OSPF on the Switch.	C	13

40.3 Command Examples

In this example, the Switch (**A**) is an Area Border Router (ABR) in an OSPF network.

Figure 5 OSPF Network Example



This example enables OSPF on the Switch, sets the router ID to **172.16.1.1**, configures an OSPF area ID as **0.0.0.0** (backbone) and enables simple authentication.

```
sysname(config)# router ospf 172.16.1.1
sysname(config-ospf)# area 0.0.0.0
sysname(config-ospf)# area 0.0.0.0 authentication
sysname(config-ospf)# area 0.0.0.0 name backbone
sysname(config-ospf)# network 172.16.1.1/24 area 0.0.0.0
sysname# show router ospf area
  index:1       active:Y        name:backbone
  area-id:0.0.0.0               auth:SIMPLE
  stub-active:N stub-no-sum:N   default-cost:15
```

This example configures an OSPF interface for the **172.16.1.1/24** network and specifies to use simple authentication with the key **1234abcd**. The priority for the Switch is also set to **1**, as this router should participate in router elections.

```
sysname(config)# interface route-domain 172.16.1.1/24
sysname(config-if)# ip ospf authentication-key abcd1234
sysname(config-if)# ip ospf priority 1
sysname# show ip ospf interface
swif2 is up, line protocol is up
  Internet Address 172.16.1.1/24, Area 0.0.0.0
  Router ID 172.16.1.1, Network Type BROADCAST, Cost: 15
  Transmit Delay is 1 sec, State Waiting, Priority 1
  No designated router on this network
  No backup designated router on this network
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:04
  Neighbor Count is 0, Adjacent neighbor count is 0
```

41

Password Commands

Use these commands to configure passwords for specific privilege levels on the Switch.

41.1 Command Summary

The following section lists the commands for this feature.

Table 93 password Command Summary

COMMAND	DESCRIPTION	M	P
`admin-password <pw-string> <confirm-string>`	Changes the administrator password. *pw-string*: 1-32 alphanumeric characters *confirm-string*: 1-32 alphanumeric characters	C	14
`password <password> [privilege <0-14>]`	Changes the password for the highest privilege level or, optionally, the specified privilege. *password*: 1-32 alphanumeric characters	C	14
`no password privilege <0-14>`	Clears the password for the specified privilege level and prevents users from entering the specified privilege level.	C	14

41.2 Command Examples

See Section 2.1.3.2 on page 16.

42

PoE Commands

Use these commands to configure Power over Ethernet (PoE). These are applicable for PoE models only.

42.1 Command Summary

The following section lists the commands for this feature.

Table 94 pwr Command Summary

COMMAND	DESCRIPTION	M	P
`show pwr`	Displays PoE (Power over Ethernet) settings on the Switch. Only available on models with the PoE feature.	E	3
`pwr interface <port-list>`	Enables PoE (Power over Ethernet) on the specified port(s).	C	13
`pwr interface <port-list> priority <critical|high|low>`	Sets the PD priority on a port to allow the Switch to allocate power to higher priority ports when the remaining power is less than the consumed power. `critical` > `high` >`low` Note: Available for non-full power models only.	C	13
`no pwr interface <port-list>`	Disables PoE (Power over Ethernet) on the specified port(s).	C	13
`pwr mibtrap`	Enables PoE MIB traps on the Switch. Traps are initiated when the usage reaches the limit set by the `pwr usagethreshold` command.	C	13
`no pwr mibtrap`	Disables PoE MIB traps on the Switch.	C	13
`pwr usagethreshold <1-99>`	Sets the percentage of power usage which initiates MIB traps.	C	13

42.2 Command Examples

This example enables Power over Ethernet (PoE) on ports 1-4 and enables traps when the power usage reaches 25%.

```
sysname# configure
sysname(config)# pwr interface 1-4
sysname(config)# pwr usagethreshold 25
sysname(config)# pwr mibtrap
sysname(config)# exit
```

This example shows the current status and configuration of Power over Ethernet.

```
sysname# show pwr

Averaged Junction Temperature: 35 (c), 95 (f).

Port    State   PD  Class  Priority  Consumption (mW)  MaxPower(mW)
----  -------  ---  -----  --------  ----------------  ------------
   1  Disable  off      0  Critical                 0             0
   2   Enable  off      0  Critical                 0             0
   3   Enable  off      0  Critical                 0             0
   4   Enable  off      0  Critical                 0             0
   5   Enable  off      0  Critical                 0             0
   6   Enable  off      0  Critical                 0             0
   7   Enable  off      0  Critical                 0             0
--------------------------------- SNIP ---------------------------------

Total Power:185.0(W)
Consuming Power:0.0(W)
Allocated Power:0.0(W)
Remaining Power:185.0(W)
```

The following table describes the labels in this screen.

Table 95 show pwr

LABEL	DESCRIPTION
Averaged Junction Temperature	This field displays the internal temperature of the PoE chipset.
Port	This field displays the port number.
State	This field indicates whether or not PoE is enabled on this port.
PD	This field indicates whether or not a powered device (PD) is allowed to receive power from the Switch on this port.
Class	This field displays the maximum power level at the input of the PoE-enabled devices connected to this port. The range of the maximum power used by the PD is described below. **0**: 0.44~12.95 W **1**: 0.44~3.84 W **2**: 3.84~6.49 W **3**: 6.49~12.95 W
Priority	When the total power requested by the PDs exceeds the total PoE power budget on the Switch, the Switch uses the PD priority to provide power to ports with higher priority.
Consumption (mW)	This field displays the amount of power the Switch is currently supplying to the PoE-enabled devices connected to this port.
MaxPower(mW)	This field displays the maximum amount of power the Switch can supply to the PoE-enabled devices connected to this port.
Total Power	This field displays the total power the Switch can provide to PoE-enabled devices.
Consuming Power	This field displays the amount of power the Switch is currently supplying to the PoE-enabled devices.

Table 95 show pwr (continued)

LABEL	DESCRIPTION
Allocated Power	This field displays the total amount of power the Switch has reserved for PoE after negotiating with the PoE device(s).
Remaining Power	This field displays the amount of power the Switch can still provide for PoE. Note: The Switch must have at least 16 W of remaining power in order to supply power to a PoE device, even if the PoE device requested less than 16 W.

43

Policy Commands

Use these commands to configure policies based on the classification of traffic flows. A classifier distinguishes traffic into flows based on the configured criteria. A policy rule defines the treatment of a traffic flow.

Configure classifiers before you configure policies. See Chapter 9 on page 45 for more information on classifiers.

43.1 Command Summary

The following section lists the commands for this feature.

Table 96 policy Command Summary

COMMAND	DESCRIPTION	M	P
`show policy`	Displays all policy related information.	E	3
`show policy <name>`	Displays the specified policy related information.	E	3

Table 96 policy Command Summary

COMMAND	DESCRIPTION	M	P
policy <*name*> classifier <*classifier-list*> <[vlan <*vlan-id*>][egress-port <*port-num*>][priority <0-7>][dscp <0-63>][tos <0-7>][bandwidth <*bandwidth*>][outgoing-packet-format <tagged|untagged>][out-of-profile-dscp <0-63>][forward-action <drop|forward>][queue-action <prio-set|prio-queue|prio-replace-tos>][diffserv-action <diff-set-tos|diff-replace-priority|diff-set-dscp>][outgoing-mirror][outgoing-eport][outgoing-non-unicast-eport][outgoing-set-vlan][metering][out-of-profile-action <[change-dscp][drop][forward] [set-drop-precedence]>][inactive]>	Configures a policy with the specified name. *name*: 32 alphanumeric characters	C	13
	Specifies which classifiers this policy applies to. *classifier-list*: names of classifiers separated by commas.		
	Specifies the parameters related to the actions: egress-port: an outbound port number priority: IEEE 802.1p priority field bandwidth: bandwidth limit in Kbps, actions can be assigned to packets which exceed the bandwidth limit (out-or-profile). out-of-profile-dscp: sets a DSCP number, if you want to replace or remark the DSCP number for out-of-profile traffic.		
	Specifies the actions for this policy: • queue-action: tells the Switch to: - set the IEEE 802.1p priority you specified in the priority parameter (prio-set) - send the packet to priority queue (prio-queue) - replace the IEEE 802.1p priority field with the tos parameter value (prio-replace-tos). • diffserv-action - choose whether you want to set the ToS field with the value you specified for the tos parameter (diff-set-tos), replace the IP ToS with IEEE 802.1p priority value (diff-replace-priority) or set the DSCP field with the dscp parameter value (diff-set-dscp) • outgoing-mirror - send the packet to the mirror port. • outgoing-eport - send the packet to the egress port. • outgoing-non-unicast-eport - send the broadcast, dlf or multicast packets (marked for dropping or to be sent to the CPU) to the egress port. • metering - enables bandwidth limitations on the traffic flows. • out-of-profile-action - specifies the actions to take for packets that exceed the bandwidth limitations: - replaces the DSCP field with the value in the out-of-profile-dscp parameter (change-dscp). - discard the out of profile packets (drop). - queues the packets that are marked for dropping (forward). - marks the out of profile traffic and drops it when network is congested (set-drop-precedence). inactive - disables the policy rule.		
no policy <*name*>	Deletes the policy.	C	13
no policy <*name*> inactive	Enables a policy.	C	13

43.2 Command Examples

This example creates a policy (**highPriority**) for the traffic flow identified via classifier **VLAN3** (see the classifier example in Chapter 9 on page 45). This policy replaces the IEEE 802.1 priority field with the IP ToS priority field (value **7**) for **VLAN3** packets.

```
sysname(config)# policy highPriority classifier VLAN3 tos 7 queue-action
prio-replace-tos
sysname(config)# exit
sysname# show policy highPriority
Policy highPriority:
  Classifiers:
    VLAN3;
  Parameters:
    VLAN = 1; Priority = 0; DSCP = 0; TOS = 7;
    Egress Port = 1; Outgoing packet format = tagged;
    Bandwidth = 0; Out-of-profile DSCP = 0;
  Action:
    Replace the 802.1 priority field with the IP TOS value;
```

44

Port Security Commands

Use these commands to allow only packets with dynamically learned MAC addresses and/or configured static MAC addresses to pass through a port on the Switch. For maximum port security, enable port security, disable MAC address learning and configure static MAC address(es) for a port.

It is not recommended you disable both port security and MAC address learning because this will result in many broadcasts.

44.1 Command Summary

The following section lists the commands for this feature.

Table 97 port-security Command Summary

COMMAND	DESCRIPTION	M	P
`show port-security`	Displays all port security settings.	E	3
`show port-security <port-list>`	Displays port security settings on the specified port(s).	E	3
`port-security`	Enables port security on the Switch.	C	13
`no port-security`	Disables port security on the device.	C	13
`port-security <port-list>`	Enables port security on the specified port(s).	C	13
`no port-security <port-list>`	Disables port security on the specified port(s).	C	13
`port-security <port-list> learn inactive`	Disables MAC address learning on the specified port(s).	C	13
`no port-security <port-list> learn inactive`	Enables MAC address learning on the specified ports.	C	13
`port-security <port-list> address-limit <number>`	Limits the number of (dynamic) MAC addresses that may be learned on the specified port(s).	C	13
`port-security <port-list> MAC-freeze`	Stops MAC address learning and enables port security on the port(s). Note: All previously-learned dynamic MAC addresses are saved to the static MAC address table.	C	13

44.2 Command Examples

This example enables port security on port 1 and limits the number of learned MAC addresses to 5.

```
sysname# configure
sysname(config)# port-security
sysname(config)# port-security 1
sysname(config)# no port-security 1 learn inactive
sysname(config)# port-security 1 address-limit 5
sysname(config)# exit
sysname# show port-security 1
  Port Security Active : YES
  Port   Active   Address Learning   Limited Number of Learned MAC Address
   01       Y             Y                              5
```

45

Port-based VLAN Commands

Use these commands to configure port-based VLAN.

These commands have no effect unless port-based VLAN is enabled.

45.1 Command Summary

The following section lists the commands for this feature.

Table 98 egress Command Summary

COMMAND	DESCRIPTION	M	P
`show interfaces config <port-list> egress`	Displays outgoing port information.	E	3
`vlan-type <802.1q|port-based>`	Specifies the VLAN type.	C	13
`interface port-channel <port-list>`	Enters config-interface mode for the specified port(s).	C	13
`egress set <port-list>`	Sets the outgoing traffic port list for a port-based VLAN.	C	13
`no egress set <port-list>`	Removes the specified ports from the outgoing traffic port list.	C	13

45.2 Command Examples

This example looks at the ports to which incoming traffic from ports 1 and 2 can be forwarded.

```
sysname# show interfaces config 1-2 egress
  Port 1: Enabled egress ports cpu, eg1
  Port 2: Enabled egress ports cpu, eg1-eg4
```

46

Protocol-based VLAN Commands

Use these commands to configure protocol based VLANs on the Switch.

46.1 Protocol-based VLAN Overview

Protocol-based VLANs allow you to group traffic based on the Ethernet protocol you specify. This allows you to assign priority to traffic of the same protocol.

See also Chapter 56 on page 183 for subnet-based VLAN commands and Chapter 62 on page 199 for VLAN commands.

46.2 Command Summary

The following section lists the commands for this feature.

Table 99 protocol-based-vlan Command Summary

COMMAND	DESCRIPTION	M	P
`show interfaces config <port-list> protocol-based-vlan`	Displays the protocol based VLAN settings for the specified port(s).	E	3
`interface port-channel <port-list>`	Enters subcommand mode for configuring the specified ports.	C	13

Table 99 protocol-based-vlan Command Summary (continued)

COMMAND	DESCRIPTION	M	P
protocol-based-vlan name <*name*> ethernet-type <*ether-num*|ip|ipx|arp|rarp|appletalk|decnet> vlan <*vlan-id*> priority <0-7>	Creates a protocol based VLAN with the specified parameters. *name* - Use up to 32 alphanumeric characters. *ether-num* - if you don't select a predefined Ethernet protocol (ip, ipx, arp, rarp, appletalk or decnet), type the protocol number in hexadecimal notation. For example, the IP protocol in hexadecimal notation is 0800 and Novell IPX is 8137. Note: Protocols in the hexadecimal number range 0x0000 to 0x05ff are not allowed. priority - specify the IEEE 802.1p priority that the Switch assigns to frames belonging to this VLAN.	C	13
no protocol-based-vlan ethernet-type <*ether-num*|ip|ipx|arp|rarp|appletalk|decnet>	Disables protocol based VLAN of the specified protocol on the port.	C	13

46.3 Command Examples

This example creates an IP based VLAN called IP_VLAN on ports 1-4 with a VLAN ID of 200 and a priority 6.

```
sysname(config)# interface port-channel 1-4
sysname(config-interface)# protocol-based-vlan name IP_VLAN ethernet-type ip
--> vlan 200 priority 6
sysname(config-interface)# exit
sysname(config)# exit
sysname# show interfaces config 1-4 protocol-based-vlan
   Name  Port  Packet type  Ethernet type  Vlan  Priority  Active
-------  ----  -----------  -------------  ----  --------  ------
IP_VLAN     1      EtherII             ip   200         6     Yes
IP_VLAN     2      EtherII             ip   200         6     Yes
IP_VLAN     3      EtherII             ip   200         6     Yes
IP_VLAN     4      EtherII             ip   200         6     Yes
sysname#
```

47

Queuing Commands

Use queuing commands to help solve performance degradation when there is network congestion.

Queuing method configuration differs across Switch models.

- Some models allow you to select a queuing method on a port-by-port basis. For example, port 1 can use Strictly Priority Queuing and ports 2-8 can use Weighted Round Robin.
- Other models allow you to specify one queuing method for all the ports at once.

47.1 Queuing Overview

The following queuing algorithms are supported by ZyXEL Switchyes:

Check your User's Guide for queuing algorithms supported by your model.

- **Strictly Priority Queuing** (**SPQ**) - services queues based on priority only. As traffic comes into the Switch, traffic on the highest priority queue, Q7 is transmitted first. When that queue empties, traffic on the next highest-priority queue, Q6 is transmitted until Q6 empties, and then traffic is transmitted on Q5 and so on. If higher priority queues never empty, then traffic on lower priority queues never gets sent.

Switch models which have only 4 queues, support a limited version of SPQ. The highest level queue is serviced using SPQ and the remaining queues use WRR queuing.

- **Weighted Fair Queuing** (**WFQ**)- guarantees each queue's minimum bandwidth based on its bandwidth weight (portion) when there is traffic congestion. WFQ is activated only when a port has more traffic than it can handle. Queues with larger weights get more guaranteed bandwidth than queues with smaller weights. This queuing mechanism is highly efficient in that it divides any available bandwidth across the different traffic queues. By default, the weight for Q0 is 1, for Q1 is 2, for Q2 is 3, and so on. Guaranteed bandwidth is calculated as follows:

$$\frac{\text{Queue Weight}}{\text{Total Queue Weight}} \times \text{Port Speed}$$

  For example, using the default setting, Q0 on Port 1 gets a guaranteed bandwidth of:

$$\frac{1}{1+2+3+4+5+6+7+8} \times 100\ \text{Mbps} = 3\ \text{Mbps}$$

- **Weighted Round Robin Scheduling** (**WRR**) - services queues on a rotating basis and is activated only when a port has more traffic than it can handle. A queue is a given an amount of bandwidth based on the queue weight value. Queues with larger weights get more service than queues with smaller weights. This queuing mechanism is highly efficient in that it divides any available bandwidth across the different traffic queues and returns to queues that have not yet emptied.
- **Hybrid Mode: WRR & SPQ or WFQ & SPQ** - some switch models allow you to configure higher priority queues to use SPQ and use WRR or WFQ for the lower level queues.

47.2 Command Summary: Port by Port Configuration

The following section lists the commands for this feature.

Table 100 Queuing Command Summary

COMMAND	DESCRIPTION	M	P
`queue priority <0-7> level <0-7>`	Sets the IEEE 802.1p priority level-to-physical queue mapping. `priority <0-7>`: IEEE 802.1p defines up to eight separate traffic types by inserting a tag into a MAC-layer frame that contains bits to define class of service. Frames without an explicit priority tag are given the default priority of the ingress port. `level <0-7>`: The Switch has up to 8 physical queues that you can map to the 8 priority levels. On the Switch, traffic assigned to higher index queues gets through faster while traffic in lower index queues is dropped if the network is congested. Note: Some models only support 4 queues.	C	13
`interface port-channel <port-list>`	Enters subcommand mode for configuring the specified ports.	C	13
`spq`	Sets the switch to use Strictly Priority Queuing (SPQ) on the specified ports.	C	13

Table 100 Queuing Command Summary (continued)

COMMAND	DESCRIPTION	M	P
`ge-spq <q0|q1| ... |q7>`	Enables SPQ starting with the specified queue and subsequent higher queues on the Gigabit ports.	C	13
`hybrid-spq lowest-queue <q0|q1| ... |q7>`	Enables SPQ starting with the specified queue and subsequent higher queues on the ports.	C	13
`wrr`	Sets the switch to use Weighted Round Robin (WRR) on the specified ports.	C	13
`wfq`	Sets the switch to use Weighted Fair Queuing (WFQ) on the specified ports.	C	13
`weight <wt1> <wt2> ... <wt8>`	Assigns a weight value to each physical queue on the Switch. When the Switch is using WRR or WFQ, bandwidth is divided across different traffic queues according to their weights. Queues with larger weights get more service than queues with smaller weights. Weight values range: 1-15.	C	13

47.3 Command Examples: Port by Port Configuration

This example configures WFQ on ports 1-5 and assigns weight values (1,2,3,4,12,13,14,15) to the physical queues (Q0 to Q8).

```
sysname(config)# interface port-channel 1-5
sysname(config-interface)# wfq
sysname(config-interface)# weight 1 2 3 4 12 13 14 15
```

47.4 Command Summary: System-Wide Configuration

The following section lists the commands for this feature.

Table 101 Queueing Command Summary

COMMAND	DESCRIPTION	M	P
`queue priority <0-7> level <0-7>`	Sets the IEEE 802.1p priority level-to-physical queue mapping. `priority <0-7>`: IEEE 802.1p defines up to eight separate traffic types by inserting a tag into a MAC-layer frame that contains bits to define class of service. Frames without an explicit priority tag are given the default priority of the ingress port. `level <0-7>`: The Switch has up to 7 physical queues that you can map to the 8 priority levels. On the Switch, traffic assigned to higher index queues gets through faster while traffic in lower index queues is dropped if the network is congested. Note: Some models only support 4 queues.	C	13
`spq`	Sets the Switch to use Strictly Priority Queuing (SPQ).	C	13
`wrr`	Sets the Switch to use Weighted Round Robin (WRR).	C	13

Table 101 Queueing Command Summary (continued)

COMMAND	DESCRIPTION	M	P
`wfq`	Sets the Switch to use Weighted Fair Queuing (WFQ).	C	13
`fe-spq <q0|q1| ... |q7>`	Enables SPQ starting with the specified queue and subsequent higher queues on the 10/100 Mbps ports.	C	13

47.5 Command Examples: System-Wide

This example configures WFQ on the Switch and assigns weight values (1,2,3,4,12,13,14,15) to the physical queues (Q0 to Q8).

```
sysname(config)# wfq
sysname(config)# interface port-channel 1-5
sysname(config-interface)# weight 1 2 3 4 12 13 14 15
```

This example configures the Switch to use WRR as a queueing method but configures the Gigabit ports 9-12 to use SPQ for queues 5, 6 and 7.

```
sysname(config)# wrr
sysname(config)# interface port-channel 9-12
sysname(config-interface)# ge-spq 5
```

48

RADIUS Commands

Use these commands to configure external RADIUS (Remote Authentication Dial-In User Service) servers.

48.1 Command Summary

The following section lists the commands for this feature.

Table 102 radius-server Command Summary

COMMAND	DESCRIPTION	M	P
`show radius-server`	Displays RADIUS server settings.	E	3
`radius-server mode <index-priority|round-robin>`	Specifies how the Switch decides which RADIUS server to select if you configure multiple servers. `index-priority`: The Switch tries to authenticate with the first configured RADIUS server. If the RADIUS server does not respond, then the Switch tries to authenticate with the second RADIUS server. `round-robin`: The Switch alternates between RADIUS servers that it sends authentication requests to.	C	13
`radius-server timeout <1-1000>`	Specify the amount of time (in seconds) that the Switch waits for an authentication request response from the RADIUS server. In `index-priority` mode, the timeout is divided by the number of servers you configure. For example, if you configure two servers and the timeout is 30 seconds, then the Switch waits 15 seconds for a response from each server.	C	13
`radius-server host <index> <ip> [auth-port <socket-number>] [key <key-string>]`	Specifies the IP address of the RADIUS authentication server. Optionally, sets the UDP port number and shared secret. *index*: 1 or 2. *key-string*: 1-32 alphanumeric characters.	C	13
`no radius-server <index>`	Resets the specified RADIUS server to its default values.	C	13

Table 103 radius-accounting Command Summary

COMMAND	DESCRIPTION	M	P
`show radius-accounting`	Displays RADIUS accounting server settings.	E	3
`radius-accounting timeout <1-1000>`	Specifies the RADIUS accounting server timeout value.	C	13

Table 103 radius-accounting Command Summary (continued)

COMMAND	DESCRIPTION	M	P
`radius-accounting host <index> <ip> [acct-port <socket-number>] [key <key-string>]`	Specifies the IP address of the RADIUS accounting server. Optionally, sets the port number and key of the external RADIUS accounting server. *index*: 1 or 2. *key-string*: 1-32 alphanumeric characters.	C	13
`no radius-accounting <index>`	Resets the specified RADIUS accounting server to its default values.	C	13

48.2 Command Examples

This example sets up one primary RADIUS server (172.16.10.10) and one secondary RADIUS server (172.16.10.11). The secondary RADIUS server is also the accounting server.

```
sysname# configure
sysname(config)# radius-server mode index-priority
sysname(config)# radius-server host 1 172.16.10.10
sysname(config)# radius-server host 2 172.16.10.11
sysname(config)# radius-accounting host 1 172.16.10.11
sysname(config)# exit
```

49

Remote Management Commands

Use these commands to specify a group of one or more “trusted computers” from which an administrator may use one or more services to manage the Switch and to decide what services you may use to access the Switch.

49.1 Command Summary

The following table describes user-input values available in multiple commands for this feature.

Table 104 remote-management User-input Values

COMMAND	DESCRIPTION
index	1-4

The following section lists the commands for this feature.

Table 105 remote-management Command Summary

COMMAND	DESCRIPTION	M	P
`show remote-management [index]`	Displays all secured client information or, optionally, a specific group of secured clients.	E	3
`remote-management <index>`	Enables the specified group of trusted computers.	C	13
`no remote-management <index>`	Disables the specified group of trusted computers.	C	13
`remote-management <index> start-addr <ip> end-addr <ip> service <[telnet] [ftp] [http] [icmp] [snmp] [ssh] [https]>`	Specifies a group of trusted computer(s) from which an administrator may use the specified service(s) to manage the Switch. Group `0.0.0.0 - 0.0.0.0` refers to every computer.	C	13
`no remote-management <index> service <[telnet] [ftp] [http] [icmp] [snmp] [ssh] [https]>`	Disables the specified service(s) for the specified group of trusted computes.	C	13

Table 106 service-control Command Summary

COMMAND	DESCRIPTION	M	P
`show service-control`	Displays service control settings.	E	3
`service-control ftp <socket-number>`	Allows FTP access on the specified service port.	C	13
`no service-control ftp`	Disables FTP access to the Switch.	C	13

Table 106 service-control Command Summary (continued)

COMMAND	DESCRIPTION	M	P
`service-control http <socket-number> <timeout>`	Allows HTTP access on the specified service port and defines the timeout period (in minutes). *timeout*: 1-255	C	13
`no service-control http`	Disables HTTPS access to the Switch.	C	13
`service-control https <socket-number>`	Allows HTTPS access on the specified service port.	C	13
`no service-control https`	Disables HTTPS access to the Switch.	C	13
`service-control icmp`	Allows ICMP management packets.	C	13
`no service-control icmp`	Disables ICMP access to the Switch.	C	13
`service-control snmp`	Allows SNMP management.	C	13
`no service-control snmp`	Disables SNMP access to the Switch.	C	13
`service-control ssh <socket-number>`	Allows SSH access on the specified service port.	C	13
`no service-control ssh`	Disables SSH access to the Switch.	C	13
`service-control telnet <socket-number>`	Allows Telnet access on the specified service port.	C	13
`no service-control telnet`	Disables Telnet access to the Switch.	C	13

49.2 Command Examples

This example allows computers in subnet 172.16.37.0/24 to access the Switch through any service except SNMP, allows the computer at 192.168.10.1 to access the Switch only through SNMP, and prevents other computers from accessing the Switch at all.

```
sysname# configure
sysname(config)# remote-management 1 start-addr 172.16.37.0 end-addr
--> 172.16.37.255 service telnet ftp http icmp ssh https
sysname(config)# remote-management 2 start-addr 192.168.10.1 end-addr
--> 192.168.10.1 service snmp
sysname(config)# exit
```

This example disables all SNMP and ICMP access to the Switch.

```
sysname# configure
sysname(config)# no service-control snmp
sysname(config)# no service-control icmp
sysname(config)# exit
```

50

RIP Commands

This chapter explains how to use commands to configure the Routing Information Protocol (RIP) on the Switch.

50.1 RIP Overview

RIP is a protocol used for exchanging routing information between routers on a network. Information is exchanged by routers periodically advertising a routing table. The Switch can be configured to receive and incorporate routing table information sent from other routers, to only send routing information to other routers, both send and receive routing information, or to neither send nor receive routing information to or from other routers on the network.

50.2 Command Summary

The following section lists the commands for this feature.

Table 107 rip Command Summary

COMMAND	DESCRIPTION	M	P
`show router rip`	Displays global RIP settings.	E	3
`router rip`	Enables and enters the RIP configuration mode on the Switch.	C	13
`exit`	Leaves the RIP configuration mode.	C	13
`no router rip`	Disables RIP on the Switch.	C	13
`interface route-domain <`*`ip-address`*`>/<`*`mask-bits`*`>`	Enters the configuration mode for this routing domain.	C	13
`ip rip direction <Outgoing|Incoming|Both|None> version <v1|v2b|v2m>`	Sets the RIP direction and version in this routing domain.	C	13

50.3 Command Examples

This example:

- Enables RIP.
- Enters the IP routing domain **172.16.1.1** with subnet mask **255.255.255.0**.

- Sets the RIP direction in this routing domain to **Both** and the version to 2 with subnet broadcasting (**v2b**); the Switch will send and receive RIP packets in this routing domain.

```
sysname(config)# router rip
sysname(config-rip)# exit
sysname(config)# interface route-domain 172.16.1.1/24
sysname(config-if)# ip rip direction Both version v2b
```

51

Running Configuration Commands

Use these commands to back up and restore configuration and firmware.

51.1 Switch Configuration File

When you configure the Switch using either the CLI (Command Line Interface) or web configurator, the settings are saved as a series of commands in a configuration file on the Switch called `running-config`. You can perform the following with a configuration file:

- Back up Switch configuration once the Switch is set up to work in your network.
- Restore a previously-saved Switch configuration.
- Use the same configuration file to set all switches (of the same model) in your network to the same settings.

You may also edit a configuration file using a text editor. Make sure you use valid commands.

The Switch rejects configuration files with invalid or incomplete commands.

51.2 Command Summary

The following table describes user-input values available in multiple commands for this feature.

Table 108 running-config User-input Values

COMMAND	DESCRIPTION
attribute	Possible values: `active, name, speed-duplex, bpdu-control, flow-control, intrusion-lock, vlan1q, vlan1q-member, bandwidth-limit, vlan-stacking, port-security, broadcast-storm-control, mirroring, port-access-authenticator, queuing-method, igmp-filtering, spanning-tree, mrstp, protocol-based-vlan, port-based-vlan, mac-authentication, trtcm, ethernet-oam, loopguard, arp-inspection, dhcp-snooping.`

The following section lists the commands for this feature.

Table 109 running-config Command Summary

COMMAND	DESCRIPTION	M	P
`show running-config [interface port-channel <port-list> [<attribute> [<...>]]]`	Displays the current configuration file. This file contains the commands that change the Switch's configuration from the default settings to the current configuration. Optionally, displays current configuration on a port-by-port basis.	E	3
`show running-config help`	Provides more information about the specified command.	E	3
`copy running-config interface port-channel <port> <port-list> [<attribute> [<...>]]`	Clones (copies) the attributes from the specified port to other ports. Optionally, copies the specified attributes from one port to other ports.	E	13
`copy running-config help`	Provides more information about the specified command.	E	13
`erase running-config`	Resets the Switch to the factory default settings.	E	13
`erase running-config interface port-channel <port-list> [<attribute> [<...>]]`	Resets to the factory default settings on a per-port basis and optionally on a per-feature configuration basis.	E	13
`erase running-config help`	Provides more information about the specified command.	E	13

51.3 Command Examples

This example resets the Switch to the factory default settings.

```
sysname# erase running-config
sysname# write memory
```

This example copies all attributes of port 1 to port 2 and copies selected attributes (active, bandwidth limit and STP settings) from port 1 to ports 5-8

```
sysname# copy running-config interface port-channel 1 2
sysname# copy running-config interface port-channel 1 5-8 active
bandwidth-limit spanning-tree
```

52

SNMP Server Commands

Use these commands to configure SNMP on the Switch.

52.1 Command Summary

The following table describes user-input values available in multiple commands for this feature.

Table 110 snmp-server User-input Values

COMMAND	DESCRIPTION
property	1-32 alphanumeric characters
options	aaa: `authentication`, `accounting`. interface: `linkup`, `linkdown`, `autonegotiation`. ip: `ping`, `traceroute`. switch: `stp`, `mactable`, `rmon`. system: `coldstart`, `warmstart`, `fanspeed`, `temperature`, `voltage`, `reset`, `timesync`, `intrusionlock`, `loopguard`.

The following section lists the commands for this feature.

Table 111 snmp-server Command Summary

COMMAND	DESCRIPTION	M	P
`show snmp-server`	Displays SNMP settings.	E	3
`snmp-server <[contact <system-contact>] [location <system-location>]>`	Sets the geographic location and the name of the person in charge of this Switch. *system-contact*: 1-32 English keyboard characters; spaces are allowed. *system-location*: 1-32 English keyboard characters; spaces are allowed.	C	13
`snmp-server version <v2c|v3|v3v2c>`	Sets the SNMP version to use for communication with the SNMP manager.	C	13
`snmp-server get-community <property>`	Sets the get community. Only for SNMPv2c or lower.	C	13
`snmp-server set-community <property>`	Sets the set community. Only for SNMPv2c or lower.	C	13
`snmp-server trap-community <property>`	Sets the trap community. Only for SNMPv2c or lower.	C	13
`snmp-server trap-destination <ip> [udp-port <socket-number>] [version <v1|v2c|v3>] [username <name>]`	Sets the IP addresses of up to four SNMP managers (stations to send your SNMP traps to). You can configure up to four managers.	C	13

Table 111 snmp-server Command Summary (continued)

COMMAND	DESCRIPTION	M	P
`no snmp-server trap-destination <ip>`	Deletes the specified SNMP manager.	C	13
`snmp-server username <name> sec-level <noauth|auth|priv> [auth <md5|sha>] [priv <des|aes>]`	Sets the authentication level for SNMP v3 user authentication. Optionally, specifies the authentication and encryption methods for communication with the SNMP manager. *name*: Must match an existing account on the Switch. noauth: Use the username as the password string sent to the SNMP manager. This is equivalent to the Get, Set and Trap Community in SNMP v2c. This is the lowest security level. auth: Implement an authentication algorithm for SNMP messages sent by this user. priv: Implement authentication and encryption for SNMP messages sent by this user. This is the highest security level. Note: The settings on the SNMP manager must be set at the same security level or higher than the security level settings on the Switch.	C	13

Table 112 snmp-server trap-destination enable traps Command Summary

COMMAND	DESCRIPTION	M	P
`snmp-server trap-destination <ip> enable traps`	Enables sending SNMP traps to a manager.	C	13
`no snmp-server trap-destination <ip> enable traps`	Disables sending of SNMP traps to a manager.	C	13
`snmp-server trap-destination <ip> enable traps aaa`	Sends all AAA traps to the specified manager.	C	13
`no snmp-server trap-destination <ip> enable traps aaa`	Prevents the Switch from sending any AAA traps to the specified manager.	C	13
`snmp-server trap-destination <ip> enable traps aaa <options>`	Sends the specified AAA traps to the specified manager.	C	13
`no snmp-server trap-destination <ip> enable traps aaa <options>`	Prevents the Switch from sending the specified AAA traps to the specified manager.	C	13
`snmp-server trap-destination <ip> enable traps interface`	Sends all interface traps to the specified manager.	C	13
`no snmp-server trap-destination <ip> enable traps interface`	Prevents the Switch from sending any interface traps to the specified manager.	C	13
`snmp-server trap-destination <ip> enable traps interface <options>`	Sends the specified interface traps to the specified manager.	C	13
`no snmp-server trap-destination <ip> enable traps interface <options>`	Prevents the Switch from sending the specified interface traps to the specified manager.	C	13
`snmp-server trap-destination <ip> enable traps ip`	Sends all IP traps to the specified manager.	C	13
`no snmp-server trap-destination <ip> enable traps ip`	Prevents the Switch from sending any IP traps to the specified manager.	C	13

Table 112 snmp-server trap-destination enable traps Command Summary (continued)

COMMAND	DESCRIPTION	M	P
`snmp-server trap-destination <ip> enable traps ip <options>`	Sends the specified IP traps to the specified manager.	C	13
`no snmp-server trap-destination <ip> enable traps ip <options>`	Prevents the Switch from sending the specified IP traps to the specified manager.	C	13
`snmp-server trap-destination <ip> enable traps switch`	Sends all switch traps to the specified manager.	C	13
`no snmp-server trap-destination <ip> enable traps switch`	Prevents the Switch from sending any switch traps to the specified manager.	C	13
`snmp-server trap-destination <ip> enable traps switch <options>`	Sends the specified switch traps to the specified manager.	C	13
`no snmp-server trap-destination <ip> enable traps switch <options>`	Prevents the Switch from sending the specified switch traps to the specified manager.	C	13
`snmp-server trap-destination <ip> enable traps system`	Sends all system traps to the specified manager.	C	13
`no snmp-server trap-destination <ip> enable traps system`	Prevents the Switch from sending any system traps to the specified manager.	C	13
`snmp-server trap-destination <ip> enable traps system <options>`	Sends the specified system traps to the specified manager.	C	13
`no snmp-server trap-destination <ip> enable traps system <options>`	Prevents the Switch from sending the specified system traps to the specified manager.	C	13

53

STP and RSTP Commands

Use these commands to configure Spanning Tree Protocol (STP) and Rapid Spanning Tree Protocol (RSTP) as defined in the following standards.

- IEEE 802.1D Spanning Tree Protocol
- IEEE 802.1w Rapid Spanning Tree Protocol

See Chapter 36 on page 125 and Chapter 37 on page 127 for more information on MRSTP and MSTP commands respectively. See also Chapter 30 on page 113 for information on loopguard commands.

53.1 Command Summary

The following section lists the commands for this feature.

Table 113 spanning-tree Command Summary

COMMAND	DESCRIPTION	M	P
`show spanning-tree config`	Displays Spanning Tree Protocol (STP) settings.	E	3
`spanning-tree mode <RSTP|MRSTP|MSTP>`	Specifies the STP mode you want to implement on the Switch.	C	13
`spanning-tree`	Enables STP on the Switch.	C	13
`no spanning-tree`	Disables STP on the Switch.	C	13
`spanning-tree hello-time <1-10> maximum-age <6-40> forward-delay <4-30>`	Sets Hello Time, Maximum Age and Forward Delay. `hello-time`: The time interval in seconds between BPDU (Bridge Protocol Data Units) configuration message generations by the root switch. `maximum-age`: The maximum time (in seconds) the Switch can wait without receiving a BPDU before attempting to reconfigure. `forward-delay`: The maximum time (in seconds) the Switch will wait before changing states.	C	13
`spanning-tree priority <0-61440>`	Sets the bridge priority of the Switch. The lower the numeric value you assign, the higher the priority for this bridge. `priority`: Must be a multiple of 4096.	C	13
`spanning-tree <port-list>`	Enables STP on a specified ports.	C	13
`no spanning-tree <port-list>`	Disables STP on listed ports.	C	13
`spanning-tree <port-list> path-cost <1-65535>`	Specifies the cost of transmitting a frame to a LAN through the port(s). It is assigned according to the speed of the bridge.	C	13

Table 113 spanning-tree Command Summary (continued)

COMMAND	DESCRIPTION	M	P
`spanning-tree <port-list> priority <0-255>`	Sets the priority for the specified ports. Priority decides which port should be disabled when more than one port forms a loop in a Switch. Ports with a higher priority numeric value are disabled first.	C	13
`spanning-tree help`	Provides more information about the specified command.	C	13

53.2 Command Examples

This example configures STP in the following ways:

1. Enables STP on the Switch.
2. Sets the bridge priority of the Switch to 0.
3. Sets the Hello Time to 4, Maximum Age to 20 and Forward Delay to 15.
4. Enables STP on port 5 with a path cost of 150.
5. Sets the priority for port 5 to 20.

```
sysname(config)# spanning-tree
sysname(config)# spanning-tree priority 0
sysname(config)# spanning-tree hello-time 4 maximum-age 20 forward-delay
--> 15
sysname(config)# spanning-tree 5 path-cost 150
sysname(config)# spanning-tree 5 priority 20
```

This example shows the current STP settings.

```
sysname# show spanning-tree config
Bridge Info:
  (a)BridgeID:                  8000-001349aefb7a
  (b)TimeSinceTopoChange:       9
  (c)TopoChangeCount:           0
  (d)TopoChange:                0
  (e)DesignatedRoot:            8000-001349aefb7a
  (f)RootPathCost:              0
  (g)RootPort:                  0x0000
  (h)MaxAge:                    20      (seconds)
  (i)HelloTime:                 2       (seconds)
  (j)ForwardDelay:              15      (seconds)
  (k)BridgeMaxAge:              20      (seconds)
  (l)BridgeHelloTime:           2       (seconds)
  (m)BridgeForwardDelay:        15      (seconds)
  (n)TransmissionLimit:         3
  (o)ForceVersion:              2
```

The following table describes the labels in this screen.

Table 114 show spanning-tree config

LABEL	DESCRIPTION
BridgeID	This field displays the unique identifier for this bridge, consisting of bridge priority plus MAC address.
TimeSinceTopoChange	This field displays the time since the spanning tree was last reconfigured.
TopoChangeCount	This field displays the number of times the spanning tree has been reconfigured.
TopoChange	This field indicates whether or not the current topology is stable. **0**: The current topology is stable. **1**: The current topology is changing.
DesignatedRoot	This field displays the unique identifier for the root bridge, consisting of bridge priority plus MAC address.
RootPathCost	This field displays the path cost from the root port on this Switch to the root switch.
RootPort	This field displays the priority and number of the port on the Switch through which this Switch must communicate with the root of the Spanning Tree.
MaxAge	This field displays the maximum time (in seconds) the root switch can wait without receiving a configuration message before attempting to reconfigure.
HelloTime	This field displays the time interval (in seconds) at which the root switch transmits a configuration message.
ForwardDelay	This field displays the time (in seconds) the root switch will wait before changing states (that is, listening to learning to forwarding).
BridgeMaxAge	This field displays the maximum time (in seconds) the Switch can wait without receiving a configuration message before attempting to reconfigure.
BridgeHelloTime	This field displays the time interval (in seconds) at which the Switch transmits a configuration message.
BridgeForwardDelay	This field displays the time (in seconds) the Switch will wait before changing states (that is, listening to learning to forwarding).
TransmissionLimit	This field displays the maximum number of BPDUs that can be transmitted in the interval specified by **BridgeHelloTime**.
ForceVersion	This field indicates whether BPDUs are RSTP (a value less than 3) or MSTP (a value greater than or equal to 3).

54

SSH Commands

Use these commands to configure SSH on the Switch.

54.1 Command Summary

The following section lists the commands for this feature.

Table 115 ssh Command Summary

COMMAND	DESCRIPTION	M	P
`show ssh`	Displays general SSH settings.	E	3
`show ssh session`	Displays current SSH session(s).	E	3
`show ssh known-hosts`	Displays known SSH hosts information.	E	3
`ssh known-hosts <host-ip> <1024|ssh-rsa|ssh-dsa> <key>`	Adds a remote host to which the Switch can access using SSH service.	C	13
`no ssh known-hosts <host-ip>`	Removes the specified remote hosts from the list of all known hosts.	C	13
`no ssh known-hosts <host-ip> <1024|ssh-rsa|ssh-dsa>`	Removes the specified remote hosts with the specified public key (1024-bit RSA1, RSA or DSA).	C	13
`show ssh key <rsa1|rsa|dsa>`	Displays internal SSH public and private key information.	E	3
`no ssh key <rsa1|rsa|dsa>`	Disables the secure shell server encryption key. Your Switch supports SSH versions 1 and 2 using RSA and DSA authentication.	C	13
`ssh <1|2> <[user@]dest-ip> [command </>]`	Connects to an SSH server with the specified SSH version and, optionally, adds commands to be executed on the server.	E	3

54.2 Command Examples

This example disables the secure shell RSA1 encryption key and removes remote hosts 172.165.1.8 and 172.165.1.9 (with an SSH-RSA encryption key) from the list of known hosts.

```
sysname(config)# no ssh key rsa1
sysname(config)# no ssh known-hosts 172.165.1.8
sysname(config)# no ssh known-hosts 172.165.1.9 ssh-rsa
```

This example shows the general SSH settings.

```
sysname# show ssh
Configuration
    Version              : SSH-1 & SSH-2 (server & client), SFTP (server)
    Server                : Enabled
    Port                  : 22
    Host key bits         : 1024
    Server key bits       : 768
    Support authentication: Password
    Support ciphers       : AES, 3DES, RC4, Blowfish, CAST
    Support MACs          : MD5, SHA1
    Compression levels    : 1~9

Sessions:
    Proto Serv Remote IP        Port Local IP         Port   Bytes In
Bytes Out
```

The following table describes the labels in this screen.

Table 116 show ssh

LABEL	DESCRIPTION
Configuration	
Version	This field displays the SSH versions and related protocols the Switch supports.
Server	This field indicates whether or not the SSH server is enabled.
Port	This field displays the port number the SSH server uses.
Host key bits	This field displays the number of bits in the Switch's host key.
Server key bits	This field displays the number of bits in the SSH server's public key.
Support authentication	This field displays the authentication methods the SSH server supports.
Support ciphers	This field displays the encryption methods the SSH server supports.
Support MACs	This field displays the message digest algorithms the SSH server supports.
Compression levels	This field displays the compression levels the SSH server supports.
Sessions	This section displays the current SSH sessions.
Proto	This field displays the SSH protocol (SSH-1 or SSH-2) used in this session.
Serv	This field displays the type of SSH state machine (SFTP or SSH) in this session.
Remote IP	This field displays the IP address of the SSH client.
Port	This field displays the port number the SSH client is using.
Local IP	This field displays the IP address of the SSH server.
Port	This field displays the port number the SSH server is using.
Bytes In	This field displays the number of bytes the SSH server has received from the SSH client.
Bytes Out	This field displays the number of bytes the SSH server has sent to the SSH client.

55

Static Route Commands

Use these commands to tell the Switch how to forward IP traffic. IP static routes are used by layer-2 Switches to ensure they can respond to management stations not reachable via the default gateway and to proactively send traffic, for example when sending SNMP traps or conducting IP connectivity tests using ping.

Layer-3 Switches use static routes to forward traffic via gateways other than those defined as the default gateway.

55.1 Command Summary

The following section lists the commands for this feature.

Table 117 ip route Command Summary

COMMAND	DESCRIPTION	M	P
`show ip route`	Displays the IP routing table.	E	3
`show ip route static`	Displays the static routes.	E	3
`ip route <ip> <mask> <next-hop-ip> [metric <metric>] [name <name>] [inactive]`	Creates a static route. If the `<ip> <mask>` already exists, the Switch deletes the existing route first. Optionally, also sets the metric, sets the name, and/or deactivates the static route. *metric*: 1-15 *name*: 1-10 English keyboard characters Note: If the `<next-hop-ip>` is not directly connected to the Switch, you must make the static route `inactive`.	C	13
`no ip route <ip> <mask>`	Removes a specified static route.	C	13
`no ip route <ip> <mask> inactive`	Enables a specified static route.	C	13

55.2 Command Examples

This example shows the current routing table.

```
sysname# show ip route
Dest            FF Len Device     Gateway         Metric stat Timer  Use

Route table in VPS00
172.16.37.0     00 24  swp00      172.16.37.206     1    041b 0      1494
127.0.0.0       00 16  swp00      127.0.0.1         1    041b 0      0
0.0.0.0         00 0   swp00      172.16.37.254     1    801b 0      12411

Original Global Route table
```

The following table describes the labels in this screen.

Table 118 show ip route

LABEL	DESCRIPTION
Dest	This field displays the destination network number. Along with **Len**, this field defines the range of destination IP addresses to which this entry applies.
FF	This field is reserved.
Len	This field displays the destination subnet mask. Along with **Dest**, this field defines the range of destination IP addresses to which this entry applies.
Device	This field is reserved.
Gateway	This field displays the IP address to which the Switch forwards packets whose destination IP address is in the range defined by **Dest** and **Len**.
Metric	This field displays the cost associated with this entry.
stat	This field is reserved.
Timer	This field displays the number of remaining seconds this entry remains valid. It displays **0** if the entry is always valid.
Use	This field displays the number of times this entry has been used to forward packets.

In this routing table, you can create an active static route if the <next-hop-ip> is in 172.16.37.0/24 or 127.0.0.0/16. You cannot create an active static route to other IP addresses.

For example, you cannot create an active static route that routes traffic for 192.168.10.1/24 to 192.168.1.1.

```
sysname# configure
sysname(config)# ip route 192.168.10.1 255.255.255.0 192.168.1.1
  Error : The Action is failed. Please re-configure setting.
```

You can create this static route if it is inactive, however.

```
sysname# configure
sysname(config)# ip route 192.168.10.1 255.255.255.0 192.168.1.1 inactive
```

You can create an active static route that routes traffic for 192.168.10.1/24 to 172.16.37.254.

```
sysname# configure
sysname(config)# ip route 192.168.10.1 255.255.255.0 172.16.37.254
sysname(config)# exit
sysname# show ip route static
  Idx Active  Name       Dest. Addr.     Subnet Mask     Gateway Addr.
Metric
   01   Y     static     192.168.10.1    255.255.255.0   172.16.37.254      1
```

56

Subnet-based VLAN Commands

Use these commands to configure subnet-based VLANs on the Switch.

56.1 Subnet-based VLAN Overview

Subnet-based VLANs allow you to group traffic based on the source IP subnet you specify. This allows you to assign priority to traffic from the same IP subnet.

See also Chapter 46 on page 155 for protocol-based VLAN commands and Chapter 62 on page 199 for VLAN commands.

56.2 Command Summary

The following section lists the commands for this feature.

Table 119 subnet-based-vlan Command Summary

COMMAND	DESCRIPTION	M	P
`show subnet-vlan`	Displays subnet based VLAN settings on the Switch.	E	3
`subnet-based-vlan`	Enables subnet based VLAN on the Switch.	C	13
`subnet-based-vlan dhcp-vlan-override`	Sets the Switch to force the DHCP clients to obtain their IP addresses through the DHCP VLAN.	C	13
`subnet-based-vlan name <name> source-ip <ip> mask-bits <mask-bits> vlan <vlan-id> priority <0-7>`	Specifies the name, IP address, subnet mask, VLAN ID of the subnet based VLAN you want to configure along with the priority you want to assign to the outgoing frames for this VLAN.	C	13
`subnet-based-vlan name <name> source-ip <ip> mask-bits <mask-bits> source-port <port> vlan <vlan-id> priority <0-7>`	Specifies the name, IP address, subnet mask, source-port and VLAN ID of the subnet based VLAN you want to configure along with the priority you want to assign to the outgoing frames for this VLAN. Note: Implementation on a per port basis is not available on all models.	C	13
`subnet-based-vlan name <name> source-ip <ip> mask-bits <mask-bits> vlan <vlan-id> priority <0-7> inactive`	Disables the specified subnet-based VLAN.	C	13
`no subnet-based-vlan`	Disables subnet-based VLAN on the Switch.	C	13

Table 119 subnet-based-vlan Command Summary (continued)

COMMAND	DESCRIPTION	M	P
`no subnet-based-vlan source-ip <ip> mask-bits <mask-bits>`	Removes the specified subnet from the subnet-based VLAN configuration.	C	13
`no subnet-based-vlan dhcp-vlan-override`	Disables the DHCP VLAN override setting for subnet-based VLAN(s).	C	13

56.3 Command Examples

This example configures a subnet-based VLAN (**subnet1VLAN**) with priority **6** and a VID of **200** for traffic received from IP subnet **172.16.37.1/24**.

```
sysname# subnet-based-vlan name subnet1VLAN source-ip 172.16.37.1 mask-bits
--> 24 vlan 200 priority 6
sysname(config)# exit
sysname# show subnet-vlan

Global Active :Yes
       Name       Src IP  Mask-Bits  Vlan  Priority  Entry Active
-----------  -----------  ---------  ----  --------  ------------
subnet1VLAN  172.16.37.1         24   200         6             1
```

57

Syslog Commands

Use these commands to configure the device's system logging settings and to configure the external syslog servers.

57.1 Command Summary

The following table describes user-input values available in multiple commands for this feature.

Table 120 syslog User-input Values

COMMAND	DESCRIPTION
type	Possible values: `system`, `interface`, `switch`, `aaa`, `ip`.

The following section lists the commands for this feature.

Table 121 syslog Command Summary

COMMAND	DESCRIPTION	M	P
`syslog`	Enables syslog logging.	C	13
`no syslog`	Disables syslog logging.	C	13

Table 122 syslog server Command Summary

COMMAND	DESCRIPTION	M	P
`syslog server <ip-address> level <level>`	Sets the IP address of the syslog server and the severity level. *level*: 0-7	C	13
`no syslog server <ip-address>`	Deletes the specified syslog server.	C	13
`syslog server <ip-address> inactive`	Disables syslog logging to the specified syslog server.	C	13
`no syslog server <ip-address> inactive`	Enables syslog logging to the specified syslog server.	C	13

Table 123 syslog type Command Summary

COMMAND	DESCRIPTION	M	P
`syslog type <type>`	Enables syslog logging for the specified log type.	C	13
`syslog type <type> facility <0-7>`	Sets the file location for the specified log type.	C	13
`no syslog type <type>`	Disables syslog logging for the specified log type.	C	13

PART V
Reference T-Z

58

TACACS+ Commands

Use these commands to configure external TACACS+ (Terminal Access Controller Access-Control System Plus) servers.

58.1 Command Summary

The following section lists the commands for this feature.

Table 124 tacacs-server Command Summary

COMMAND	DESCRIPTION	M	P
`show tacacs-server`	Displays TACACS+ server settings.	E	3
`tacacs-server timeout <1-1000>`	Specifies the TACACS+ server timeout value.	C	13
`tacacs-server mode <index-priority|round-robin>`	Specifies the mode for TACACS+ server selection.	C	13
`tacacs-server host <index> <ip> [auth-port <socket-number>] [key <key-string>]`	Specifies the IP address of the specified TACACS+ server. Optionally, sets the port number and key of the TACACS+ server. *index*: 1 or 2. *key-string*: 1-32 alphanumeric characters	C	13
`no tacacs-server <index>`	Disables TACACS+ authentication on the specified server.	C	13

Table 125 tacacs-accounting Command Summary

COMMAND	DESCRIPTION	M	P
`show tacacs-accounting`	Displays TACACS+ accounting server settings.	E	3
`tacacs-accounting timeout <1-1000>`	Specifies the TACACS+ accounting server timeout value.	C	13
`tacacs-accounting host <index> <ip> [acct-port <socket-number>] [key <key-string>]`	Specifies the IP address of the specified TACACS+ accounting server. Optionally, sets the port number and key of the external TACACS+ accounting server. *index*: 1 or 2. *key-string*: 1-32 alphanumeric characters	C	13
`no tacacs-accounting <index>`	Disables TACACS+ accounting on the specified server.	C	13

59

TFTP Commands

Use these commands to back up and restore configuration and firmware via TFTP.

59.1 Command Summary

The following section lists the commands for this feature.

Table 126 tftp Command Summary

COMMAND	DESCRIPTION	M	P
`copy tftp flash <ip> <remote-file>`	Restores firmware via TFTP.	E	13
`copy tftp config <index> <ip> <remote-file>`	Restores configuration with the specified filename from the specified TFTP server. *index*: 1.	E	13
`copy running-config tftp <ip> <remote-file>`	Backs up running configuration to the specified TFTP server with the specified file name.	E	13

60

Trunk Commands

Use these commands to logically aggregate physical links to form one logical, higher-bandwidth link. The Switch adheres to the IEEE 802.3ad standard for static and dynamic (Link Aggregate Control Protocol, LACP) port trunking.

Different models support different numbers of trunks (T1, T2, ...). This chapter uses a model that supports three trunks (T1, T2, and T3).

60.1 Command Summary

The following section lists the commands for this feature.

Table 127 trunk Command Summary

COMMAND	DESCRIPTION	M	P
`show trunk`	Displays link aggregation information.	E	3
`trunk <T1|T2|T3>`	Activates a trunk group.	C	13
`no trunk <T1|T2|T3>`	Disables the specified trunk group.	C	13
`trunk <T1|T2|T3> interface <port-list>`	Adds a port(s) to the specified trunk group.	C	13
`no trunk <T1|T2|T3> interface <port-list>`	Removes ports from the specified trunk group.	C	13
`trunk <T1|T2|T3> lacp`	Enables LACP for a trunk group.	C	13
`no trunk <T1|T2|T3> lacp`	Disables LACP in the specified trunk group.	C	13
`trunk interface <port-list> timeout <lacp-timeout>`	Defines LACP timeout period (in seconds) for the specified port(s). *lacp-timeout*: 1 or 30	C	13

Table 128 lacp Command Summary

COMMAND	DESCRIPTION	M	P
`show lacp`	Displays LACP (Link Aggregation Control Protocol) settings.	E	3
`lacp`	Enables Link Aggregation Control Protocol (LACP).	C	13
`no lacp`	Disables the link aggregation control protocol (dynamic trunking) on the Switch.	C	13
`lacp system-priority <1-65535>`	Sets the priority of an active port using LACP.	C	13

60.2 Command Examples

This example activates trunk 1 and places ports 5-8 in the trunk using static link aggregation.

```
sysname(config)# trunk t1
sysname(config)# trunk t1 interface 5-8
```

This example disables trunk one (T1) and removes ports 1, 3, 4, and 5 from trunk two (T2).

```
sysname(config)# no trunk T1
sysname(config)# no trunk T3 lacp
sysname(config)# no trunk T2 interface 1,3-5
```

This example looks at the current trunks.

```
sysname# show trunk
Group ID 1:     inactive
  Status: -
  Member number: 0
Group ID 2:     inactive
  Status: -
  Member number: 0
Group ID 3:     inactive
  Status: -
  Member number: 0
```

The following table describes the labels in this screen.

Table 129 show trunk

LABEL	DESCRIPTION
Group ID	This field displays the trunk ID number and the current status. **inactive**: This trunk is disabled. **active**: This trunk is enabled.
Status	This field displays how the ports were added to the trunk. **-**: The trunk is disabled. **Static**: The ports are static members of the trunk. **LACP**: The ports joined the trunk via LACP.
Member Number	This field shows the number of ports in the trunk.
Member	This field is displayed if there are ports in the trunk. This field displays the member port(s) in the trunk.

This example shows the current LACP settings.

```
sysname# show lacp
AGGREGATOR INFO:
ID: 1
  [(0000,00-00-00-00-00-00,0000,00,0000)][(0000,00-00-00-00-00-00
-->,0000,00,0000)]
LINKS :
SYNCS :

ID: 2
  [(0000,00-00-00-00-00-00,0000,00,0000)][(0000,00-00-00-00-00-00
-->,0000,00,0000)]
LINKS :
SYNCS :

ID: 3
  [(0000,00-00-00-00-00-00,0000,00,0000)][(0000,00-00-00-00-00-00
--> ,0000,00,0000)]
LINKS :
SYNCS :
```

The following table describes the labels in this screen.

Table 130 show lacp

LABEL	DESCRIPTION
ID	This field displays the trunk ID to identify a trunk group, that is, one logical link containing multiple ports.
[(0000,00-00-00-00-00-00,0000,00,0000)]	This field displays the system priority, MAC address, key, port priority, and port number.
LINKS	This field displays the ports whose link state are up.
SYNCS	These are the ports that are currently transmitting data as one logical link in this trunk group.

61

trTCM Commands

This chapter explains how to use commands to configure the Two Rate Three Color Marker (trTCM) feature on the Switch.

61.1 trTCM Overview

Two Rate Three Color Marker (trTCM, defined in RFC 2698) is a type of traffic policing that identifies packets by comparing them to two user-defined rates: the Committed Information Rate (CIR) and the Peak Information Rate (PIR). trTCM then tags the packets:

- red - if the packet exceeds the PIR
- yellow - if the packet is below the PIR, but exceeds the CIR
- green - if the packet is below the CIR

The colors reflect the packet's loss priority and the Switch changes the packet's DiffServ Code Point (DSCP) value based on the color.

61.2 Command Summary

The following section lists the commands for this feature.

Table 131 trtcm Command Summary

COMMAND	DESCRIPTION	M	P
`trtcm`	Enables trTCM on the Switch.	C	13
`trtcm mode <color-aware|color-blind>`	Sets the mode for trTCM on the Switch.	C	13
`no trtcm`	Disables trTCM feature on the Switch.	C	13
`interface port-channel <port-list>`	Enters subcommand mode for configuring the specified ports.	C	13
`trtcm`	Enables trTCM on the specified port(s).	C	13
`no trtcm`	Disables trTCM on the port(s).	C	13
`trtcm cir <rate>`	Sets the Commit Information Rate on the port(s).	C	13
`trtcm pir <rate>`	Sets the Peak Information Rate on the port(s).	C	13
`trtcm dscp green <0-63>`	Specifies the DSCP value to use for packets with low packet loss priority.	C	13

Table 131 trtcm Command Summary (continued)

COMMAND	DESCRIPTION	M	P
trtcm dscp yellow <0-63>	Specifies the DSCP value to use for packets with medium packet loss priority.	C	13
trtcm dscp red <0-63>	Specifies the DSCP value to use for packets with high packet loss priority.	C	13

61.3 Command Examples

This example activates trTCM on the Switch with the following settings:

- Sets the Switch to inspect the DSCP value of the packets (color-aware mode).
- Enables trTCM on ports 1-5.
- Sets the Committed Information Rate (CIR) to 4000 Kbps.
- Sets the Peak Information Rate (PIR) to 4500 Kbps.
- Specifies DSCP value 7 for green packets, 22 for yellow packets and 44 for red packets.

```
sysname(config)# trtcm
sysname(config)# trtcm mode color-aware
sysname(config)# interface port-channel 1-5
sysname(config-interface)# trtcm
sysname(config-interface)# trtcm cir 4000
sysname(config-interface)# trtcm pir 4500
sysname(config-interface)# trtcm dscp green 7
sysname(config-interface)# trtcm dscp yellow 22
sysname(config-interface)# trtcm dscp red 44
sysname(config-interface)# exit
sysname(config)# exit
sysname# show running-config interface port-channel 1 trtcm
  Building configuration...

  Current configuration:

interface port-channel 1
  trtcm
  trtcm cir 4000
  trtcm pir 4500
  trtcm dscp green 7
  trtcm dscp yellow 22
  trtcm dscp red 44
exit
```

62

VLAN Commands

Use these commands to configure IEEE 802.1Q VLAN.

See Chapter 63 on page 203 for VLAN IP commands.

62.1 VLAN Overview

A VLAN (Virtual Local Area Network) allows a physical network to be partitioned into multiple logical networks. Devices on a logical network belong to one group. A device can belong to more than one group. With VLAN, a device cannot directly talk to or hear from devices that are not in the same group(s); the traffic must first go through a router.

VLAN is unidirectional; it only governs outgoing traffic.

62.2 VLAN Configuration Overview

1. Use the `vlan <vlan-id>` command to configure or create a VLAN on the Switch. The Switch automatically enters config-vlan mode. Use the `exit` command when you are finished configuring the VLAN.
2. Use the `interface port-channel <port-list>` command to set the VLAN settings on a port. The Switch automatically enters config-interface mode. Use the `pvid <vlan-id>` command to set the VLAN ID you created for the port-list in the PVID table. Use the `exit` command when you are finished configuring the ports.

```
sysname (config)# vlan 2000
sysname (config-vlan)# name up1
sysname (config-vlan)# fixed 5-8
sysname (config-vlan)# no untagged 5-8
sysname (config-vlan)# exit
sysname (config)# interface port-channel 5-8
sysname (config-interface)# pvid 2000
sysname (config-interface)# exit
```

See Chapter 24 on page 97 for `interface port-channel` commands.

62.3 Command Summary

The following section lists the commands for this feature.

Table 132 vlan Command Summary

COMMAND	DESCRIPTION	M	P
`show vlan`	Displays the status of all VLANs.	E	3
`show vlan <vlan-id>`	Displays the status of the specified VLAN.	E	3
`vlan-type <802.1q|port-based>`	Specifies the VLAN type.	C	13
`vlan <vlan-id>`	Enters config-vlan mode for the specified VLAN. Creates the VLAN, if necessary.	C	13
`fixed <port-list>`	Specifies the port(s) to be a permanent member of this VLAN group.	C	13
`no fixed <port-list>`	Sets fixed port(s) to normal port(s).	C	13
`forbidden <port-list>`	Specifies the port(s) you want to prohibit from joining this VLAN group.	C	13
`no forbidden <port-list>`	Sets forbidden port(s) to normal port(s).	C	13
`inactive`	Disables the specified VLAN.	C	13
`no inactive`	Enables the specified VLAN.	C	13
`name <name>`	Specifies a name for identification purposes. *name*: 1-64 English keyboard characters	C	13
`normal <port-list>`	Specifies the port(s) to dynamically join this VLAN group using GVRP	C	13
`untagged <port-list>`	Specifies the port(s) you don't want to tag all outgoing frames transmitted with this VLAN Group ID.	C	13
`no untagged <port-list>`	Specifies the port(s) you want to tag all outgoing frames transmitted with this VLAN Group ID.	C	13
`no vlan <vlan-id>`	Deletes a VLAN.	C	13

The following section lists the commands for the ingress checking feature

VLAN ingress checking implementation differs across Switch models.

- Some models enable or disable VLAN ingress checking on all the ports via the `vlan1q ingress-check` command.

- Other models enable or disable VLAN ingress checking on each port individually via the `ingress-check` command in the config-interface mode.

Table 133 vlan1q ingress-check Command Summary

COMMAND	DESCRIPTION	M	P
`show vlan1q ingress-check`	Displays ingress check settings on the Switch.	E	3
`vlan1q ingress-check`	Enables ingress checking on the Switch. The Switch discards incoming frames on a port for VLANs that do not include this port in its member set.	C	13
`no vlan1q ingress-check`	Disables ingress checking on the Switch.	C	13

Table 134 ingress-check Command Summary

COMMAND	DESCRIPTION	M	P
`interface port-channel <port-list>`	Enters config-interface mode for the specified port(s).	C	13
`ingress-check`	Enables ingress checking on the specified ports. The Switch discards incoming frames for VLANs that do not include this port in its member set.	C	13
`no ingress-check`	Disables ingress checking on the specified ports.	C	13

62.4 Command Examples

This example configures ports 1 to 5 as fixed and untagged ports in VLAN 2000.

```
sysname (config)# vlan 2000
sysname (config-vlan)# fixed 1-5
sysname (config-vlan)# untagged 1-5
```

This example deletes entry 2 in the static VLAN table.

```
sysname (config)# no vlan 2
```

This example shows the VLAN table.

```
sysname# show vlan
  The Number of VLAN:    3
  Idx. VID   Status    Elap-Time    TagCtl
  ---- ----  -------- ------------ ------------------------
  1    1    Static     0:12:13     Untagged :1-2
                                    Tagged   :

  2   100    Static     0:00:17    Untagged :
                                    Tagged   :1-4

  3   200    Static     0:00:07    Untagged :1-2
                                    Tagged   :3-8
```

The following table describes the labels in this screen.

Table 135 show vlan

LABEL	DESCRIPTION
The Number of VLAN	This field displays the number of VLANs on the Switch.
Idx.	This field displays an entry number for each VLAN.
VID	This field displays the VLAN identification number.
Status	This field displays how this VLAN was added to the Switch. **Dynamic**: The VLAN was added via GVRP. **Static**: The VLAN was added as a permanent entry **Other**: The VLAN was added in another way, such as Multicast VLAN Registration (MVR).
Elap-Time	This field displays how long it has been since a dynamic VLAN was registered or a static VLAN was set up.
TagCtl	This field displays untagged and tagged ports. **Untagged**: These ports do not tag outgoing frames with the VLAN ID. **Tagged**: These ports tag outgoing frames with the VLAN ID.

This example enables ingress checking on ports 1-5.

```
sysname (config)# interface port-channel 1-5
sysname (config-vlan)# ingress-check
```

63

VLAN IP Commands

Use these commands to configure the default gateway device and add IP domains for VLAN.

63.1 IP Interfaces Overview

The Switch needs an IP address for it to be managed over the network. The factory default IP address is 192.168.1.1. The subnet mask specifies the network number portion of an IP address. The factory default subnet mask is 255.255.255.0.

63.2 Command Summary

The following section lists the commands for this feature.

Table 136 vlan ip address Command Summary

COMMAND	DESCRIPTION	M	P
`show vlan <vlan-id>`	Displays the status of the specified VLAN.	E	3
`vlan <1-4094>`	Enters config-vlan mode for the specified VLAN. Creates the VLAN, if necessary.	C	13
`ip address default-management dhcp-bootp`	Configures the Switch to get the in-band management IP address from a DHCP server.	C	13
`no ip address default-management dhcp-bootp`	Configures the Switch to use the static in-band management IP address. The Switch uses the default IP address of 192.168.1.1 if you do not configure a static IP address.	C	13
`ip address default-management <ip-address> <mask>`	Sets and enables the in-band management IP address and subnet mask.	C	13
`ip address default-management dhcp-bootp release`	Releases the in-band management IP address provided by a DHCP server.	C	13
`ip address default-management dhcp-bootp renew`	Updates the in-band management IP address provided by a DHCP server.	C	13
`ip address <ip-address> <mask>`	Sets the IP address and subnet mask of the Switch in the specified VLAN.	C	13
`ip address <ip-address> <mask> manageable`	Sets the IP address and subnet mask of the Switch in the specified VLAN. Some switch models require that you execute this command to ensure that remote management via HTTP, Telnet or SNMP is activated.	C	13
`no ip address <ip-address> <mask>`	Deletes the IP address and subnet mask from this VLAN.	C	13

Table 136 vlan ip address Command Summary (continued)

COMMAND	DESCRIPTION	M	P
`ip address default-gateway <ip-address>`	Sets a default gateway IP address for this VLAN.	C	13
`no ip address default-gateway`	Deletes the default gateway from this VLAN.	C	13

63.3 Command Examples

See Section 3.4 on page 22.

64

VLAN Port Isolation Commands

Use these commands to configure VLAN port isolation on the Switch. VLAN port isolation allows each port to communicate only with the CPU management port and the uplink ports, but not to communicate with each other.

64.1 Command Summary

The following section lists the commands for this feature.

Table 137 vlan1q port-isolation Command Summary

COMMAND	DESCRIPTION	M	P
`show vlan1q port-isolation`	Displays port isolation settings.	E	3
`vlan1q port-isolation`	Enables VLAN port isolation.	C	13
`no vlan1q port-isolation`	Disables VLAN port isolation.	C	13

65

VLAN Stacking Commands

Use these commands to add an outer VLAN tag to the inner IEEE 802.1Q tagged frames that enter your network.

65.1 Command Summary

The following section lists the commands for this feature.

Table 138 vlan-trunking Command Summary

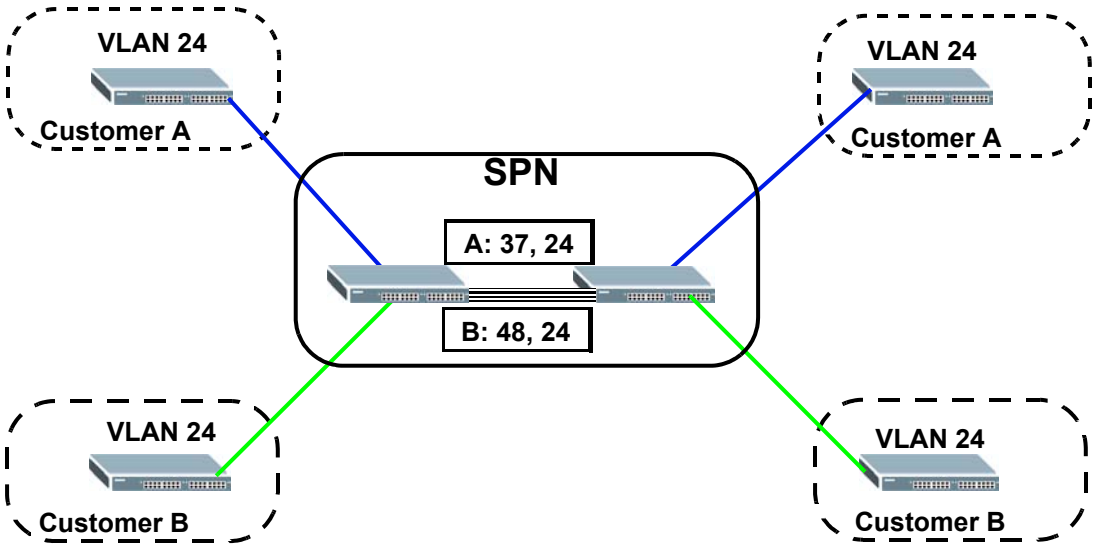
COMMAND	DESCRIPTION	M	P
`show vlan-stacking`	Displays VLAN stacking settings.	E	3
`vlan-stacking`	Enables VLAN stacking on the Switch.	C	13
`no vlan-stacking`	Disables VLAN stacking on the Switch.	C	13
`vlan-stacking <sptpid>`	Sets the SP TPID (Service Provider Tag Protocol Identifier). SP TPID is a standard Ethernet type code identifying the frame and indicating whether the frame carries IEEE 802.1Q tag information. Enter a four-digit hexadecimal number from 0000 to FFFF.	C	13
`interface port-channel <port-list>`	Enters config-interface mode for the specified port(s).	C	13
`vlan-stacking priority <0-7>`	Sets the priority of the specified port(s) in VLAN stacking.	C	13
`vlan-stacking role <normal|access|tunnel>`	Sets the VLAN stacking port roles of the specified port(s). `normal`: The Switch ignores frames received (or transmitted) on this port with VLAN stacking tags. `access`: the Switch adds the SP TPID tag to all incoming frames received on this port. `tunnel`: (available for Gigabit and faster ports only) for egress ports at the edge of the service provider's network. Note: In order to support VLAN stacking on a port, the port must be able to allow frames of 1526 Bytes (1522 Bytes + 4 Bytes for the second tag) to pass through it.	C	13
`vlan-stacking SPVID <1-4094>`	Sets the service provider VID of the specified port(s).	C	13

65.2 Command Examples

In the following example figure, both **A** and **B** are Service Provider's Network (**SPN**)

customers with VPN tunnels between their head offices and branch offices respectively. Both have an identical VLAN tag for their VLAN group. The service provider can separate these two VLANs within its network by adding tag **37** to distinguish customer **A** and tag **48** to distinguish customer **B** at edge device 1 and then stripping those tags at edge device 2 as the data frames leave the network.

Figure 6 Example: VLAN Stacking



This example shows how to configure ports 1 and 2 on the Switch to tag incoming frames with the service provider's VID of 37 (ports are connected to customer A network). This example also shows how to set the priority for ports 1 and 2 to 3.

```
sysname(config)# vlan-stacking
sysname(config)# vlan-stacking 8100
sysname(config)# interface port-channel 1-2
sysname(config-interface)# vlan-stacking role access
sysname(config-interface)# vlan-stacking spvid 37
sysname(config-interface)# vlan-stacking priority 3
sysname(config-interface)# exit
sysname(config)# exit
sysname# show vlan-stacking
Switch Vlan Stacking Configuration
Operation: active
STPID: 0x8100

Port            Role            SPVID           Priority
01              access          37              3
02              access          37              3
03              access          1               0
04              access          1               0
05              access          1               0
....
```

66

VLAN Trunking Commands

Use these commands to decide what the Switch should do with frames that belong to unknown VLAN groups.

66.1 Command Summary

The following section lists the commands for this feature.

Table 139 vlan-trunking Command Summary

COMMAND	DESCRIPTION	M	P
`interface port-channel <port-list>`	Enters config-interface mode for the specified port(s).	C	13
`vlan-trunking`	Enables VLAN trunking on ports connected to other switches or routers (but not ports directly connected to end users). This allows frames belonging to unknown VLAN groups to go out via the VLAN-trunking port.	C	13
`no vlan-trunking`	Disables VLAN trunking on the port(s).	C	13

67

VRRP Commands

This chapter explains how to use commands to configure the Virtual Router Redundancy Protocol (VRRP) on the Switch.

67.1 VRRP Overview

VRRP is a protocol that allows you to configure redundant router connections. The protocol reduces downtime in case of a single link failure. Multiple routers are connected and one is elected as the master router. If the master router fails, then one of the backup routers takes over the routing function within a routing domain.

67.2 Command Summary

The following section lists the commands for this feature.

Table 140 VRRP Command Summary

COMMAND	DESCRIPTION	M	P
`router vrrp network <ip-address>/<mask-bits> vr-id <1~7> uplink-gateway <ip-address>`	Adds a new VRRP network and enters the VRRP configuration mode.	C	13
`name <name>`	Sets a descriptive name of the VRRP setting for identification purposes.	C	13
`priority <1~254>`	Sets the priority of the uplink-gateway.	C	13
`interval <1~255>`	Sets the time interval (in seconds) between Hello message transmissions.	C	13
`primary-virtual-ip <ip-address>`	Sets the primary VRRP virtual gateway IP address.	C	13
`no primary-virtual-ip <ip-address>`	Resets the primary VRRP virtual gateway IP address.	C	13
`secondary-virtual-ip <ip-address>`	Sets the secondary VRRP virtual gateway IP address.	C	13
`no secondary-virtual-ip`	Sets the network to use the default secondary virtual gateway (0.0.0.0).	C	13
`no primary-virtual-ip`	Resets the network to use the default primary virtual gateway (interface IP address).	C	13
`inactive`	Disables the VRRP settings.	C	13
`no inactive`	Activates this VRRP.	C	13

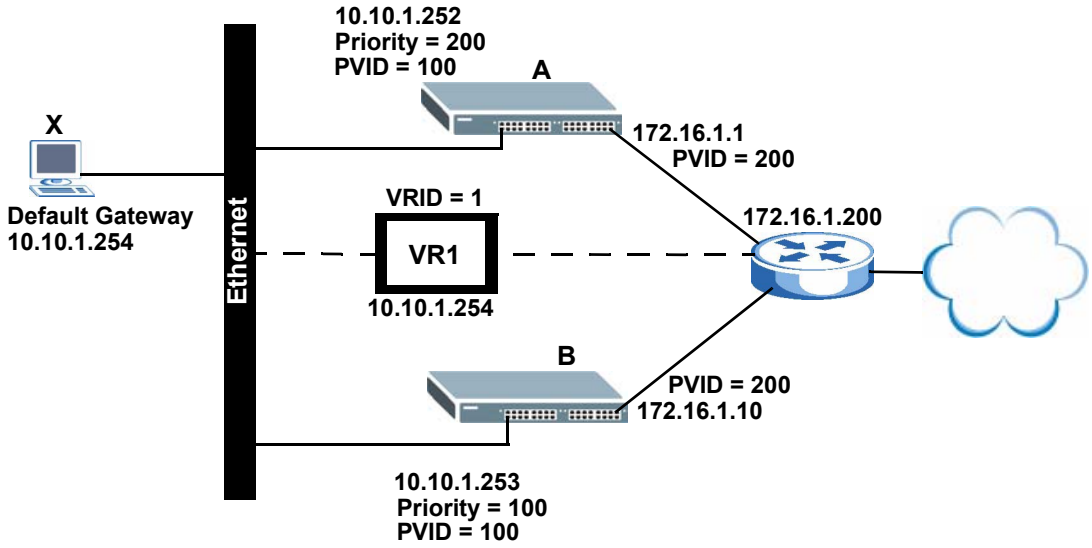
Table 140 VRRP Command Summary (continued)

COMMAND	DESCRIPTION	M	P
`no preempt`	Disables VRRP preemption mode.	C	13
`preempt`	Enables preemption mode.	C	13
`exit`	Exits from the VRRP command mode.	C	13
`no router vrrp network <ip-address>/<mask-bits> vr-id <1~7>`	Deletes VRRP settings.	C	13
`interface route-domain <ip-address>/<mask-bits> ip vrrp authentication-key <key>`	Sets the VRRP authentication key. *key*: Up to 8 alphanumeric characters.	C	13
`interface route-domain <ip-address>/<mask-bits> no ip vrrp authentication-key`	Resets the VRRP authentication key.	C	13
`show router vrrp`	Displays VRRP settings.	C	13

67.3 Command Examples

The following figure shows a VRRP network example with the switches (**A** and **B**) implementing one virtual router **VR1** to ensure the link between the host **X** and the uplink gateway **G**. Host **X** is configured to use **VR1** (192.168.1.254) as the default gateway. Switch **A** has a higher priority, so it is the master router. Switch **B**, having a lower priority, is the backup router.

Figure 7 Example: VRRP



This example shows how to create the IP routing domains and configure the Switch to act as router **A** in the topology shown in Figure 7 on page 212.

```
sysname# config
sysname(config)# vlan 100
sysname(config-vlan)# fixed 1-4
sysname(config-vlan)# untagged 1-4
sysname(config-vlan)# ip address 10.10.1.252 255.255.255.0
sysname(config-vlan)# exit
sysname(config) interface port-channel 1-4
sysname(config-interface)# pvid 100
sysname(config-interface)# exit
sysname(config)# vlan 200
sysname(config-vlan)# fixed 24-28
sysname(config-vlan)# untagged 24-28
sysname(config-vlan)# ip address 172.16.1.1 255.255.255.0
sysname(config-vlan)# exit
sysname(config)# interface port-channel 24-28
sysname(config-interface)# pvid 200
sysname(config-interface)# exit
sysname(config)# router vrrp network 10.10.1.252/24 vr-id 1 uplink-gateway
172.16.1.200
sysname(config-vrrp)# name VRRP-networkA
sysname(config-vrrp)# priority 200
sysname(config-vrrp)# interval 2
sysname(config-vrrp)# primary-virtual-ip 10.10.1.254
sysname(config-vrrp)# exit
sysname(config)#
```

This example shows how to create the IP routing domains and configure the Switch to act as router **B** in the topology shown in Figure 7 on page 212.

```
sysname# config
sysname(config)# vlan 100
sysname(config-vlan)# fixed 1-4
sysname(config-vlan)# untagged 1-4
sysname(config-vlan)# ip address 10.10.1.253 255.255.255.0
sysname(config-vlan)# exit
sysname(config) interface port-channel 1-4
sysname(config-interface)# pvid 100
sysname(config-interface)# exit
sysname(config)# vlan 200
sysname(config-vlan)# fixed 24-28
sysname(config-vlan)# untagged 24-28
sysname(config-vlan)# ip address 172.16.1.10 255.255.255.0
sysname(config-vlan)# exit
sysname(config)# interface port-channel 24-28
sysname(config-interface)# pvid 200
sysname(config-interface)# exit
sysname(config)# router vrrp network 10.10.1.253/24 vr-id 1 uplink-gateway
172.16.1.200
sysname(config-vrrp)# name VRRP-networkB
sysname(config-vrrp)# interval 2
sysname(config-vrrp)# primary-virtual-ip 10.10.1.254
sysname(config-vrrp)# exit
sysname(config)#
```

68

Additional Commands

Use these commands to configure or perform additional features on the Switch.

68.1 Command Summary

The following section lists the commands for this feature.

Table 141 Command Summary: Changing Modes or Privileges

COMMAND	DESCRIPTION	M	P
`enable`	Changes the session's privilege level to 14 and puts the session in enable mode (if necessary). The user has to provide the enable password. See Section 2.1.3.1 on page 16.	E	0
`enable <0-14>`	Raises the session's privilege level to the specified level and puts the session in enable mode if the specified level is 13 or 14. The user has to provide the password for the specified privilege level. See Section 2.1.3.2 on page 16.	E	0
`disable`	Changes the session's priority level to 0 and changes the mode to user mode. See Section 2.1.3.3 on page 17.	E	13
`configure`	Changes the mode to config mode.	E	13
`interface port-channel <port-list>`	Enters config-interface mode for the specified port(s).	C	13
`mvr <1-4094>`	Enters config-mvr mode for the specified MVR (multicast VLAN registration). Creates the MVR, if necessary.	C	13
`vlan <1-4094>`	Enters config-vlan mode for the specified VLAN. Creates the VLAN, if necessary.	C	13
`exit`	Returns to the previous mode.	C	13
`logout`	Logs out of the CLI.	E	0

Table 142 Command Summary: Additional Enable Mode

COMMAND	DESCRIPTION	M	P
`baudrate <1|2|3|4|5>`	Changes the console port speed. 1: 38400 bps 2: 19200 bps 3: 9600 bps 4: 57600 bps 5: 115200 bps	E	13
`boot config`	Restarts the Switch (cold reboot) with the specified configuration file.	E	13

Table 142 Command Summary: Additional Enable Mode (continued)

COMMAND	DESCRIPTION	M	P
`cable-diagnostics <port-list>`	Perform a physical wire-pair test of the Ethernet connections on the specified port(s). **Ok**: The physical connection between the wire-pair is okay. **Open**: There is no physical connection between the wire-pair.	E	13
`ping <ip|host-name> [vlan <vlan-id>] [size <0-1472>] [-t]`	Sends Ping packets to the specified Ethernet device. `vlan vlan-id`: Specifies the VLAN ID to which the Ethernet device belongs. `size <0-1472>`: Specifies the size of the Ping packet. `-t`: Sends Ping packets to the Ethernet device indefinitely. Press `[CTRL]+C` to terminate the Ping process.	E	0
`ping help`	Provides more information about the specified command.	E	0
`reload config`	Restarts the system (warm reboot) with the specified configuration file.	E	13
`show alarm-status`	Displays alarm status.	E	0
`show cpu-utilization`	Displays the CPU utilization statistics on the Switch.	E	0
`show hardware-monitor <C|F>`	This command is not available in all models. Displays current hardware monitor information with the specified temperature unit (Celsius **C** or Fahrenheit **F**).	E	0
`show poe-status`	This command is available for PoE models only. Displays information about Power over Ethernet (PoE).	E	0
`show system-information`	Displays general system information.	E	0
`show version [flash]`	Display the version of the currently running firmware on the Switch. Optionally, display the version of the currently installed firmware on the flash memory.	E	0
`test interface port-channel <port-list>`	Performs an internal loopback test on the specified ports. The test returns `Passed!` or `Failed!`.	E	13
`traceroute <ip|host-name> [vlan <vlan-id>] [ttl <1-255>] [wait <1-60>] [queries <1-10>]`	Determines the path a packet takes to the specified Ethernet device. `vlan <vlan-id>`: Specifies the VLAN ID to which the Ethernet device belongs. `ttl <1-255>`: Specifies the Time To Live (TTL) period. `wait <1-60>`: Specifies the time period to wait. `queries <1-10>`: Specifies how many times the Switch performs the traceroute function.	E	0
`traceroute help`	Provides more information about the specified command.	E	0
`write memory`	Saves current configuration in volatile memory to the configuration file the Switch is currently using.	E	13

Table 143 Command Summary: Additional Configure Mode

COMMAND	DESCRIPTION	M	P
`bcp-transparency`	Enables Bridge Control Protocol (BCP) transparency on the Switch.	C	13
`default-management <in-band|out-of-band>`	Sets which traffic flow (in-band or out-of-band) the Switch sends packets or originating from itself (such as SNMP traps, ping	E	13
`hostname <name>`	Sets the Switch's name for identification purposes. `name`: 1-64 printable characters; spaces are allowed if you put the string in double quotation marks (“).	C	13

68.2 Command Examples

This example checks the cable pairs on port 7.

```
sysname# cable-diagnostics 7
port 7
  cable diagnostics result
        pairA: Ok
        pairB: Ok
```

This example sends Ping requests to an Ethernet device with IP address 172.16.37.254.

```
sysname# ping 172.16.37.254
Resolving 172.16.37.254... 172.16.37.254
 sent  rcvd  rate    rtt     avg    mdev     max     min  reply from
    1     1  100       0       0       0       0       0  172.16.37.254
    2     2  100       0       0       0       0       0  172.16.37.254
    3     3  100      10       1       3      10       0  172.16.37.254
```

The following table describes the labels in this screen.

Table 144 ping

LABEL	DESCRIPTION
sent	This field displays the sequence number of the ICMP request the Switch sent.
rcvd	This field displays the sequence number of the ICMP response the Switch received.
rate	This field displays the percentage of ICMP responses for ICMP requests.
rtt	This field displays the round trip time of the ping.
avg	This field displays the average round trip time to ping the specified IP address.
mdev	This field displays the standard deviation in the round trip time to ping the specified IP address.
max	This field displays the maximum round trip time to ping the specified IP address.
min	This field displays the minimum round trip time to ping the specified IP address.
reply from	This field displays the IP address from which the Switch received the ICMP response.

This example shows the current status of the various alarms in the Switch.

```
sysname# show alarm-status
             name  status  suppressAlarm  alarmLED
----------------  ------  -------------  --------
          VOLTAGE  Normal             No       Off
      TEMPERATURE  Normal             No       Off
              FAN  Normal             No       Off
    POE OVER LOAD  Normal             No       Off
POE SHORT CIRCUIT  Normal             No       Off
     POE POWERBOX  Normal            Yes       Off
```

The following table describes the labels in this screen.

Table 145 show alarm-status

LABEL	DESCRIPTION
name	This field displays the name or type of the alarm.
status	This field displays the status of the alarm. **Normal**: The alarm is off. **Error**: The alarm is on.
suppressAlarm	This field displays whether or not the alarm is inactive.
alarmLED	This field displays whether or not the LED for this alarm is on.

This example shows the current and recent CPU utilization.

```
sysname# show cpu-utilization
  CPU usage status:
   baseline 1715384 ticks
   sec   ticks   util sec   ticks   util sec   ticks   util sec   ticks
util
   --- ------- ------ --- ------- ------ --- ------- ------ --- -------
     0  657543  61.67   1  255118  85.13   2  394329  77.01   3  620008
63.85
     4  195580  88.60   5  791000  53.89   6  137625  91.98   7  508456
70.36
-------------------------------- SNIP --------------------------------
```

The following table describes the labels in this screen.

Table 146 show cpu-utilization

LABEL	DESCRIPTION
baseline	This field displays the number of CPU clock cycles per second.
sec	This field displays the historical interval. Interval 0 is the time starting one second ago to the current instant. Interval 1 is the time starting two seconds ago to one second ago. Interval 2 is the time starting three seconds ago to two seconds ago.
ticks	This field displays the number of CPU clock cycles the CPU was not used during the interval.
util	This field displays the CPU utilization during the interval. `util = [(baseline - ticks) / baseline] * 100`

This example looks at the current sensor readings from various places in the hardware.

```
sysname# show hardware-monitor C

Temperature Unit : (C)
Temperature(%c)  Current    Max    Min  Threshold  Status
---------------  -------  -----  -----  ---------  ------
           CPU      33.0   35.0   28.0       85.0  Normal
           MAC      31.0   33.0   27.0       75.0  Normal
         LOCAL      33.0   34.0   28.0       75.0  Normal

FAN Speed(RPM)  Current   Max   Min  Threshold  Status
--------------  -------  ----  ----  ---------  ------
          FAN1     7356  7769  6569       3000  Normal
          FAN2     6087  6279  6020       3000  Normal
          FAN3     6157  6301  6067       3000  Normal

Voltage(V)  Current    Max    Min  Threshold  Status
----------  -------  -----  -----  ---------  ------
   1.25VIN    1.243  1.256  1.243      +/-6%  Normal
    1.8VIN    1.869  1.880  1.869      +/-6%  Normal
    3.3VIN    3.372  3.398  3.372      +/-6%  Normal
    2.5VIN    2.593  2.593  2.593      +/-6%  Normal
```

The following table describes the labels in this screen.

Table 147 show hardware-monitor

LABEL	DESCRIPTION
Temperature Unit	This field displays the unit of measure for temperatures in this screen.
Temperature	This field displays the location of the temperature sensors.
Current	This field displays the current temperature at this sensor.
Max	This field displays the maximum temperature measured at this sensor.
Min	This field displays the minimum temperature measured at this sensor.
Threshold	This field displays the upper temperature limit at this sensor.
Status	**Normal:** The current temperature is below the threshold. **Error**: The current temperature is above the threshold.
FAN Speed(RPM)	This field displays the fans in the Switch. Each fan has a sensor that is capable of detecting and reporting when the fan speed falls below the threshold.
Current	This field displays the current speed of the fan at this sensor.
Max	This field displays the maximum speed of the fan measured at this sensor.
Min	This field displays the minimum speed of the fan measured at this sensor. It displays "<41" for speeds too small to measure. (See the User's Guide to find out what speeds are too small to measure in your Switch.)
Threshold	This field displays the minimum speed at which the fan should work.
Status	**Normal**: This fan is running above the minimum speed. **Error**: This fan is running below the minimum speed.
Voltage(V)	This field displays the various power supplies in the Switch. Each power supply has a sensor that is capable of detecting and reporting when the voltage is outside tolerance.

Table 147 show hardware-monitor (continued)

LABEL	DESCRIPTION
Current	This field displays the current voltage at this power supply.
Max	This field displays the maximum voltage measured at this power supply.
Min	This field displays the minimum voltage measured at this power supply.
Threshold	This field displays the percentage tolerance within which the Switch still works.
Status	**Normal**: The current voltage is within tolerance. **Error**: The current voltage is outside tolerance.

This example displays multicast VLAN configuration on the Switch.

```
sysname> show multicast vlan
  Multicast Vlan Status

  Index   VID    Type
  -----   ----   ----------
      1   123    MVR
```

The following table describes the labels in this screen.

Table 148 show multicast vlan

LABEL	DESCRIPTION
Index	This field displays an entry number for the multicast VLAN.
VID	This field displays the multicast VLAN ID.
Type	This field displays what type of multicast VLAN this is. **MVR**: This VLAN is a Multicast VLAN Registration (MVR). **Static**: This VLAN is configured via IGMP snooping VLAN in fixed mode. **Dynamic**: This VLAN is learned dynamically in auto mode. See Chapter 22 on page 91 for more information about IGMP snooping VLAN and IGMP modes.

This example shows the current status of Power over Ethernet.

```
sysname# show poe-status
Total Power (W)          : 185.0
Consuming Power (W)              : 0.0
Allocated Power (W)              : 0.0
Remaining Power (W)              : 185.0
```

The following table describes the labels in this screen.

Table 149 show poe-status

LABEL	DESCRIPTION
Total Power	This field displays the total power the Switch can provide to PoE-enabled devices.
Consuming Power	This field displays the amount of power the Switch is currently supplying to the PoE-enabled devices.

Table 149 show poe-status (continued)

LABEL	DESCRIPTION
Allocated Power	This field displays the total amount of power the Switch has reserved for PoE after negotiating with the PoE device(s).
Remaining Power	This field displays the amount of power the Switch can still provide for PoE. Note: The Switch must have at least 16 W of remaining power in order to supply power to a PoE device, even if the PoE device requested less than 16 W.

This example looks at general system information about the Switch

```
sysname# show system-information

System Name             : ES-2024PWR
System Contact          :
System Location         :
Ethernet Address        : 00:13:49:ae:fb:7a
ZyNOS F/W Version       : V3.80(AII.0)b0 | 04/18/2007
RomRasSize              : 1746416
System up Time          :   280:32:52 (605186d ticks)
Bootbase Version        : V1.00 | 05/17/2006
ZyNOS CODE              : RAS Apr 18 2007 19:59:49
Product Model           : ES-2024PWR
```

The following table describes the labels in this screen.

Table 150 show system-information

LABEL	DESCRIPTION
System Name	This field displays the system name (or hostname) of the Switch.
System Contact	This field displays the name of the person in charge of this Switch. Use the snmp-server command to configure this. See Chapter 52 on page 169.
System Location	This field displays the geographic location of this Switch. Use the snmp-server command to configure this. See Chapter 52 on page 169.
Ethernet Address	This field displays the MAC address of the Switch.
ZyNOS F/W Version	This field displays the firmware version the Switch is running.
RomRasSize	This field displays how much ROM is used.
System up Time	This field displays how long the switch has been running since it last started up.
Bootbase Version	This field displays the bootbase version the Switch is using.
ZyNOS CODE	This field displays the ZyNOS operating system version the Switch is using.
Product Model	This field displays the model name.

This example runs an internal loopback test on ports 3-6.

```
sysname# test interface port-channel 3-6
Testing internal loopback on port 3 :Passed!
  Ethernet Port 3 Test ok.
Testing internal loopback on port 4 :Passed!
  Ethernet Port 4 Test ok.
Testing internal loopback on port 5 :Passed!
  Ethernet Port 5 Test ok.
Testing internal loopback on port 6 :Passed!
  Ethernet Port 6 Test ok.
```

This example displays route information to an Ethernet device with IP address `192.168.1.100`.

```
sysname> traceroute 192.168.1.100
traceroute to 192.168.1.100, 30 hops max, 40 byte packet
  1:192.168.1.100 (10 ms) (10 ms) (0 ms)
traceroute done:
sysname>
```

PART VI
Appendices and Index of Commands

A

Default Values

Some commands, particularly `no` commands, reset settings to their default values. The following table identifies the default values for these settings.

Table 151 Default Values for Reset Commands

COMMAND	DEFAULT VALUE
`no aaa authentication enable`	Method 1: enable Method 2: none Method 3: none
`no aaa authentication login`	Method 1: local Method 2: none Method 3: none
`no aaa accounting update`	0 minutes
`no arp inspection filter-aging-time`	300 seconds
`no arp inspection log-buffer entries`	32 messages
`no arp inspection log-buffer logs`	5 syslog messages 1 second
`no radius-server <index>`	IP address: 0.0.0.0 Port number: 1812 Key: blank
`no radius-accounting <index>`	IP address: 0.0.0.0 Port number: 1813 Key: blank

B

Legal Information

Copyright

Disclaimer

ZyXEL does not assume any liability arising out of the application or use of any products, or software described herein. Neither does it convey any license under its patent rights nor the patent rights of others. ZyXEL further reserves the right to make changes in any products described herein without notice. This publication is subject to change without notice.

Trademarks

ZyNOS (ZyXEL Network Operating System) is a registered trademark of ZyXEL Communications, Inc. Other trademarks mentioned in this publication are used for identification purposes only and may be properties of their respective owners.

Certifications

Federal Communications Commission (FCC) Interference Statement

This device complies with Part 15 of FCC rules. Operation is subject to the following two conditions:

- This device may not cause harmful interference.
- This device must accept any interference received, including interference that may cause undesired operations.

FCC Warning

This device has been tested and found to comply with the limits for a Class A digital switch, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a commercial environment. This device 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 device 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.

CE Mark Warning:

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 BSMI (Bureau of Standards, Metrology and Inspection) A Warning:

警告使用者
這是甲類的資訊產品，在居住的環境使用時，
可能造成射頻干擾，在這種情況下，
使用者會被要求採取某些適當的對策.

Notices

Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

This Class A digital apparatus complies with Canadian ICES-003.

Cet appareil numérique de la classe A est conforme à la norme NMB-003 du Canada.

CLASS 1 LASER PRODUCT

APPAREIL A LASER DE CLASS 1

PRODUCT COMPLIES WITH 21 CFR 1040.10 AND 1040.11.

PRODUIT CONFORME SELON 21 CFR 1040.10 ET 1040.11.

Viewing Certifications

1. Go to http://www.zyxel.com.
2. Select your product on the ZyXEL home page to go to that product's page.
3. Select the certification you wish to view from this page.

ZyXEL Limited Warranty

ZyXEL warrants to the original end user (purchaser) that this product is free from any defects in materials or workmanship for a period of up to two years from the date of purchase. During the warranty period, and upon proof of purchase, should the product have indications of failure due to faulty workmanship and/or materials, ZyXEL will, at its discretion, repair or replace the defective products or components without charge for either parts or labor, and to whatever extent it shall deem necessary to restore the product or components to proper operating

condition. Any replacement will consist of a new or re-manufactured functionally equivalent product of equal or higher value, and will be solely at the discretion of ZyXEL. This warranty shall not apply if the product has been modified, misused, tampered with, damaged by an act of God, or subjected to abnormal working conditions.

Note

Repair or replacement, as provided under this warranty, is the exclusive remedy of the purchaser. This warranty is in lieu of all other warranties, express or implied, including any implied warranty of merchantability or fitness for a particular use or purpose. ZyXEL shall in no event be held liable for indirect or consequential damages of any kind to the purchaser.

To obtain the services of this warranty, contact ZyXEL's Service Center for your Return Material Authorization number (RMA). Products must be returned Postage Prepaid. It is recommended that the unit be insured when shipped. Any returned products without proof of purchase or those with an out-dated warranty will be repaired or replaced (at the discretion of ZyXEL) and the customer will be billed for parts and labor. All repaired or replaced products will be shipped by ZyXEL to the corresponding return address, Postage Paid. This warranty gives you specific legal rights, and you may also have other rights that vary from country to country.

Registration

Register your product online to receive e-mail notices of firmware upgrades and information at www.zyxel.com for global products, or at www.us.zyxel.com for North American products.

C

Customer Support

Please have the following information ready when you contact customer support.

Required Information

- Product model and serial number.
- Warranty Information.
- Date that you received your device.
- Brief description of the problem and the steps you took to solve it.

"+" is the (prefix) number you dial to make an international telephone call.

Corporate Headquarters (Worldwide)

- Support E-mail: support@zyxel.com.tw
- Sales E-mail: sales@zyxel.com.tw
- Telephone: +886-3-578-3942
- Fax: +886-3-578-2439
- Web: www.zyxel.com, www.europe.zyxel.com
- FTP: ftp.zyxel.com, ftp.europe.zyxel.com
- Regular Mail: ZyXEL Communications Corp., 6 Innovation Road II, Science Park, Hsinchu 300, Taiwan

Costa Rica

- Support E-mail: soporte@zyxel.co.cr
- Sales E-mail: sales@zyxel.co.cr
- Telephone: +506-2017878
- Fax: +506-2015098
- Web: www.zyxel.co.cr
- FTP: ftp.zyxel.co.cr
- Regular Mail: ZyXEL Costa Rica, Plaza Roble Escazú, Etapa El Patio, Tercer Piso, San José, Costa Rica

Czech Republic

- E-mail: info@cz.zyxel.com
- Telephone: +420-241-091-350
- Fax: +420-241-091-359
- Web: www.zyxel.cz

- Regular Mail: ZyXEL Communications, Czech s.r.o., Modranská 621, 143 01 Praha 4 - Modrany, Ceská Republika

Denmark

- Support E-mail: support@zyxel.dk
- Sales E-mail: sales@zyxel.dk
- Telephone: +45-39-55-07-00
- Fax: +45-39-55-07-07
- Web: www.zyxel.dk
- Regular Mail: ZyXEL Communications A/S, Columbusvej, 2860 Soeborg, Denmark

Finland

- Support E-mail: support@zyxel.fi
- Sales E-mail: sales@zyxel.fi
- Telephone: +358-9-4780-8411
- Fax: +358-9-4780-8448
- Web: www.zyxel.fi
- Regular Mail: ZyXEL Communications Oy, Malminkaari 10, 00700 Helsinki, Finland

France

- E-mail: info@zyxel.fr
- Telephone: +33-4-72-52-97-97
- Fax: +33-4-72-52-19-20
- Web: www.zyxel.fr
- Regular Mail: ZyXEL France, 1 rue des Vergers, Bat. 1 / C, 69760 Limonest, France

Germany

- Support E-mail: support@zyxel.de
- Sales E-mail: sales@zyxel.de
- Telephone: +49-2405-6909-69
- Fax: +49-2405-6909-99
- Web: www.zyxel.de
- Regular Mail: ZyXEL Deutschland GmbH., Adenauerstr. 20/A2 D-52146, Wuerselen, Germany

Hungary

- Support E-mail: support@zyxel.hu
- Sales E-mail: info@zyxel.hu
- Telephone: +36-1-3361649
- Fax: +36-1-3259100
- Web: www.zyxel.hu
- Regular Mail: ZyXEL Hungary, 48, Zoldlomb Str., H-1025, Budapest, Hungary

India

- Support E-mail: support@zyxel.in
- Sales E-mail: sales@zyxel.in
- Telephone: +91-11-30888144 to +91-11-30888153
- Fax: +91-11-30888149, +91-11-26810715
- Web: http://www.zyxel.in
- Regular Mail: India - ZyXEL Technology India Pvt Ltd., II-Floor, F2/9 Okhla Phase -1, New Delhi 110020, India

Japan

- Support E-mail: support@zyxel.co.jp
- Sales E-mail: zyp@zyxel.co.jp
- Telephone: +81-3-6847-3700
- Fax: +81-3-6847-3705
- Web: www.zyxel.co.jp
- Regular Mail: ZyXEL Japan, 3F, Office T&U, 1-10-10 Higashi-Gotanda, Shinagawa-ku, Tokyo 141-0022, Japan

Kazakhstan

- Support: http://zyxel.kz/support
- Sales E-mail: sales@zyxel.kz
- Telephone: +7-3272-590-698
- Fax: +7-3272-590-689
- Web: www.zyxel.kz
- Regular Mail: ZyXEL Kazakhstan, 43 Dostyk Ave., Office 414, Dostyk Business Centre, 050010 Almaty, Republic of Kazakhstan

Malaysia

- Support E-mail: support@zyxel.com.my
- Sales E-mail: sales@zyxel.com.my
- Telephone: +603-8076-9933
- Fax: +603-8076-9833
- Web: http://www.zyxel.com.my
- Regular Mail: ZyXEL Malaysia Sdn Bhd., 1-02 & 1-03, Jalan Kenari 17F, Bandar Puchong Jaya, 47100 Puchong, Selangor Darul Ehsan, Malaysia

North America

- Support E-mail: support@zyxel.com
- Sales E-mail: sales@zyxel.com
- Telephone: +1-800-255-4101, +1-714-632-0882
- Fax: +1-714-632-0858
- Web: www.us.zyxel.com
- FTP: ftp.us.zyxel.com

- Regular Mail: ZyXEL Communications Inc., 1130 N. Miller St., Anaheim, CA 92806-2001, U.S.A.

Norway

- Support E-mail: support@zyxel.no
- Sales E-mail: sales@zyxel.no
- Telephone: +47-22-80-61-80
- Fax: +47-22-80-61-81
- Web: www.zyxel.no
- Regular Mail: ZyXEL Communications A/S, Nils Hansens vei 13, 0667 Oslo, Norway

Poland

- E-mail: info@pl.zyxel.com
- Telephone: +48-22-333 8250
- Fax: +48-22-333 8251
- Web: www.pl.zyxel.com
- Regular Mail: ZyXEL Communications, ul. Okrzei 1A, 03-715 Warszawa, Poland

Russia

- Support: http://zyxel.ru/support
- Sales E-mail: sales@zyxel.ru
- Telephone: +7-095-542-89-29
- Fax: +7-095-542-89-25
- Web: www.zyxel.ru
- Regular Mail: ZyXEL Russia, Ostrovityanova 37a Str., Moscow 117279, Russia

Singapore

- Support E-mail: support@zyxel.com.sg
- Sales E-mail: sales@zyxel.com.sg
- Telephone: +65-6899-6678
- Fax: +65-6899-8887
- Web: http://www.zyxel.com.sg
- Regular Mail: ZyXEL Singapore Pte Ltd., No. 2 International Business Park, The Strategy #03-28, Singapore 609930

Spain

- Support E-mail: support@zyxel.es
- Sales E-mail: sales@zyxel.es
- Telephone: +34-902-195-420
- Fax: +34-913-005-345
- Web: www.zyxel.es
- Regular Mail: ZyXEL Communications, Arte, 21 5ª planta, 28033 Madrid, Spain

Sweden

- Support E-mail: support@zyxel.se
- Sales E-mail: sales@zyxel.se
- Telephone: +46-31-744-7700
- Fax: +46-31-744-7701
- Web: www.zyxel.se
- Regular Mail: ZyXEL Communications A/S, Sjöporten 4, 41764 Göteborg, Sweden

Thailand

- Support E-mail: support@zyxel.co.th
- Sales E-mail: sales@zyxel.co.th
- Telephone: +662-831-5315
- Fax: +662-831-5395
- Web: http://www.zyxel.co.th
- Regular Mail: ZyXEL Thailand Co., Ltd., 1/1 Moo 2, Ratchaphruk Road, Bangrak-Noi, Muang, Nonthaburi 11000, Thailand.

Ukraine

- Support E-mail: support@ua.zyxel.com
- Sales E-mail: sales@ua.zyxel.com
- Telephone: +380-44-247-69-78
- Fax: +380-44-494-49-32
- Web: www.ua.zyxel.com
- Regular Mail: ZyXEL Ukraine, 13, Pimonenko Str., Kiev 04050, Ukraine

United Kingdom

- Support E-mail: support@zyxel.co.uk
- Sales E-mail: sales@zyxel.co.uk
- Telephone: +44-1344-303044, 08707-555779 (UK only)
- Fax: +44-1344-303034
- Web: www.zyxel.co.uk
- FTP: ftp.zyxel.co.uk
- Regular Mail: ZyXEL Communications UK Ltd., 11 The Courtyard, Eastern Road, Bracknell, Berkshire RG12 2XB, United Kingdom (UK)

Index of Commands

Use of undocumented commands or misconfiguration can damage the unit and possibly render it unusable.