ZYXEL
NETWORKS

CLI Reference Guide

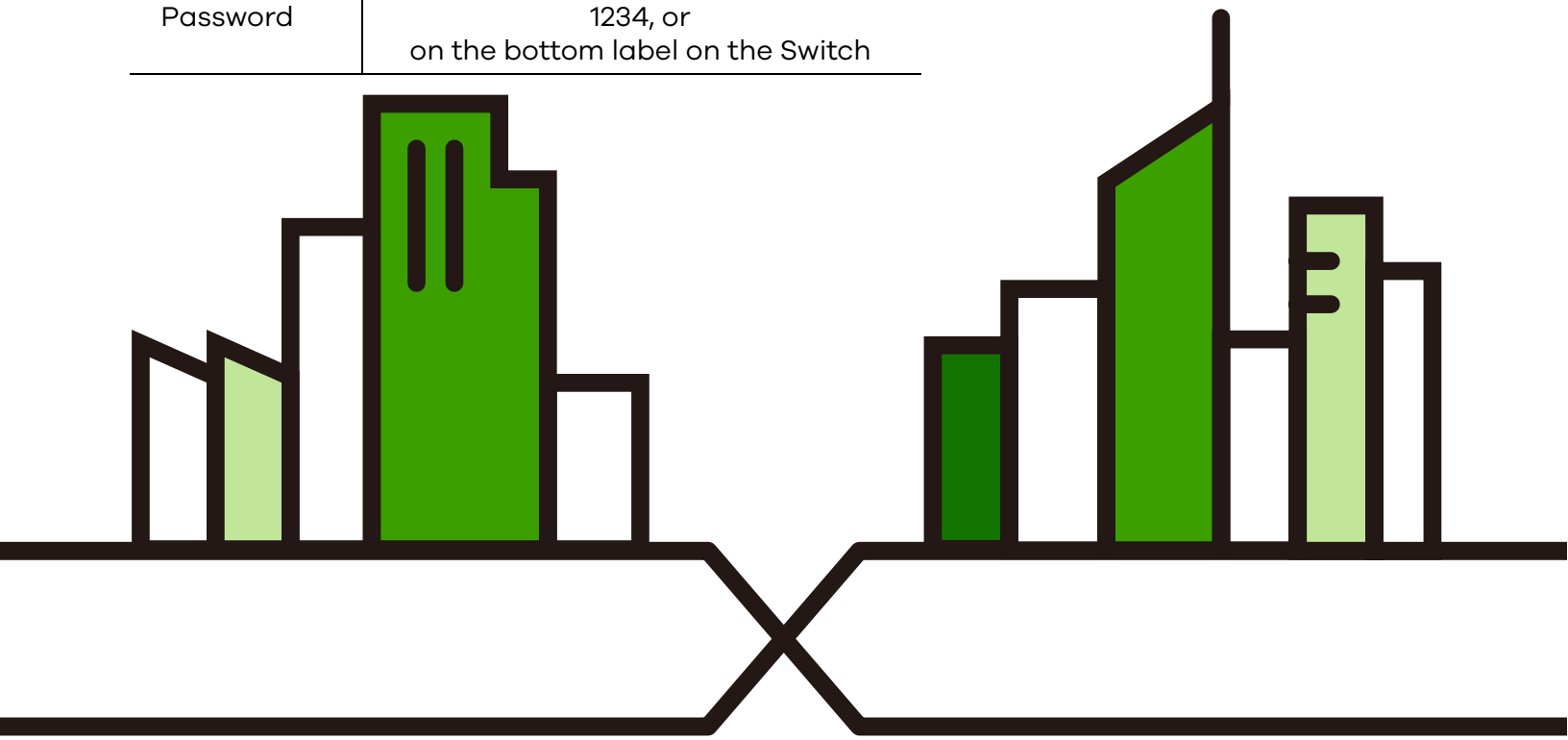
Ethernet Switch Series

Managed Ethernet Switches

FaOS Version 1.00 / ZyNOS Version 4.80–5.00 Edition 1, 12/2024

Default Login Details

Out-of-Band MGMT Port	https://192.168.0.1
In-Band Ports	https://setup.zyxel https://DHCP-assigned IP, or https://192.168.1.1
User Name	admin
Password	1234, or on the bottom label on the Switch



Copyright © 2024 Zyxel and/or its affiliates. All Rights Reserved.

IMPORTANT!
READ CAREFULLY BEFORE USE.
KEEP THIS GUIDE FOR FUTURE REFERENCE.

This is a Reference Guide for a series of products intended for people who want to configure the Switch through Command Line Interface (CLI).

Note: Every effort has been made to ensure that the information in this guide is accurate.

How To Use This Guide

1 Read Chapter 1 on page 10 for how to access and use the CLI (Command Line Interface).

2 Read Chapter 3 on page 18 to learn about the CLI user and privilege modes.

Do not use commands not documented in this guide.

Related Documentation

- Quick Start Guide

  The Quick Start Guide shows how to connect the Switch and access the Web Configurator.

- User's Guide

  The User's Guide explains how to use the Web Configurator to configure the Switch.

Note: It is recommended you use the Web Configurator to configure the Switch.

- Nebula Control Center (NCC) Online Help

  Go to *https://nebula.zyxel.com/cc/ui/index.html#/help* to see how to manage the Switch remotely through Nebula Control Center.

- More Information

  Go to *support.zyxel.com* to find other information on the Switch.

About This CLI Reference Guide

Intended Audience

This manual is intended for people who want to configure Zyxel Switches through Command Line Interface (CLI).

The version number on the cover page refers to the latest firmware version supported by the Zyxel Switches. This guide applies to FaOS 1.00, ZyNOS 5.00, ZyNOS 4.90 and ZyNOS 4.80 at the time of writing.

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.

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.

Note: 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 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.
- In some commands you specify slots or interfaces by the Access ID <aid>, use "?" to show which types of interfaces you can specify. For example, you might be able to use: `slot-<slot> | <ge|msc>-<slot>-<port> | <ge|msc>-<slot>-<port>&&-<port>`.
  - Use "`msc-<slot>-<port>`" for an uplink slot on the management switch card.
  - Use "`ge-<slot>-<port>`" for a Gigabit Ethernet port or switch settings on a PON interface.
  - Use "`pon-<slot>-<port>`" to configure PON interface settings.
  - A "slot" is a chassis slot.
  - The "port" is 1-N where N is the number of ports on the card.
  - Use && to specify a range of ports.
- 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 3 on page 18 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 do not have a high enough privilege level you may not be able to view or execute some of the commands. See Chapter 3 on page 18 for more information on privilege levels.

Contents Overview

PART I
Introduction

CHAPTER 1
Introduction

1.1 Overview

This command line interface (CLI) Reference Guide introduces the command line interface of the Switch. Use the listed commands in this Guide to check the Switch status and/or configure the Switch.

Note: 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* for product specific User Guides and product certifications.

At the time of writing, this Guide includes the following FaOS 1.00, ZyNOS 5.00, ZyNOS 4.90 and ZyNOS 4.80 Switches.

Table 2 FaOS 1.00 Switch

SERIES	MODELS	ADDITIONAL LICENSE	SWITCH TYPE	CLI SUPPORT
CX4800-56F	CX4800-56F	No available license	Layer-3	CLI full configuration in Standalone mode and Cloud mode.

Table 3 ZyNOS 5.00 Switches

SERIES	MODELS	ADDITIONAL LICENSE	SWITCH TYPE	CLI SUPPORT
GS2220 Series	GS2220-10/10HP/28/ 28HP/50/50HP	No available license	Layer-2	CLI full configuration in Standalone mode and Cloud mode.

Table 4 ZyNOS 4.90 Switch

SERIES	MODELS	ADDITIONAL LICENSE	SWITCH TYPE	CLI SUPPORT
GS1350 Series	GS1350-6HP/12HP/ 18HP/26HP	No available license	Layer-2	CLI full configuration in Standalone mode and Cloud mode.

Table 5 ZyNOS 4.80 Switches

SERIES	MODELS	ADDITIONAL LICENSE	SWITCH TYPE	CLI SUPPORT
GS2220 Series	GS2220-10/10HP/28/ 28HP/50/50HP	No available license	Layer-2	CLI full configuration in Standalone mode and Cloud mode.
XGS2220 Series	XGS2220-30/30HP/30F/ 54/54HP/54FP		Layer-3	

Table 5 ZyNOS 4.80 Switches (continued)

SERIES	MODELS	ADDITIONAL LICENSE	SWITCH TYPE	CLI SUPPORT
XMG1930 Series	XMG1930-30/HP	Access L3 License	Layer-3	CLI basic status checking. Requires licenses to unlock CLI full configuration in Standalone mode and Cloud mode.
XS1930 Series	XS1930-10/12HP/12F			
XS3800-28	XS3800-28	Basic Routing License	Layer-3	CLI full configuration in Standalone mode and Cloud mode.

Some Switches require licenses to unlock additional licensed services. See Section 1.1.1 on page 11 for more information.

1.1.1 License Option

At the time of writing, the following Switch licenses unlock the below services as shown in the table. The licenses are valid for the lifetime of the Switch.

You can register your Switch and manage the Switch licenses at *www.myzyxel.com*. See Section 79.1 on page 316 for the license registration information.

Note: See your Switch's datasheet for the default feature specification.

Table 6 Switch License Comparison

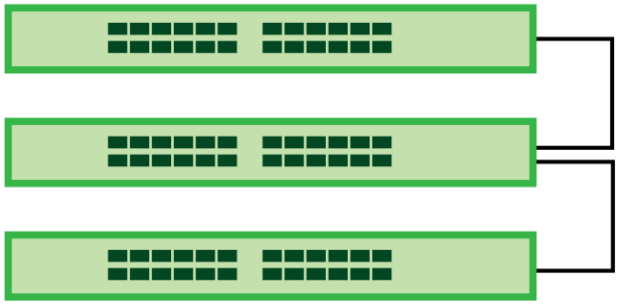
LICENSE NAME	MODEL/SERIES	LICENSED SERVICES
Basic Routing License	XS3800-28	• RIPv1,v2 • OSPF v2 • DVMRP • IGMP • L3 Loopback Interface Note: XS3800-28 supports all Access L3 License features by default.
Access L3 License	XMG1930 Series XS1930 Series	• CLI (Command Line Interface) configuration Note: This management method is supported using the console port (XMG1930 only), telnet or SSH. • IP Address table (up to 1,024 entries) • MAC Address table (up to 32,000 entries) • SNMP (Simple Network Management Protocol) Trap • Private MIB (Management Information Base) • Auto PD (powered device) Recovery • Flex Link (primary/backup link) • OAM (Operations, Administration and Maintenance) • Asymmetric Flow Control • BPDU (Bridge Protocol Data Units) Control • ZULD (Zyxel Unidirectional Link Detection) • MAC Pinning • IGMP Snooping Smart Forward • IPv6 Multicast • MLD Snooping Proxy • MVR (Multicast VLAN Registration) configuration • Diffserv (Differentiated Services) • sFlow (sampled Flow) agent • MRSTP (Multiple Rapid Spanning Tree Protocol) • Subnet / Protocol / MAC Based VLANs • 802.1Q Static VLANs (up to 4,094 entries) • VLAN Isolation / Mapping / Stacking • Selective QinQ • DHCP Server Guard • IPv4 Static Route (up to 64 entries) • IPv6 Static Route (up to 64 entries) • Multiple TACACS+ (Terminal Access Controller Access Control System) Server • TACACS+ Authentication • TACACS+ Accounting • IPv4 Classifier (up to 256 entries) • Policy Rule (up to 384 entries) • Anti-Arpscan (Address Resolution Protocol scan) • BPDU (Bridge Protocol Data Units) Guard • Errdisable (Error-Disable) • IPv4 / IPv6 Source Guard • ARP (Address Resolution Protocol) Freeze • ARP Inspection • MAC Authentication per VLAN • Compound Authentication • MAC Freeze • Auto Configuration file download • DHCP Client Option 60 • Networked AV Mode • IPv6 NS (Neighbor Solicitation) Tracking • CLV Mode

If your Switch needs to be replaced due to certain causes, contact our support team for the license transfer process.

1.2 Stacking Mode

The Switch can work in Stacking mode and directly connect to other switches. The switches then operate together and act as a single switch or a virtual chassis. The stackable switches can be managed from a master switch in the stack. See Section 82.1 on page 327 for more information about stacking and the stacking commands.

Figure 1 Stacking Example



The following Switches support stacking at the time of writing.

Table 7 Switch Models that Support Stacking

SERIES/MODELS	MAXIMUM SWITCHES ALLOWED PER STACK
XGS2220 Series	4
XS3800-28	4

1.3 Switch-specific Features

The following features and commands are only supported by certain Switches.

Table 8 Switch-specific Features

FEATURE/COMMAND	SUPPORTED MODEL/SERIES	QUICK LINKS
Fiber Module Rescue	XGS2220/XMG1930/XS1930 Series	*reset sfp <port-list>*
Green Ethernet – EEE	GS1350/GS2220/XGS2220/ XMG1930/XS1930 Series XS3800-28	*green-ethernet eee*
Green Ethernet – Auto Power Down	GS1350/GS2220/XGS2220/ XMG1930/XS1930 Series XS3800-28	*green-ethernet auto-power-down*
Green Ethernet – Short Reach	GS1350/GS2220/XGS2220/ XMG1930/XS1930 Series XS3800-28	*green-ethernet short-reach*
Trunk Non-unicast Traffic Criteria Settings	CX4800-56F/XS3800-28	*trunk non-unicast criteria <src|dst|port|src-mac|dst-mac|src-ip|dst-ip>*
Hardware Monitor Commands	GS1350/GS2220/XGS2220/ XMG1930/XS1930 Series CX4800-56F/XS3800-28	*Hardware Monitor Commands Overview*

Table 8 Switch-specific Features (continued)

FEATURE/COMMAND	SUPPORTED MODEL/SERIES	QUICK LINKS
CLV Commands	GS2220/XGS2220 Series XMG1930/XS1930 Series with Access L3 license CX4800-56F/XS3800-28	*CLV Overview*
4-Port and 2-Port Stacking Modes	XGS2220 Series	*stacking port-mode <2-ports | 4-ports>*
Remote Management Commands (IPv6)	GS1350/GS2220 Series	*show remote-management6 [index]* *remote-management6 <index> start-addr <ipv6> end-addr <ipv6> service <[telnet] [ftp] [http] [icmp] [snmp] [ssh] [https]>*
Redirect to a secure web browser page, from HTTP to HTTPS	GS1350/GS2220 Series CX4800-56F	*service-control http redirect-to-https*
Login user name	GS1350/GS2220 Series CX4800-56F	*admin-username <name>*
Change the Default Login Password	GS2220 Series	*Change the Default Login Password*
Password Complexity	GS2220 Series	*password complexity*
SNMP User Password Encryption	GS2220 Series	*password encryption*
Lock the IP Address	GS2220 Series	*logins lockout block-period* *logins lockout retry-count* *logins lockout attempt-timeout*
SSH Authorized Keys Commands	GS1350/GS2220 Series CX4800-56F	*show ssh authorized-keys* *import ssh <username> authorized-keys <key-string>* *clear ssh authorized-keys* *clear ssh known-hosts*
Regenerate SSH Host Key	GS2220 Series	*ssh regen-key rsa*
IGMP Snooping Querier Query Interval	GS2220 Series CX4800-56F	*igmp-snooping querier query-interval <1-65535>*
SNMP sends system trap when log entries reach 90%	GS2220 Series	*snmp-server trap-destination <ip> enable traps system system-log*
3 Time Sync Servers Setup	GS2220 Series CX4800-56F	*timesync server <time-server1> [<time-server2> [<time-server3>]]*

CHAPTER 2
Command Line Interface

2.1 CLI Overview

The command line interface provides a management interface where you can check the Switch status, interface statistics, and configure the Switch settings. The CLI is also helpful when you want to troubleshoot your configuration on the Switch.

2.2 Accessing the CLI

Use any of the following methods to access the CLI.

2.2.1 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 9 Default Settings for the Console Port

SETTING	DEFAULT VALUE
Terminal Emulation	VT100
Baud Rate	115200 bps
Parity	None
Number of Data Bits	8
Number of Stop Bits	1
Flow Control	None

3 Press [ENTER] to open the login screen.

2.2.2 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 10 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.

2.2.3 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 10 on page 16 and Table 11 on page 16. Make sure your computer IP address is in the same subnet, unless you are accessing the Switch through one or more routers.

2.3 Logging in

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

Table 11 Default User Name and Password

SETTING	DEFAULT VALUE
User Name	admin
Password	1234

Note: The Switch automatically logs you out of the management interface after 5 minutes of inactivity. If this happens to you, simply log back in again.

Change the Default Login Password

You will be asked to change the default password (**1234**) the first time you log in. The new password rules are:

- 4 to 32 characters in length, and
- [?], [|], ['], ["], [,], [[ ], [ ]] and space are not allowed.

Note: To find the default password on some newer Switch models, see the label on the bottom of the Switch.

2.4 Using Shortcuts and Getting Help

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

Table 12 CLI Shortcuts and Help

COMMAND / KEYS	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, enter `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`.

2.5 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
```

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

2.6 Logging Out

Enter `logout` to log out of the CLI. You have to be in user, enable, or config mode. See Chapter 3 on page 18 for more information about modes.

CHAPTER 3
Privilege Level and Command Mode

3.1 Privilege Level and Command Mode Overview

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.

3.2 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.

3.2.1 Privilege Levels for Commands

The privilege level of each command is listed in the Reference A-G chapters on page 30.

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 13 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, SNMP user accounts, the authentication method sequence and authorization settings, multiple logins, administrator and enable passwords, and configuration information display.
14	Configure login accounts, SNMP user accounts, the authentication method sequence and authorization settings, multiple logins, and administrator and enable passwords, and display configuration information.

3.2.2 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 47 on page 196.
- 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.

3.2.3 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.

3.2.3.1 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 Section 62.2 on page 249 for more information about this command.

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

The password is sent in plain text and stored in the Switch's buffers. Use this command to set the cipher password for password encryption.

`password cipher <password>`

<*password*> consists of 32 alphanumeric characters. For example, the following command encrypts the enable password with a 32-character cipher password. See Section 62.2 on page 249 for more information about this command.

```
sysname(config)# password cipher qwertyuiopasdfghjklzxcvbnm123456
```

3.2.3.2 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 Section 62.2 on page 249 for more information about this command.

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

Note: For ZyNOS 5.00, see password complexity for more information on the number of alphanumeric characters required for <*password*>.

3.2.3.3 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.

3.2.3.4 show privilege command

This command displays the session's current privilege level. This command is available in user mode or enable mode.

```
sysname# show privilege
  Current privilege level : 14
```

3.3 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.

3.3.1 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.

3.3.2 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 14 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-mvr	sysname(config-mvr)#	Configure multicast VLAN.
config-route-domain	sysname(config-if)#	Enable and enter configuration mode for an IPv4 or IPv6 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-ma	sysname(config-ma)#	Configure a Maintenance Association (MA) in Connectivity Fault Management (CFM).
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 15 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

3.4 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 Enter 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 Enter configure and press [ENTER]. This takes you to the config mode.

5 Enter 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.

CHAPTER 4
Initial Setup

4.1 Initial Setup Overview

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

4.2 Changing the Administrator Password

Note: It is recommended you change the default administrator password. You can encrypt the password using the password encryption command. See Chapter 62 on page 248 for more information.

Use this command to change the administrator password.

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

Up to 32 characters are allowed for the new password except [?], [|], ['], ["], [space], or [,].

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

Note: For ZyNOS 5.00, see password complexity for more information on the number of alphanumeric characters required for <*password*>.

4.3 Changing the Enable Password

Note: It is recommended you change the default enable password. You can encrypt the password using the password encryption command. See Chapter 62 on page 248 for more information.

Use this command to change the enable password.

password <*password*>

Up to 32 characters are allowed for the new password except [?], [|], ['], ["], [space], or [,].

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

Note: For ZyNOS 5.00, see password complexity for more information on the number of alphanumeric characters required for <*password*>.

4.4 Prohibiting Concurrent Logins

By default, multiple CLI sessions are allowed through 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 57 on page 224 for more `multi-login` commands.

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

4.5 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 default-management 172.16.0.1 255.255.255.0
```

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

4.6 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 through 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
```

4.7 Using Auto Configuration

Follow the steps below to set up configurations on the Switch, so you can load an auto configuration file automatically from a TFTP server when you reboot the Switch.

Note: You need to set up configurations on a DHCP server and TFTP server first to use auto configuration.

1 Use this command to enable auto configuration on the Switch.
`auto-config`

```
sysname# config
sysname(config)# auto-config
```

2 Use this command to enable the DHCP mode for auto configuration.
`auto-config dhcp`

```
sysname# config
sysname(config)# auto-config dhcp
```

3 Use this command to configure the Switch as a DHCP client.
`ip address default-management dhcp-bootp`

```
sysname# config
sysname(config)# vlan 1
sysname(config-vlan)# ip address default-management dhcp-bootp
```

4 Use this command to enable DHCP option 60.
`ip address default-management dhcp-bootp option-60`

When you enable DHCP option 60, make sure you set up a Vendor Class Identifier. The Vendor Class Identifier specifies the Zyxel Switch that should receive the auto configuration file.
Skip this step if you are not enabling DHCP option 60.

```
sysname# config
sysname(config)# vlan 1
sysname(config-vlan)# ip address default-management dhcp-bootp option-60
```

5 Use this command to define a Vendor Class Identifier for DHCP option 60.
`ip address default-management dhcp-bootp option-60 class-id <class-id>`

In this example, we use "ZyxelCorp".
Skip this step if you do not need to define a Vendor Class Identifier.

```
sysname# config
sysname(config)# vlan 1
sysname(config-vlan)# ip address default-management dhcp-bootp option-60
class-id ZyxelCorp
```

6 Use this command to check the settings for auto configuration.
`show running-config`

```
GS1350# show running-config
  Building configuration...

  Current configuration:

; Product Name = GS1350-26HP
; Firmware Version = V4.90(ABPL.0)b3 | 11/06/2023
no service-control telnet
no service-control snmp
no cloud center discovery
vlan 1
  name 1
  normal ""
  fixed 1-26
  forbidden ""
  untagged 1-26
  ip address default-management dhcp-bootp
exit
interface vlan 1
  ipv6
  ipv6 address autoconfig
  ipv6 address dhcp client ia-na
exit
timesync server 1.pool.ntp.org
timesync ntp
service-control http 80 55
pwr mode consumption
```

7 You need to save the current configuration in a configuration file, so the Switch will load the auto configuration files from the TFTP server automatically when rebooting.
Use this command to save the current configuration in a configuration file.
`write memory [<index>]`
For [<*index*>], you can enter a value to save the current configuration to a specified configuration file. 1 is for Config 1, and 2 is for Config 2.

In this example, we save the current configuration to Config 1.

```
sysname# write memory 1
.....................................................................
.........................
```

8 Use this command to reboot the Switch.
`reload config [1|2]`
For [1|2], 1 is for Config 1, and 2 is for Config 2.

In this example, we load Config 1 to reboot the Switch.

```
sysname# reload config 1
Do you really want to reboot system with configuration file 1? [y/N]y
Bootbase Version: V1.00 | 11/22/2023
DRAM calibration...PASSED
RAM: Size = 131072 Kbytes

ZyNOS version : V4.90(ABPL.0) | 11/22/2023

Press any key to enter debug mode within 1 second.
.....................
     (Compressed)
     Version: GS1350, start: b4962430
     Length: 16F0668, Checksum: 03AA
     Compressed Length: 2EE424, Checksum: 87A5
Copyright (c) 1994 - 2023 Zyxel Communications Corp.
initialize mgmt, initialize switch, ethernet address: 00:19:cb:00:00:01
Initializing MSTP.............
Initializing VLAN Database...
Initializing IP Interface...
Initializing Advanced Applications...
Initializing Command Line Interface...
Initializing Web Interface...
Restore System Configuration...
Start Auto Configuration...
..............
Try to download and restore configuration file from TFTP://10.90.90.11/
TestConf2
Downloading....
Get the file TestConf2, length 289 bytes.
Restoring......
Auto-config processes successfully.
Press ENTER to continue...
```

9 Use this command to check whether the auto configuration file was loaded successfully.
`Show auto-config`

```
Mode: DHCP
State: Success
Filename: TFTP://10.90.90.11/TestConf2
```

4.8 Using Custom Default

Follow the steps below to set up configurations on the Switch, so you can load a customized default file when you reboot the Switch.

1 Use this command to enable custom default on the Switch.
`custom-default`

```
sysname# config
sysname(config)# custom-default
```

2 Use this command to save the current configuration settings permanently to a customized default file on the Switch.
`copy running-config custom-default`

```
sysname# copy running-config custom-default
.....................................................................
.........................
```

3 Use this command to reboot the system and load a saved customized default file on the Switch.
`reload custom-default`

```
sysname# reload custom-default
Do you really want to restore system to custom default settings and
reboot?[y/N]y
.......

Bootbase Version: V1.00 | 11/22/2023
DRAM calibration...PASSED
RAM: Size = 131072 Kbytes
ZyNOS Version: V4.90(ABPL.0) | 11/22/2023

Press any key to enter debug mode within 1 second.
.................
     (Compressed)
     Version: GS1350, start: b4962430
     Length: 16F0668, Checksum: 03AA
     Compressed Length: 2EE424, Checksum: 87A5
Copyright (c) 1994 - 2023 Zyxel Communications Corp.
initialize mgmt, initialize switch, ethernet address: 00:19:cb:00:00:01
Initializing MSTP.............
Initializing VLAN Database...
Initializing IP Interface...
Initializing Advanced Applications...
Initializing Command Line Interface...
Initializing Web Interface...
Restore System Configuration...
Press ENTER to continue...
```

4.9 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

Product Model           : GS1350-26HP
System Name             : GS1350
System Mode             : Standalone
System Contact          :
System Location         :
System up Time          :  1011:30:18 (d90bb588 ticks)
Ethernet Address        : b8:ec:a3:ff:f2:a2
Bootbase Version        : V1.00 | 11/22/2023
ZyNOS F/W Version       : V4.90(ABPL.0) | 11/22/2023
Hardware Version        : V1.0
Config Boot Image       : 1
Current Boot Image      : 1
Current Configuration   : 1
RomRasSize              : 6440206
Serial Number           : S222L18090003
Register MAC Address    : b8:ec:a3:ff:f2:a2
sysname#
```

See Table 280 on page 405 for more information about these attributes.

4.10 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 1-52
  forbidden ""
  untagged 1-52
  ip address 192.168.1.1 255.255.255.0
exit
interface route-domain 192.168.1.1/24
exit
pwr mode consumption
```

PART II
Reference A-G

CHAPTER 5
AAA Commands

5.1 Command Summary

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

The following section lists the commands for this feature.

Table 16 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 methods for checking privilege level of administrators.	E	3
aaa authentication enable <*method1*> [<*method2*> ...]	Specifies the first, second, and third method used for checking privileges. *method*: local, 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 17 aaa accounting Command Summary

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
no aaa accounting commands	Disables accounting of command sessions on the Switch.	C	13

Table 17 aaa accounting Command Summary (continued)

COMMAND	DESCRIPTION	M	P
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 through SSH, Telnet or the console port.	E	3
aaa accounting exec <start-stop|stop-only> <radius|tacacs+> [broadcast]	Enables accounting of administrative sessions through SSH, Telnet and console port and specifies the mode and protocol method. Optionally, sends accounting information for administrative sessions through 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 through 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

Table 18 aaa authorization Command Summary

COMMAND	DESCRIPTION	M	P
show aaa authorization	Displays authorization settings configured on the Switch.	E	3
show aaa authorization dot1x	Displays the authorization method used to allow an IEEE 802.1x client to have different bandwidth limit or VLAN ID assigned through the external server.	E	3
show aaa authorization exec	Displays the authorization method used to allow an administrator which logs in the Switch through Telnet or SSH to have different access privilege level assigned through the external server.	E	3
aaa authorization console	Enables authorization of allowing an administrator which logs in the Switch through the console port to have different access privilege level assigned through the external server.	C	14
aaa authorization dot1x radius	Enables authorization for IEEE 802.1x clients using RADIUS.	C	14
aaa authorization exec <radius|tacacs+>	Specifies which method (radius or tacacs+) should be used for administrator authorization.	C	14
no aaa authorization console	Disables authorization of allowing an administrator which logs in the Switch through the console port to have different access privilege level assigned through the external server.	C	14

Table 18 aaa authorization Command Summary (continued)

COMMAND	DESCRIPTION	M	P
no aaa authorization dot1x	Disables authorization for IEEE 802.1x clients using RADIUS.	C	14
no aaa authorization exec	Disables authorization of allowing an administrator which logs in the Switch through Telnet or SSH to have different access privilege level assigned through the external server.	C	14

Table 19 aaa encryption Command Summary

COMMAND	DESCRIPTION	M	P
aaa server key encryption	Enables AAA server key encryption. The Switch will store server (RADIUS, TACACS+) keys you set in an encrypted format instead of plain text to enhance key security. The encrypted secret (key) will be preceded by the word "key-cipher" in the configuration file (called running-config)." Note: If a key is encrypted, it will remain in the encrypted format even if you later disable server key encryption.	C	14
no aaa server key encryption	Disables AAA server key encryption. The encrypted server key will not be changed back to plain text. Note: Be careful who can access configuration files with plain text keys!	C	14

5.2 Command Example

This example enables AAA server key encryption, and sets the RADIUS server 1 (192.168.1.15) key.

```
sysname# config
sysname(config)# aaa server key encryption
sysname(config)# radius-server host 1 192.168.1.15 key 12345678
sysname(config)# exit
sysname#
```

Use the following command to display the current config. You can see the displayed server key is now encrypted.

```
sysname# show run
  Building configuration...

  Current configuration:

; Product Name = XS3800-28
; Firmware Version = V4.80(ABML.0)b7 | 04/07/2022
.
.
radius-server host 1 192.168.1.10 key-cipher ZJP4wRc/
1eTprnqmowZWs7HDejwjanEb29g24zMH8XSEiKe5kN2b3Hhq7v7kTeXozkJc4dfP2BW
hoKqLB
.
.
password encryption
aaa server key encryption
display aaa authentication authorization server
sysname#
```

CHAPTER 6
Anti-Arpscan

6.1 Anti-Arpscan Overview

Address Resolution Protocol (ARP), RFC 826, is a protocol used to convert a network-layer IP address to a link-layer MAC address. ARP scan is used to scan the network of a certain interface for alive hosts. It shows the IP address and MAC addresses of all hosts found. Hackers could use ARP scan to find targets in your network. Anti-arpscan is used to detect unusual ARP scan activity and block suspicious hosts or ports.

Unusual ARP scan activity is determined by port and host thresholds that you set. A port threshold is determined by the number of packets received per second on the port. If the received packet rate is over the threshold, then the port is put into an Err-Disable state. You can recover the normal state of the port manually if this happens and after you identify the cause of the problem.

A host threshold is determined by the number of ARP-request packets received per second. There is a global threshold rate for all hosts. If the rate of a host is over the threshold, then that host is blocked by using a MAC address filter. A blocked host is released automatically after the MAC aging time expires.

Note: A port-based threshold must be larger than the host-based threshold or the host-based threshold will not work.

6.2 Command Summary

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

Table 20 Interface Command Values

COMMAND	DESCRIPTION
port-list	A list of one or more ports, separated by commas with no spaces. The list may also contain ranges of ports signified by a hyphen. For example: 1,3,5–8,10.

The following section lists the commands for this feature.

Table 21 anti arpscan Command Summary

COMMAND	DESCRIPTION	M	P
`anti arpscan`	Enables Anti-arpscan on the Switch.	C	13
`anti arpscan host threshold <2-100>`	Sets the maximum number of ARP-request packets allowed by a host before it is blocked. If the rate of a host is over the threshold, then that host is blocked by using a MAC address filter. A blocked host is released automatically after the MAC aging time expires.	C	13

Table 21 anti arpscan Command Summary (continued)

COMMAND	DESCRIPTION	M	P
anti arpscan port threshold <2-255>	Sets the maximum number of packets per second allowed on the port before it is blocked.	C	13
anti arpscan trust host <*ip-address*> <*mask*> [name <*name*>]	Creates a trusted host identified by IP address and subnet mask. Anti-arpscan is not performed on trusted hosts.	C	13
clear anti arpscan host	Unblocks all hosts.	E	13
clear anti arpscan host interface port-channel <*port-list*>	Unblocks all hosts connected to the specified ports.	E	13
interface port-channel <*port-list*>	Enters config-interface mode for the specified ports.	C	13
anti arpscan trust	Sets the port as a trusted port. This prevents the port from being shutdown due to receiving too many ARP messages.	C	13
no anti arpscan	Disables Anti-arpscan on the Switch.	C	13
no anti arpscan host threshold	Resets the host threshold to its default value.	C	13
no anti arpscan port threshold	Resets the port threshold to its default value.	C	13
no anti arpscan trust host <*ip-address*> <*mask*>	Removes a trusted host.	C	13
show anti arpscan	Displays what ports are trusted and are forwarding traffic or are disabled.	E	3
show anti arpscan host	Displays the host that has been blocked.	E	3

CHAPTER 7
ARP Commands

7.1 Command Summary

Use these commands to view and configure the ARP table on the Switch. The ARP table contains IP-to-MAC address mappings for network devices connected to the Switch.

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

Table 22 Interface Command Values

COMMAND	DESCRIPTION
port-list	A list of one or more ports, separated by commas with no spaces. The list may also contain ranges of ports signified by a hyphen. For example: 1,3,5–8,10.

The following section lists the commands for this feature.

Table 23 arp Command Summary

COMMAND	DESCRIPTION	M	P
arp aging-time <60-1000000>	Sets how long dynamically learned ARP entries remain in the ARP table before they age out (and must be relearned).	C	13
arp name <*name*> ip <*ip-address*> mac <*mac-addr*> vlan <*vlan-id*> interface port-channel <*port-list*>	Creates a static ARP entry which will not age out.	C	13
arp name <*name*> ip <*ip-address*> mac <*mac-addr*> vlan <*vlan-id*> interface port-channel <*port-list*> inactive	Creates a static ARP entry but disables it.	C	13
no arp ip <*ip-address*> mac <*mac-addr*> vlan <*vlan-id*>	Deletes a static ARP entry from the ARP table.	C	13
no arp ip <*ip-address*> mac <*mac-addr*> vlan <*vlan-id*> inactive	Enables the specified static ARP entry.	C	13
show ip arp	Displays the ARP table.	E	3
show ip arp count	Displays the number of ARP entries in the ARP table.	E	3
clear ip arp	Removes all of the dynamic entries from the ARP table.	E	13
clear ip arp interface port-channel <*port-list*>	Removes the dynamic entries learned on the specified port.	E	13
clear ip arp ip <*ip-address*>	Removes the dynamic entries learned with the specified IP address.	E	13

7.2 Command Examples

This example creates a static ARP entry and shows the ARP table on the Switch.

```
sysname# config
sysname(config)# arp name test ip 192.168.1.99 mac 00:c5:d8:01:23:45 vlan
1 interface port-channel 3
sysname(config)# exit
sysname# show ip arp
  Index   IP              MAC               VLAN  Port    Age(s)  Type
  1       192.168.1.1     00:19:cb:37:00:49  1     CPU     0       static
  2       192.168.1.99    00:c5:d8:01:23:45  1     3       0       static
  3       192.168.2.1     00:19:cb:37:00:49  465   CPU     0       static
sysname#
```

The following table describes the labels in this screen.

Table 24 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.
Port	This field displays the number of the port from which the IP address was learned. **CPU** indicates this IP address is the Switch's management IP address.
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.

CHAPTER 8
ARP Inspection Commands

8.1 ARP Inspection Overview

ARP (Address Resolution Protocol) allows network devices to discover each other's MAC addresses, in order to communicate. For example, Device A wants to send data to Device B, Device A broadcasts an ARP request within its broadcast domain, requesting the MAC address of Device B. Device B replies with an ARP response packet containing its MAC address and IP address.

Malicious devices can take advantage of this process by intercepting ARP requests and broadcasting spoofed ARP responses. For example: Malicious Device C receives the ARP request sent from Device A, and responds with an ARP packet containing its own MAC address and Device B's IP address. Now all traffic meant for Device B is sent to Device C, allowing Device C to perform a man in the middle attack.

ARP Inspection prevents this type of attack, by ensuring the Switch only relays non-malicious ARP responses.

8.1.1 ARP Inspection Process

When ARP Inspection is enabled, the Switch performs the following actions:

1. The Switch intercepts an ARP packet that is being sent through an untrusted port.
2. The Switch verifies the ARP packet is valid, meaning that it contains a correctly formatted data, and drops the packet if it is invalid.
3. The Switch compares the IP-to-MAC-address mapping in the ARP packet to a list of trusted mappings. The trusted list is created automatically by DHCP Snooping, and also contains all static IP Source Binding table entries.

   If the packet's IP-to-MAC-address mapping is not on the trusted list, the Switch drops the packet and then creates a MAC address filter to block all traffic from the source MAC address and from the source VLAN ID of the ARP packet.
4. The Switch optionally logs the event.

Note: You can mark ports as trusted or untrusted. The Switch only inspects ARP packets from untrusted ports. Typically, you should only mark a port as trusted if the port is connected to another switch that also has ARP Inspection enabled.

Note: By default, the Switch performs ARP inspection on all VLANs. However, you can limit ARP inspection to specific VLANs in order to save CPU resources.

8.1.2 ARP Packet Rate Limiting

Inspecting ARP packets consumes the Switch CPU resources. This allows a malicious device to perform a denial-of-service (DoS) attack on the Switch by broadcasting a very high number of ARP packets.

ARP packet rate limiting prevents these types of attacks, by limiting the number of packets per second (PPS) that a port inspects. If this limit is exceeded, the port enters an error state and drops all ARP packets.

8.2 Command Summary

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

Table 25 Interface Command Values

COMMAND	DESCRIPTION
port-list	A list of one or more ports, separated by commas with no spaces. The list may also contain ranges of ports signified by a hyphen. For example: 1,3,5–8,10.

The following section lists the commands for this feature.

Table 26 arp inspection Command Summary

COMMAND	DESCRIPTION	M	P
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
show arp inspection	Displays ARP inspection configuration details.	E	3
clear arp inspection statistics	Removes all ARP inspection statistics on the Switch.	E	3
clear arp inspection statistics vlan <*vlan-list*>	Removes ARP inspection statistics for the specified VLANs.	E	3
show arp inspection statistics	Displays all ARP inspection statistics on the Switch.	E	3
show arp inspection statistics vlan <vlan-list>	Displays ARP inspection statistics for the specified VLANs.	E	3

Table 27 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
clear arp inspection filter	Deletes 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

Table 27 Command Summary: arp inspection filter (continued)

COMMAND	DESCRIPTION	M	P
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 28 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
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 29 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 ports.	E	3
interface port-channel <*port-list*>	Enters config-interface mode for the specified ports.	C	13
arp inspection trust	Sets the ports to be trusted. The Switch does not inspect or discard ARP packets passing through the ports.	C	13
no arp inspection trust	Sets the ports to be untrusted. The Switch inspects all ARP packets passing through the ports.	C	13
arp inspection limit rate <*pps*>	Limits the maximum number of ARP packets per second (pps) the ports accepts. The Switch drops all packets that exceed the limit. The value must be in the range 0 – 2048. The default value is 15.	C	13
arp inspection limit rate <*pps*> burst interval <*seconds*>	Limits the maximum number of ARP packets per second (pps) the interface accepts within the specified time interval. After each burst interval, the pps count is reset.	C	13
no arp inspection limit	Sets no limit on the number of ARP packets per second (pps) the interface accepts.	C	13

Table 30 Command Summary: arp inspection vlan

COMMAND	DESCRIPTION	M	P
show arp inspection vlan <*vlan-list*>	Displays ARP inspection settings for the specified VLANs.	E	3
arp inspection vlan <*vlan-list*>	Enables ARP inspection on the specified VLANs.	C	13
no arp inspection vlan <*vlan-list*>	Disables ARP inspection on the specified VLANs.	C	13
arp inspection vlan <*vlan-list*> logging [all|none|permit|deny]	Enables logging of ARP inspection events on the specified VLANs. 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 VLANs.	C	13

8.3 Command Examples

This example enables ARP inspection on a range of ports, and limits the number of ARP packets per second to 5.

```
sysname# configure
sysname(config)# arp inspection
sysname(config)# interface port-channel 1-3,8,10-100
sysname(config)# no arp inspection trust
sysname(config)# arp inspection limit rate 5
```

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
```

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
```

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
```

CHAPTER 9
ARP Learning Commands

9.1 Command Summary

Use these commands to configure how the Switch updates the ARP table.

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

Table 31 Interface Command Values

COMMAND	DESCRIPTION
port-list	A list of one or more ports, separated by commas with no spaces. The list may also contain ranges of ports signified by a hyphen. For example: 1,3,5–8,10.

The following section lists the commands for this feature.

Table 32 arp-learning Command Summary

COMMAND	DESCRIPTION	M	P
`interface port-channel <port-list>`	Enters config-interface mode for the specified ports.	C	13
`arp-learning <arp-reply|gratuitous-arp|arp-request>`	Sets the ARP learning mode the Switch uses on the port. `arp-reply`: the Switch updates the ARP table only with the ARP replies to the ARP requests sent by the Switch. `gratuitous-arp`: the Switch updates its ARP table with either an ARP reply or a gratuitous ARP request. A gratuitous ARP is an ARP request in which both the source and destination IP address fields are set to the IP address of the device that sends this request and the destination MAC address field is set to the broadcast address. `arp-request`: the Switch updates the ARP table with both ARP replies, gratuitous ARP requests and ARP requests.	C	13
`no arp-learning`	Resets the ARP learning mode to its default setting (`arp-reply`).	C	13

9.2 Command Examples

This example changes the ARP learning mode on port 8 from `arp-reply` to `arp-request`.

```
sysname# configure
sysname(config)# interface port-channel 8
sysname(config-interface)# arp-learning arp-request
```

CHAPTER 10 Auto Configuration Commands

10.1 Auto Configuration Overview

The Switch can download a pre-saved auto configuration file automatically when you reboot the Switch using the DHCP or HTTPS mode. This will overwrite the running configuration stored in the Switch's RAM instead of the startup configuration stored in the Switch's flash memory.

You can use the DHCP mode to load an auto configuration file from a TFTP server automatically when you reboot the Switch. The Switch must have a dynamic IP address assigned by a DHCP server. Also, make sure the Switch can communicate with the TFTP server.

Note: You need to set up configurations on a DHCP server and TFTP server first to use auto configuration.

10.2 Command Summary

The following section lists the commands for this feature.

Table 33 auto-config Command Summary

COMMAND	DESCRIPTION	M	P
`auto-config`	Enables auto configuration. When auto configuration is enabled, the Switch can receive an auto configuration file.	C	14
`no auto-config`	Disables auto configuration.	C	14
`auto-config <dhcp | https>`	Selects the DHCP or HTTPS mode for auto configuration. dhcp: Enables the DHCP mode for auto configuration. When auto configuration DHCP is enabled, the Switch can receive an auto configuration file from a TFTP server. The location of the TFTP server is provided by a DHCP server. `https`: Enables the HTTPS mode for auto configuration. When auto configuration HTTPS is enabled, the Switch will use the URL you specified using the `auto-config url` command to access a web server and download the auto configuration file using HTTPS.	C	14

Table 33 auto-config Command Summary (continued)

COMMAND	DESCRIPTION	M	P
auto-config url <*https://host/filename*>	Types the URL that can be used to access and download the auto configuration file from a web server using HTTPS. For example, https://webserverIPaddressconfigfilename.cfg.	C	14
auto-config vlan <*vlan-id*>	Enters the VLAN ID of the DHCP server that assigns the TFTP server IP address and auto configuration file name to the Switch.	C	14
show auto-config	The following information is displayed: • The mode that is used for auto configuration. • The status to see whether an auto configuration file is successfully loaded to the Switch after you reboot the Switch. • The name of the auto configuration file that is loaded after you reboot the Switch.	E	3

See Chapter 97 on page 377 for the commands to enable and disable DHCP option 60.

10.3 Command Examples

See Section 4.7 on page 25 for an example of how to configure auto configuration using the DHCP mode on the Switch.

CHAPTER 11 Bandwidth Control Commands

11.1 Bandwidth Control Overview

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

Note: 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.

Note: The CIR should be less than the PIR.

See Section 11.3 on page 49 and Section 11.4 on page 50 for examples.

11.2 Command Summary

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

Table 34 User-input Values: running-config

COMMAND	DESCRIPTION
port-list	A list of one or more ports, separated by commas with no spaces. The list may also contain ranges of ports signified by a hyphen. For example: 1,3,5–8,10.
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 35 Command Summary: bandwidth-control & bandwidth-limit

COMMAND	DESCRIPTION	M	P
show interfaces config <*port-list*> bandwidth-control	Displays the current settings for bandwidth control on the specified ports.	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 ports.	C	13
bandwidth-limit ingress <*rate*>	Sets the maximum bandwidth allowed for incoming traffic on the ports.	C	13
bandwidth-limit egress	Enables bandwidth limits for outgoing traffic on the ports.	C	13
bandwidth-limit egress <*rate*>	Sets the maximum bandwidth allowed for outgoing traffic on the ports.	C	13
no bandwidth-limit ingress	Disables ingress bandwidth limits on the specified ports.	C	13
no bandwidth-limit egress	Disables egress bandwidth limits on the specified ports.	C	13
bandwidth-limit cir	Enables commit rate limits on the specified ports.	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 ports.	C	13
bandwidth-limit pir <*rate*>	Sets the maximum bandwidth allowed for the incoming traffic flow on the specified ports.	C	13
no bandwidth-limit cir	Disables commit rate limits on the specified ports.	C	13
no bandwidth-limit pir	Disables peak rate limits on the specified ports.	C	13

11.3 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
```

11.4 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
```

CHAPTER 12
BPDU Guard

12.1 BPDU Guard Overview

A BPDU (Bridge Protocol Data Units) is a data frame that contains information about STP. STP-aware switches exchange BPDUs periodically.

The BPDU guard feature allows you to prevent any new STP-aware switch from connecting to an existing network and causing STP topology changes in the network. If there is any BPDU detected on the ports on which BPDU guard is enabled, the Switch disables the ports automatically. You can then enable the ports manually through the Web Configurator or the commands. With error-disable recovery, you can also have the ports become active after a certain time interval.

12.2 Command Summary

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

Table 36 Interface Command Values

COMMAND	DESCRIPTION
port-list	A list of one or more ports, separated by commas with no spaces. The list may also contain ranges of ports signified by a hyphen. For example: 1,3,5–8,10.

The following section lists the commands for this feature.

Table 37 bpduguard Command Summary

COMMAND	DESCRIPTION	M	P
bpduguard	Enabled BPDU guard on the Switch.	C	13
no bpduguard	Disables BPDU guard on the Switch.	C	13
interface port-channel <*port-list*>	Enters config-interface mode for the specified ports.	C	13
bpduguard	Enabled BPDU guard on the ports.	C	13
no bpduguard	Disables BPDU guard on the ports.	C	13
show bpdupguard	Displays whether BPDU guard is enabled on the Switch and the port status.	E	3

CHAPTER 13
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.

Note: 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 13.2 on page 53 and Section 13.3 on page 53 for examples.

13.1 Command Summary

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

Table 38 User-input Values: broadcast-limit, multicast-limit and dlf-limit

COMMAND	DESCRIPTION
pkt/s	Specifies the maximum number of packets per second accepted by a Switch port.
port-list	A list of one or more ports, separated by commas with no spaces. The list may also contain ranges of ports signified by a hyphen. For example: 1,3,5–8,10.

The following section lists the commands for this feature.

Table 39 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 on the specified ports.	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 ports.	C	13
`bmstorm-limit <rate>`	Specifies the maximum rate at which the Switch receives broadcast, Multicast, and destination lookup failure (DLF) packets on the specified ports. Different models support different rate limiting incremental steps. See your User's Guide for more information.	C	13

Table 39 Command Summary: storm-control, bmstorm-limit, and bstorm-control (continued)

COMMAND	DESCRIPTION	M	P
no bmstorm-limit	Disables broadcast storm control on the specified ports.	C	13
broadcast-limit	Enables the broadcast packet limit on the specified ports.	C	13
broadcast-limit <*pkt/s*>	Specifies the maximum number of broadcast packets the Switch accepts per second on the specified ports. The Switch will generate a trap and/or log when the actual rate is higher than the specified threshold.	C	13
no broadcast-limit	Disables broadcast packet limit no the specified ports.	C	13
multicast-limit	Enables the Multicast packet limit on the specified ports.	C	13
multicast-limit <*pkt/s*>	Specifies the maximum number of Multicast packets the Switch accepts per second on the specified ports. The Switch will generate a trap and/or log when the actual rate is higher than the specified threshold.	C	13
no multicast-limit	Disables Multicast packet limit on the specified ports.	C	13
dlf-limit	Enables the DLF packet limit on the specified ports.	C	13
dlf-limit <*pkt/s*>	Specifies the maximum number of DLF packets the Switch accepts per second on the specified ports.	C	13
no dlf-limit	Disables DLF packet limits no the specified ports.	C	13

13.2 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
```

13.3 Command Example: broadcast-limit, multicast-limit and 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
```

CHAPTER 14
Certificates Commands

14.1 Certificates Overview

The Switch can use HTTPS certificates that are verified by a third-party to create secure HTTPS connections between your computer and the Switch. This way, you may securely access the Switch using the Web Configurator. See Chapter 32 on page 114 for more information about HTTPS.

Certificates are based on public-private key pairs. A certificate contains the certificate owner's identity and public key. Certificates provide a way to exchange public keys for use in authentication.

Use these commands to import an HTTPS certificate to the Switch. You can also clear or show the HTTPS certificate imported to the Switch.

14.2 Command Summary

The following section lists the commands for this feature.

Table 40 auto-config Command Summary

COMMAND	DESCRIPTION	M	P
`import certificate https`	Imports the HTTPS certificate from the FTP server to the Switch. See Section 14.3 on page 56 for the example. Note: You need to upload an HTTPS certificate file to the FTP server first. The Switch is the FTP server. Note: In stacking mode, if synchronize certificates is enabled, then running this command on the Master Switch synchronizes the imported certificate to all stacking members (slave switches).	E	13
`clear certificate https`	Removes the HTTPS certificate uploaded to the Switch.	E	13
`show https certificate`	Displays the HTTPS certificates.	E	3

Table 40 auto-config Command Summary (continued)

COMMAND	DESCRIPTION	M	P
synchronize certificate	Allows the Master Switch in stacking mode to synchronize CA-signed certificates to stacking members (slave switches). The stacking members save the certificates to non-volatile memory. The Master Switch also deletes all CA-signed certificates on stacking members if the certificates do not exist on the Master Switch.	C	13
no synchronize certificate	Stops the Master Switch in stacking mode from synchronizing CA-signed certificates to all stacking members.	C	13

In an IPv6 packet header, the "Next Header" field identifies the next level protocol. The following table shows some common IPv6 Next Header values.

Table 41 Common IPv6 Next Header Values

PROTOCOL TYPE	VALUE
IPv6 Hop-by-Hop Option	0
IPv4	4
TCP	6
UDP	17
IPv6	41
Routing Header for IPv6	43
Fragment Header for IPv6	44
Encapsulation Security Payload	50
Authentication Header	51
ICMP for IPv6	58
No Next Header for IPv6	59
Destination Options for IPv6	60

14.3 Command Example

This example shows you how to import the HTTPS certificate to the Switch.

FTP Server

First, we need to upload an HTTPS certificate file to the FTP server. The Switch is the FTP server.

1 Select **Start** > **All Programs** > **Accessories** > **Command Prompt**.

2 Use the `ftp <ip address>` command and enter the Switch IP address to have your computer ping the Switch. In this example, we use the default out-of-band IP address (**192.168.0.1**) for the Switch IP address.

Use the default in-band management IP address (**192.168.1.1**), DHCP-assigned IP address, static IP address, or the default out-of-band IP address (**192.168.0.1**). It doesn't matter which IP address you use as long as your computer can ping the Switch.

3 Enter the login username and password of the Switch. The default username is **admin** and associated default password is **1234**.

```
C:\Users>ftp 192.168.0.1
Connected to 192.168.0.1
220 XS3800 FTP version 1.0 ready at Fri Oct 19 05:14:22 2018
User (192.168.0.1:(none)): admin
331 Enter PASS command
Password:
230 Logged in
ftp>
```

4 Enter the `put <file name> https-cert` command to upload an HTTPS certificate file to the Switch.

```
ftp> put CAfile.pfx https-cert
```

The Switch

Access the CLI. See Chapter 1 for more information about how to access the CLI.

1 Enter the `import certificate https` command to import the HTTPS certificate from the FTP server to the Switch.

2 Type the certificate file's password that was created when the PKCS #12 file was exported.

```
sysname# import certificate https
Password:*****

Import Successfully
```

CHAPTER 15
Classifier Commands

15.1 Classifier Overview

Use these commands to classify packets into traffic flows. After classifying traffic, policy commands (Chapter 64 on page 260) can be used to ensure that a traffic flow gets the requested treatment in the network.

15.2 Command Summary

The following section lists the commands for this feature.

Table 42 Command Summary: classifier

COMMAND	DESCRIPTION	M	P
`show classifier [<name>]`	Displays classifier configuration details.	E	3
`clear classifier match-count [<name>]`	Removes the number of times all or the specified classifier rule is applied.	E	3

Table 42 Command Summary: classifier (continued)

COMMAND	DESCRIPTION	M	P
classifier <*name*> < [weight <0-65535>][packet- format <802.3untag|802.3tag| EtherIIuntag|EtherIItag>] [priority <0-7>] [inner-priority <*0-7*>] [vlan <*vlan-id*>] [inner-vlan <*vlan-id-list*>][ethernet-type <*ether-num*|ip|ipx|arp|rarp|appletalk|decnet|ipv6|IPv6>] [source-mac <*src-mac-addr*> [mask <*mask*>]] [source-port <*port-list*>] [source-trunk <*trunk-list*>] [destination-port <*port-list*>] [destination-mac <*dest-mac-addr*> [mask <*mask*>]] [ip-packet-length <*0-65535*> to <0-65525>] [dscp <*0-63*>] [precedence <*0-7*>] [tos <*0-255*>] [ipv6-dscp <0-63>] [ipv6-dscp <*0-63*>] [ip-protocol <*protocol-num*|tcp|udp|icmp|egp| ospf|rsvp|igmp|igp|pim|ipsec> [establish-only]] [ipv6-next-header <*protocol-num*|tcp|udp|icmpv6> [establish-only]] [ipv6-next-header <*protocol-num*|tcp|udp|icmpv6> [establish-only]][source-ip <*src-ip-addr*> [mask-bits <*mask-bits*>]] [ipv6-source-ip <*src-ipv6-addr*> [prefix-length <*prefix-length*>]] [ipv6-source-ip <*src-ipv6-addr*> [prefix-length <*prefix-length*>]] [source-socket <*socket-num*> [to <*socket-num*>]]] [destination-ip <*dest-ip-addr*> [mask-bits <*mask-bits*>]] [ipv6-destination-ip <*dest-ipv6-addr*> [prefix-length <*prefix-length*>]] [ipv6-destination-ip <*dest-ipv6-addr*> [prefix-length <*prefix-length*>]] [destination-socket <*socket-num*> [to <*socket-num*>]]] [time-range <*name*>] [log] [count] [inactive]>	Configures a classifier. Specify the parameters to identify the traffic flow: • weight: Enter the weight the priority of the Classifier rule when the match order is in manual mode. A higher weight means a higher priority. • priority: Type *0* to classify traffic from any priority level or type a priority level with *1* being the highest priority. • inner-priority: Type *0* to classify traffic from any inner priority level or type a priority level with *1* being the highest priority. • vlan-id: Type *0* to classify traffic from any VLAN or type a specific VLAN ID number. • inner-vlan-id: Type *0* to classify traffic from any inner VLAN or type a specific inner VLAN ID number. • ethernet-type: Enter one of the Ethernet types or type the hexadecimal number that identifies an Ethernet type (see Table 43 on page 60). • source-mac: Enter the source MAC address of the packet. • source-port: Enter any to classify traffic received on any port or type a specific port number. • source-trunk: Enter any to classify traffic from any trunk group or type a specific trunk group ID number. • destination-port: Enter any to classify traffic to any destination port or type a specific port number. • destination-mac: Enter the destination MAC address of the packet. • ip-protocol: Enter one of the protocols or type the port number that identifies the protocol (see Table 44 on page 60). • mask: type the mask for the specified MAC address to determine which bits a packet's MAC address should match. Enter "f" for each bit of the specified MAC address that the traffic's MAC address should match. Enter "0" for the bits of the matched traffic's MAC address, which can be of any hexadecimal characters. For example, if you set the MAC address to 00:13:49:00:00:00 and the mask to ff:ff:ff:00:00:00, a packet with a MAC address of 00:13:49:12:34:56 matches this criteria. • tos: Enter any to classify traffic from any ToS, or set an IP Precedence (the first 3 bits of the 8-bit ToS field) value and a Type of Service (the last 5 bits of the 8-bit ToS field) value. • establish-only: Enter this to identify only TCP packets used to establish TCP connections. • source-ip: Enter the source IPv4 address of the packet. • ipv6-source-ip: Enter the source IPv6 address of the packet. • source-socket: (for UDP or TCP protocols only) Specify the protocol port number. • destination-ip: Enter the destination IPv4 address of the packet. • ipv6-destination-ip: Enter the destination IPv6 address of the packet. • destination-socket: (for UDP or TCP protocols only) specify the protocol port number. • time-range: Enter the name of a pre-defined time-range rule. • inactive: Disables this classifier.	C	13

Table 42 Command Summary: classifier (continued)

COMMAND	DESCRIPTION	M	P
`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
`classifier match-order <auto|manual>`	Use *manual* to have classifier rules applied according to the weight of each rule you configured. Use *auto* to have classifier rules applied according to the layer of the item configured in the rule.	C	13
`classifier logging`	Creates a log when packets match a classifier rule during a defined time interval.	C	13
`classifier logging interval <0-65535>`	Enter the length of the time period (in seconds) to count matched packets for a classifier rule. Enter an integer from 0 – 65535. 0 means that no logging is done.	C	13
`no classifier logging`	Disallows the Switch to create a log message when packets match a classifier rule during a defined time interval.	C	13

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

Table 43 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 an IPv4 packet header, the “Protocol” field identifies the next level protocol. The following table shows some common IPv4 protocol types and the corresponding protocol number. Refer to http://www.iana.org/assignments/protocol-numbers for a complete list.

Table 44 Common IPv4 Protocol Types and Protocol Numbers

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

In an IPv6 packet header, the "Next Header" field identifies the next level protocol. The following table shows some common IPv6 Next Header values.

Table 45 Common IPv6 Next Header Values

PROTOCOL TYPE	VALUE
IPv6 Hop-by-Hop Option	0
IPv4	4
TCP	6
UDP	17
IPv6	41
Routing Header for IPv6	43
Fragment Header for IPv6	44
Encapsulation Security Payload	50
Authentication Header	51
ICMP for IPv6	58
No Next Header for IPv6	59
Destination Options for IPv6	60

15.3 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. See the policy example in Chapter 64 on page 260.

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

This example creates a classifier (**Class1**) for packets which have a source MAC address of 11:22:33:45:67:89 and are received on port 1. You can then use the policy command and the name **Class1** to apply policy rules to this traffic flow. See the policy example in Chapter 64 on page 260.

```
sysname# config
sysname(config)# classifier Class1 source-mac 11:22:33:45:67:89 source-port
1
sysname(config)# exit
sysname# show classifier
Index Active Name                              Rule
    1 Yes    Class1                          SrcMac = 11:22:33:45:67:89; S...
```

The default value of match-order is auto. Use the following command to make weight work by changing the default value of match-order to manual and configuring a classifier weight value where the higher the weight, the higher the priority.

```
sysname# config
sysname(config)#classifier match-order manual
sysname(config)#classifier 1 weight 12345 source-port 1/1
```

CHAPTER 16
Cluster Commands

16.1 Command Summary

The following section lists the commands for this feature.

Table 46 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 the switches that are potential cluster members. The switches must be directly connected.	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 members and their running status.	E	3
show cluster member config	Displays the current cluster members.	E	3
show cluster member mac <*mac*>	Displays the running status of the cluster members.	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

16.2 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/GS2220-10HP/GS2220-10HP
      1 00:13:49:00:00:02/XS3800-28/XS3800-28
      2 00:19:cb:00:00:02/GS2220-28HP/GS2220-28HP
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 GS2220-10HP                     Online
      2 00:13:49:00:00:02 XS3800-28                       Online
```

The following table describes the labels in this screen.

Table 47 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.


XS3800-28# show version
  Current ZyNOS version: V4.80(ABML.0)b7 | 04/07/2022
XS3800-28# 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 48 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.

CHAPTER 17
CLV Commands

17.1 CLV Overview

Use these commands to configure VLAN settings on the Switch in clv mode. In Zyxel configuration mode, you need to use the VLAN commands to configure a VLAN first, then specify the ports which you want to configure and tag all outgoing frames with the specified VLAN ID. In clv mode, you need to specify the ports first, then configure frames which you want to tag with the specified VLAN ID.

Note: See Table 8 on page 13 for the products that support the CLV commands.

CLV mode is supported only in the Command Line Interface (CLI). If you have enabled CLV mode to configure the Switch's VLAN settings, further VLAN changes you make through the Web Configurator will not be saved and applied completely. You can still use the Web Configurator to view the VLAN status.

If you want to configure VLAN settings in both the Web Configurator and the CLI, just return to Zyxel configuration mode by turning off CLV mode.

17.2 Command Summary

The following section lists the commands for this feature. There are three different ways that you can configure ports on the Switch. Use **Access** mode to untag outgoing frames; usually connect a port in **Access** mode to a computer. Use **Trunk** mode to tag outgoing frames; usually connect a port in **Trunk** mode to another Switch. Use **Hybrid** mode to tag or untag outgoing frames; usually connect a port in **Hybrid** mode to another Switch or computer.

Suppose port 1 is configured as a native VLAN with VLAN ID 100. Then all untagged incoming traffic that goes out from port 1 will be tagged with VLAN ID 100.

Suppose port 2 is configured in **Access** mode. Then all outgoing traffic from port 2 will be untagged.

Suppose port 3 is configured in **Trunk** mode. Then all outgoing traffic from port 3 will be tagged with VLAN ID 100.

Figure 2 Trunk – Access Mode Example

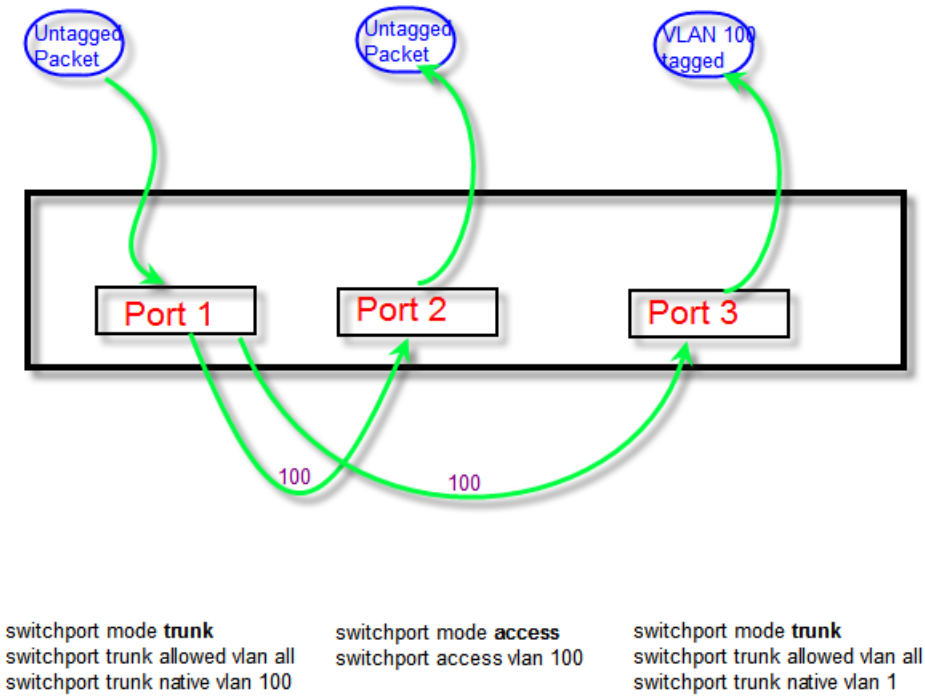


Table 49 Interface Command Values

COMMAND	DESCRIPTION
port-list	A list of one or more ports, separated by commas with no spaces. The list may also contain ranges of ports signified by a hyphen. For example: 1,3,5–8,10.

Table 50 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

Table 51 clv Command Summary

COMMAND	DESCRIPTION	M	P
clv	Enables clv mode.	C	13
no clv	Disables clv mode.	C	13

Table 52 switchport mode Command Summary

COMMAND	DESCRIPTION	M	P
interface port-channel <*port-list*>	Enters config-interface mode for the specified ports.	C	13

Table 52 switchport mode Command Summary (continued)

COMMAND	DESCRIPTION	M	P
switchport mode <access|trunk|hybrid>	Specifies VLAN configuration mode on the specified ports. • Use **Access** to untag outgoing frames with a VLAN ID. • Use **Trunk** to tag outgoing frames with a VLAN ID. • Use **Hybrid** to tag or untag outgoing frames with a VLAN ID.	C	13
no switchport mode	Resets VLAN configuration mode to the default switchport mode. The default switchport mode is hybrid mode.	C	13

Table 53 switchport access Command Summary

COMMAND	DESCRIPTION	M	P
interface port-channel <*port-list*>	Enters config-interface mode for the specified ports.	C	13
switchport mode access	Sets the specified interface in access mode.	C	13
switchport access <*vlan-id*>	Untags all outgoing frames with the specified VLAN ID.	C	13
no switchport access vlan	Resets all outgoing frames to the default VLAN ID. The default VLAN ID is VLAN 1.	C	13

Table 54 switchport trunk Command Summary

COMMAND	DESCRIPTION	M	P
interface port-channel <*port-list*>	Enters config-interface mode for the specified ports.	C	13
switchport mode trunk	Sets the specified interface in trunk mode.	C	13
switchport trunk allowed vlan <*vlan-list*>	Tags all outgoing frames with the specified VLAN ID.	C	13
no switchport trunk allowed vlan <*vlan-list*>	Disables the specified VLAN trunk on the ports.	C	13
switchport trunk allowed vlan all	Tags all outgoing frames for all VLANs.	C	13
no switchport trunk allowed vlan all	Disables all VLAN trunks on the ports.	C	13
switchport trunk native vlan <*vlan-id*>	Tags all incoming untagged frames with the specified VLAN ID. The default VLAN ID is VLAN 1 for all ports. Sets a VLAN ID in the range 1 to 4094.	C	13
no switchport trunk native vlan	Resets all incoming untagged frames to the default VLAN ID. The default VLAN ID is VLAN 1.	C	13

Table 55 switchport hybrid Command Summary

COMMAND	DESCRIPTION	M	P
interface port-channel <*port-list*>	Enters config-interface mode for the specified ports.	C	13
switchport mode hybrid	Sets the specified interface in hybrid mode.	C	13
switchport hybrid allowed vlan <*vlan-list*> tagged	Tags all outgoing frames with the specified VLAN ID.	C	13
switchport hybrid allowed vlan <*vlan-list*> untagged	Untags all outgoing frames with the specified VLAN ID.	C	13
no switchport hybrid allowed vlan <*vlan-list*>	Disables the specified VLAN ID on the ports.	C	13

Table 55 switchport hybrid Command Summary (continued)

COMMAND	DESCRIPTION	M	P
switchport hybrid pvid <*vlan-id*>	Tags all incoming untagged frames with the specified VLAN ID.	C	13
no switchport hybrid pvid <*vlan-id*>	Resets all incoming untagged frames to the default VLAN ID. The default VLAN ID is VLAN 1.	C	13

Table 56 switchport forbidden Command Summary

COMMAND	DESCRIPTION	M	P
interface port-channel <*port-list*>	Enters config-interface mode for the specified ports.	C	13
switchport forbidden vlan add <*vlan-list*>	Prohibits the specified ports from joining the specified VLAN group.	C	13
switchport forbidden vlan add all	Prohibits the specified ports from joining all VLAN groups.	C	13
switchport forbidden vlan remove <*vlan-list*>	Sets forbidden ports in the specified VLAN to normal ports.	C	13
switchport forbidden vlan remove all	Sets all forbidden ports in the port list to normal ports.	C	13

17.3 Command Examples

This example configures clv mode.

```
sysname# config
sysname(config)# clv
```

Note: The following commands all have clv mode enabled.

This example configures clv for VLAN 20 on port 1.

```
sysname# config
sysname(config)# interface port-channel 1
sysname(config-interface)# switchport mode access
sysname(config-interface)# switchport access vlan 20
sysname(config-interface)# exit
```

This example activates clv for VLAN 100 and VLAN 20 on ports 1 to 3. This example prohibits ports 1 to 3 from joining VLAN 200.

```
sysname# config
sysname(config)# interface port-channel 1-3
sysname(config-interface)# switchport mode trunk
sysname(config-interface)# switchport trunk allowed vlan 100
sysname(config-interface)# switchport trunk native vlan 20
sysname(config-interface)# switchport forbidden vlan add 200
sysname(config-interface)# exit
```

This example configures port 4 as the tagged port in VLAN 20 and the untagged port in VLAN 100. This example also configures 200 as the PVID on port 4.

```
sysname# config
sysname(config)# interface port-channel 4
sysname(config-interface)# switchport mode hybrid
sysname(config-interface)# switchport hybrid allowed vlan 20 tagged
sysname(config-interface)# switchport hybrid allowed vlan 100 untagged
sysname(config-interface)# switchport hybrid pvid 200
sysname(config-interface)# exit
```

This example shows the VLAN table.

```
sysname# show vlan
  The Number of VLAN :     4
  Idx.  VID   Status     Elap-Time    TagCtl
  ----  ----  ---------  -----------  ---------------------------------
---

    1     1     Static    145:03:37  Access :1-3,6-52
                                     Trunk  :

    2    20     Static      1:47:09  Access :
                                     Trunk  :4

    3   100     Static     26:04:36  Access :4
                                     Trunk  :1-3

    4   200     Static      2:01:54  Access :
                                     Trunk  :
```

The following table describes the labels in this screen.

Table 57 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 through 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. **Access**: These ports do not tag outgoing frames with the VLAN ID. **Trunk**: These ports tag outgoing frames with the VLAN ID.

This example shows the VLAN 100 status.

```
sysname# show vlan 100
  802.1Q VLAN ID : 100
  Name           :
  Status         : Static
  Elapsed Time   :   26:05:15

  Port Information Mode
  ---------------- ----
     1              Trunk
     2              Trunk
     3              Trunk
     4              Hybrid
```

CHAPTER 18
Custom Default Commands

18.1 Custom Default Overview

You can save the current configuration settings to a customized default file, so you can load it when you reboot the Switch.

18.2 Command Summary

The following section lists the commands for this feature.

Table 58 custom-default Command Summary

COMMAND	DESCRIPTION	M	P
`custom-default`	Enables custom default.	C	14
`no custom-default`	Disables custom default.	C	14

See Chapter 78 on page 313 for the commands to save the current configuration settings permanently to a customized default file, and load it when rebooting the Switch.

18.3 Command Examples

See Section 4.8 on page 27 for an example of how to configure custom default on the Switch.

CHAPTER 19
Date and Time Commands

19.1 Command Summary

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

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

Table 59 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 60 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. Note: You can configure a time zone with a 30-minute offset (for example, UTC –630).	C	13
`time daylight-saving-time`	Enables daylight saving time. The current time is updated if daylight saving time has started.	C	13

Table 60 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 61 timesync Command Summary

COMMAND	DESCRIPTION	M	P
show timesync	Displays time server information.	E	3
timesync server <time-server1> [<time-server2> [<time-server3>]]	Sets the IPv4 / IPv6 address or domain name of the first, second, and third timeservers. The Switch attempts to connect to the timeserver for up to 60 seconds. 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

19.2 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 sets the first, second, and third time servers.

```
sysname# configure
sysname(config)# timesync server 0.pool.ntp.org 1.pool.ntp.org
time.google.com
```

This example looks at the current time server settings.

```
sysname# show timesync


  Time Configuration
  ----------------------------
  Time Zone                          :UTC 0
  Time Sync Mode                     :USE_NTP
  Time Server 1                      :0.pool.ntp.org
  Time Server 2                      :1.pool.ntp.org
  Time Server 3                      :time.google.com
  Time Server Sync Status            :CONNECTING
  Time Server Sync Interval(minutes):1440
```

The following table describes the labels in this screen.

Table 62 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 1 / 2 / 3	This field displays the IPv4 / IPv6 address or domain name of the time server. The Switch will search for the first, then the second, then the third time server for around 60 seconds.
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.

CHAPTER 20
DHCP Commands

20.1 DHCP Overview

Use these commands to configure DHCP features on the Switch.

- Use the dhcp option commands to configure DHCP Option 82 profiles.
- 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. (This command is available on a layer 3 Switch only.)

20.2 Command Summary

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

Table 63 Interface Command Values

COMMAND	DESCRIPTION
port-list	A list of one or more ports, separated by commas with no spaces. The list may also contain ranges of ports signified by a hyphen. For example: 1,3,5–8,10.

The following section lists the commands for this feature.

Table 64 dhcp option Command Summary

COMMAND	DESCRIPTION	M	P
dhcp option profile <*name*> [circuit-id [slot-port] [vlan] [hostname] [string <*string*>]] [remote-id [mac] [string <*string*>]]	Creates a DHCPv4 option 82 profile.	C	13
no dhcp option profile <*name*>	Deletes the specified DHCPv4 option 82 profile.	C	13
show dhcp option profile	Displays DHCP option 82 profile settings.	E	3

Table 65 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
dhcp relay <*vlan-id*> helper-address <*remote-dhcp-server1*> [<*remote-dhcp-server2*>] [<*remote-dhcp-server3*>] [option profile <*name*>]	Enables DHCP relay on the specified VLAN and sets the IP address of up to 3 DHCP servers. Optionally, specify a pre-defined DHCP option 82 profile that the Switch applies to all ports in this VLAN. 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
dhcp relay <*vlan-id*> interface port-channel <*port-list*> option profile <*name*>	Specifies a pre-defined DHCP option 82 profile that the Switch applies to the specified ports in this VLAN. The Switch adds the Circuit ID sub-option and/or Remote ID sub-option specified in the profile to DHCP requests that it relays to a DHCP server.	C	13
dhcp relay <*vlan-id*> source-address <*ip-addr*>	Specifies the source IP address that the Switch adds to DHCP requests from clients in this VLAN before forwarding them. The source IP address helps DHCP clients obtain an appropriate IP address when you configure multiple routing domains on a VLAN.	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*> interface port-channel <*port-list*> option	Sets the Switch to not apply a DHCP option 82 profile to the specified ports in this VLAN.	C	13
no dhcp relay <*vlan-id*> source-address	Removes the source IP address setting and sets this field set to 0.0.0.0. The Switch automatically sets the source IP address of the DHCP requests to the IP address of the interface on which the packet is received.	C	13
no dhcp relay <*vlan-id*> option	Disables the relay agent information option 82.	C	13

Table 66 dhcp relay-broadcast Command Summary

COMMAND	DESCRIPTION	M	P
dhcp relay-broadcast	The broadcast behavior of DHCP packets (within the VLANs on which DHCP relay is enabled) will not be terminated by the Switch.	C	13
no dhcp relay-broadcast	The Switch terminates the broadcast behavior of DHCP packets within the VLANs on which DHCP relay is enabled.	C	13

Table 67 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 interface port-channel <*port-list*> option profile <*name*>	Specifies a pre-defined DHCP option 82 profile that the Switch applies to the specified ports. Note: The profile you specify here has priority over the one you set using the dhcp smart-relay option profile <*name*> command.	C	13
dhcp smart-relay option profile <*name*>	Specifies a pre-defined DHCPv4 option 82 profile that the Switch applies to all ports. The Switch adds the Circuit ID sub-option and/or Remote ID sub-option specified in the profile to DHCP requests that it relays to a DHCP server.	C	13
no dhcp smart-relay interface port-channel <*port-list*>	Sets the Switch to not apply a DHCP option 82 profile to the specified ports.	C	13

Table 68 dhcp server Command Summary

COMMAND	DESCRIPTION	M	P
dhcp server <*vlan-id*> starting-address <*ip-addr*> <*subnet-mask*> size-of-client-ip-pool <1-1024>	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 <1-1024> [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
dhcp server guard	Enables DHCP Server Guard on the Switch. When enabled, the Switch only forwards DHCP packets received on trusted ports. DHCP packets received on untrusted ports are dropped. You can set ports as trusted or untrusted using the interface port-channel command. By default, all ports are untrusted. Note: DHCP Server Guard cannot be enabled if DHCP Snooping is enabled.	C	13
no dhcp server guard	Disables DHCP Server Guard on the Switch.	C	13
interface port-channel <*port-list*>	Enters config-interface mode for the specified ports.	C	13
dhcp server trust	Sets the specified ports as trusted for DHCP Server Guard. The Switch forwards DHCP packets received on the port.	C	13

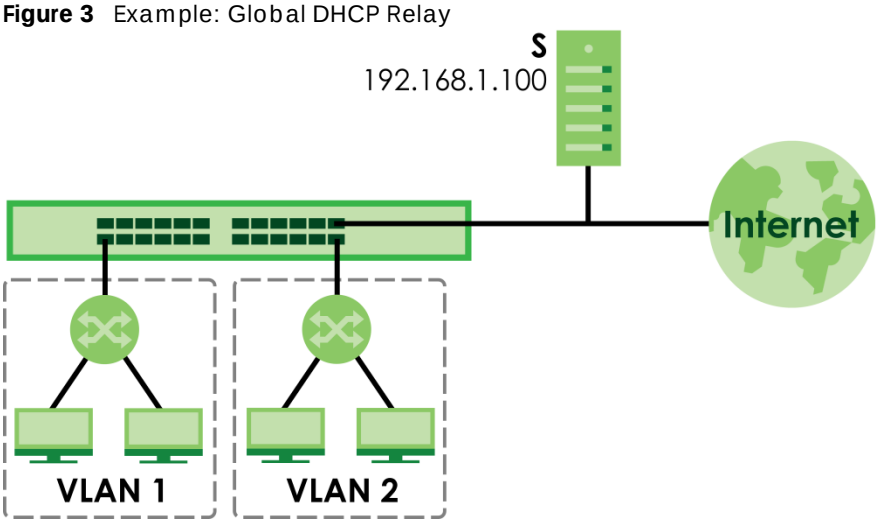
Table 68 dhcp server Command Summary (continued)

COMMAND	DESCRIPTION	M	P
`no dhcp server trust`	Sets the specified ports as untrusted for DHCP Server Guard. If DHCP Server Guard is enabled, the Switch drops DHCP packets received on the port.	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
`show dhcp server`	Displays DHCP server settings.	E	13
`show dhcp server <vlan-id>`	Displays DHCP server settings in a specified VLAN.	E	13

20.3 Command Examples

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

Figure 3 Example: Global DHCP Relay

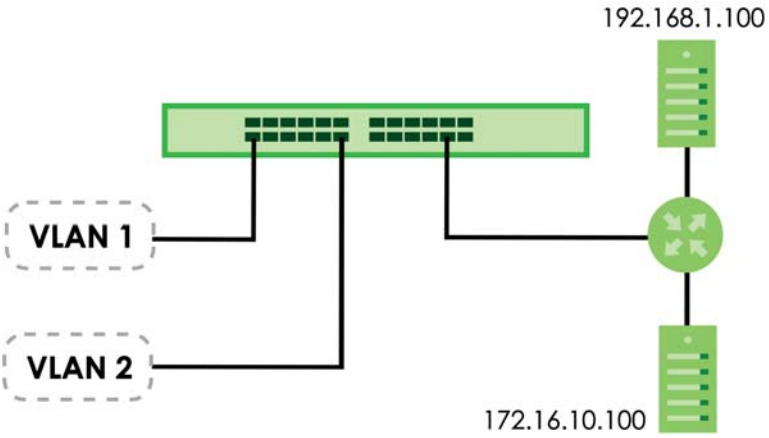


This example shows how to configure the Switch for this configuration. DHCP relay agent information option 82 is also enabled.

```
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 4 Example: DHCP Relay for Two VLANs

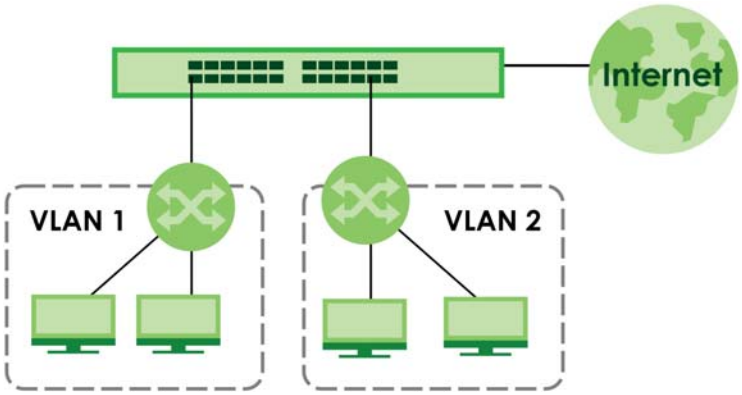


This example shows how to configure these DHCP servers. The VLANs are already configured.

```
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 5 Example: DHCP Relay for Two VLANs



This example shows how to configure the DHCP server for VLAN 1 with the configuration shown in Figure 5 on page 81. 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
```

In this example, we enable DHCP Server Guard, set ports 5 and 6 as trusted (as they are connected to a DHCP server), and then verify the settings are active on the Switch.

```
sysname# configure
sysname(config)# dhcp server guard
sysname(config)# interface port-channel 5-6
sysname(config-interface)# dhcp server trust
sysname(config-interface)# exit
sysname# show running-config
 interface port-channel 5
  dhcp server trust
 interface port-channel 6
  dhcp server trust
dhcp server guard
```

CHAPTER 21
DHCP Snooping and DHCP VLAN Commands

21.1 DHCP Snooping and DHCP VLAN Overview

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 server packets on the network and builds a binding table dynamically by snooping DHCP server packets. The Switch allows only the authorized DHCP server on a trusted port to assign IP addresses. Clients on your network will only receive DHCP packets from the authorized DHCP server.

21.2 Command Summary

The following section lists the commands for this feature.

Table 69 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
show dhcp snooping option [vlan <*vlan-list*>] [interface <*port-list*>]	Displays the DHCP option 82 profile that the Switch applies to ports in the specified VLAN or to the specified ports.	E	3
dhcp snooping	Enables DHCP Snooping on the Switch. Note: DHCP Snooping cannot be enabled if DHCP Server Guard is enabled.	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

Table 69 dhcp snooping Command Summary (continued)

COMMAND	DESCRIPTION	M	P
no dhcp snooping database timeout	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	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
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. Note: When DHCP Snooping is disabled on a VLAN, the Switch still uses CPU resources to examine packets from the VLAN. To prevent the Switch from processing packets from a VLAN at the hardware level, use the command dhcp snooping bypass-vlan.	C	13
dhcp snooping vlan <*vlan-list*> interface port-channel <*port-list*> option profile <*name*>	Specifies a pre-defined DHCP option 82 profile that the Switch applies to the specified ports in the specified VLAN.	C	13
no dhcp snooping vlan <*vlan-list*> interface port-channel <*port-list*> option	Sets the Switch to not apply a DHCP option 82 profile to the specified ports.	C	13
dhcp snooping vlan <*vlan-list*> option profile <*name*>	Specifies a pre-defined DHCP option 82 profile that the Switch applies to all ports in the specified VLAN.	C	13
clear dhcp snooping database statistics	Delete all statistics records of DHCP requests going through the Switch.	E	13
dhcp snooping bypass-vlan <*vlan-list*>	Sets the Switch to not process DHCP packets from the specified VLANs. When DHCP Snooping is disabled on a VLAN, the Switch still uses CPU resources to examine packets from the VLAN. This command prevent the Switch from processing packets from a VLAN at the hardware level.	C	13
no dhcp snooping bypass-vlan <*vlan-list*>	Sets the Switch to process DHCP packets from the specified VLANs.	C	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

Table 69 dhcp snooping Command Summary (continued)

COMMAND	DESCRIPTION	M	P
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 70 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

21.3 Command Examples

This example:

- Enables DHCP snooping on the 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 the Switch to not process DHCP packets on VLAN 5.
- 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)# dhcp snooping bypass-vlan 5
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
```

CHAPTER 22
DiffServ Commands

22.1 Command Summary

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

The following section lists the commands for this feature.

Table 71 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 ports. The list consists of one or more ports, separated by commas with no spaces. The list may also contain ranges of ports signified by a hyphen. For example: 1,3,5–8,10.	C	13
`diffserv`	Enables DiffServ on the ports.	C	13
`no diffserv`	Disables DiffServ on the ports.	C	13

CHAPTER 23
Display Commands

23.1 Command Summary

Use these commands to display configuration information.

The following section lists the commands for this feature.

Table 72 display Command Summary

COMMAND	DESCRIPTION	M	P
display user <[system][snmp]>	Displays all or specific user account information in the configuration file. system: Displays system account information, such as admin, enable or login username and password. snmp: Displays SNMP user account information.	C	14
no display user <[system][snmp]>	Hide all or specific user account information in the configuration file.	C	14
display aaa <[authentication][authorization][server]>	Displays all or specific AAA information in the configuration file. authentication: Displays authentication information in the configuration file. authorization: Displays authorization information in the configuration file. server: Displays authentication server information in the configuration file.	C	14
no display aaa <[authentication][authorization][server]>	Hide all or specific AAA information in the configuration file.	C	14

CHAPTER 24
DVMRP Commands

24.1 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.

24.2 Command Summary

The following section lists the commands for this feature.

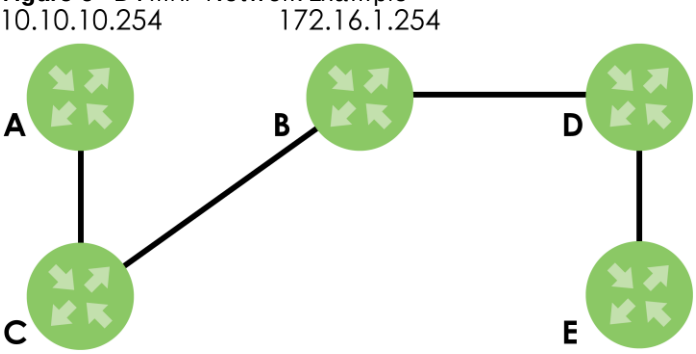
Table 73 Command Summary: DVMRP

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
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

24.3 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 6 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
```

CHAPTER 25
Error Disable and Recovery Commands

25.1 CPU Protection Overview

Switches exchange protocol control packets in a network to get the latest networking information. If a Switch receives large numbers of control packets, such as ARP, BPDU or IGMP packets, which are to be processed by the CPU, the CPU may become overloaded and be unable to handle regular tasks properly.

The CPU protection feature allows you to limit the rate of ARP, BPDU and IGMP packets to be delivered to the CPU on a port. This enhances the CPU efficiency and protects against potential DoS attacks or errors from other networks. You then can choose to drop control packets that exceed the specified rate limit or disable a port on which the packets are received.

25.2 Error-Disable Recovery Overview

Some features, such as loop guard or CPU protection, allow the Switch to shut down a port or discard specific packets on a port when an error is detected on the port. For example, if the Switch detects that packets sent out the ports loop back to the Switch, the Switch can shut down the ports automatically. After that, you need to enable the ports or allow the packets on a port manually through the Web Configurator or the commands. With error-disable recovery, you can set the disabled ports to become active or start receiving the packets again after the time interval you specify.

User Input Values

This section lists the common term definition appears in this chapter.

Table 74 error-disable recovery command user input values

USER INPUT	DESCRIPTION
port-list	A list of one or more ports, separated by commas with no spaces. The list may also contain ranges of ports signified by a hyphen. For example: 1,3,5–8,10.

25.3 Command Summary

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

Table 75 Interface Command Values

COMMAND	DESCRIPTION
port-list	A list of one or more ports, separated by commas with no spaces. The list may also contain ranges of ports signified by a hyphen. For example: 1,3,5–8,10.

The following section lists the commands for this feature.

Table 76 cpu-protection Command Summary

COMMAND	DESCRIPTION	M	P
`interface port-channel <port-list>`	Enables a port or a list of ports for configuration.	C	13
`cpu-protection cause <ARP|BPDU|IGMP> rate-limit <0-256>`	Sets the maximum number of ARP, BPDU or IGMP packets that the specified ports are allowed to receive or transmit per second. `0` means no rate limit.	C	13
`clear cpu-protection interface port-channel <port-list> cause <ARP|BPDU|IGMP>`	Resets the "Total Drop" counters for the specified ports to zero (0). You can see the counter using the `show cpu-protection` command. The "Total Drops" means the number of ARP, BPDU or IGMP packets that have been dropped due to the Error Disable feature in `rate-limitation` mode.	E	13
`reset cpu-protection interface port-channel <port-list> cause <ARP|BPDU|IGMP>`	Sets the specified ports to handle all ARP, BPDU or IGMP packets in stead of ignoring them, if the ports are in `inactive-reason` mode (set by using the `errdisable detect cause` command).	E	13
`show cpu-protection interface port-channel <port-list>`	Shows the CPU Protection settings and the number of ARP, BPDU and/or IGMP packets that has been dropped by the Error Disable feature for the specified ports.	E	13

Table 77 errdisable recovery Command Summary

COMMAND	DESCRIPTION	M	P
`errdisable detect cause <ARP|BPDU|IGMP>`	Sets the Switch to detect if the number of ARP, BPDU or IGMP packets exceeds the rate limit on ports (set by using the `cpu-protection cause` command).	C	13
`errdisable detect cause <ARP|BPDU|IGMP> mode <inactive-port|inactive-reason|rate-limitation>`	Sets the action that the Switch takes when the number of ARP, BPDU or IGMP packets exceeds the rate limit on ports. `inactive-port`: The Switch shuts down the port. `inactive-reason`: The Switch bypasses the processing of the specified control packets (such as ARP or IGMP packets), or drops all the specified control packets (such as BPDU) on the port. `rate-limitation`: The Switch drops the additional control packets the ports have to handle in every one second.	C	13
`errdisable recovery`	Turns on the disabled port recovery function on the Switch.	C	13
`errdisable recovery cause <loopguard|ARP|BPDU|IGMP|anti-arpscan|bpduguard|zuld>`	Enables the recovery timer for the specified feature that causes the Switch to shut down ports.	C	13

Table 77 errdisable recovery Command Summary (continued)

COMMAND	DESCRIPTION	M	P
errdisable recovery cause <loopguard|ARP|BPDU|IGMP|anti-arpscan|bpduguard|zuld> interval <30-2592000>	Sets how many seconds the Switch waits before enabling the ports which was shut down.	C	13
no errdisable detect cause <ARP|BPDU|IGMP>	Disables the rate limit for ARP, BPDU or IGMP packets on ports, set by using the cpu-protection cause command.	C	13
no errdisable recovery	Turns off the disabled port recovery function on the Switch.	C	13
no errdisable recovery cause <loopguard|ARP|BPDU|IGMP|anti-arpscan|bpduguard|zuld>	Disables the recovery timer for the specified feature that causes the Switch to shut down a port.	C	13
show errdisable	Displays which ports are detected (by Error Disable), the mode of the ports, and which packets (ARP, BPDU, or IGMP) are being detected.	E	13
show errdisable detect	Displays the Error Disable settings including the available protocol of packets (ARP, BPDU or IGMP), the current status (enabled or disabled), and the corresponding action the Switch takes when a detected port is handling packets over the limit.	E	13
show errdisable recovery	Displays the disabled port recovery settings and after how many seconds which ports will be activated.	E	13

25.4 Command Examples

This example shows you how to configure the following:

- limit the number of ARP packets that port 7 can handle to 100 packets per second.
- set to shut down port 7 when the number ARP packets the port should handle exceeds the rate limit.
- display the CPU protection settings that you just set for port 7.

- display the Error Disable status and action mode for ARP packet handling.

```
sysname# config
sysname(config)# interface port-channel 7
sysname(config-interface)# cpu-protection cause ARP rate-limit 100
sysname(config-interface)# exit
sysname(config)# errdisable detect cause ARP
sysname(config)# errdisable detect cause ARP mode inactive-port
sysname(config)# exit
sysname# show cpu-protection interface port-channel 7
  Port : 7

  Reason        Rate                Mode     Total Drops
  ------     -------     ---------------     -----------
     ARP         100       inactive-port               -
    BPDU           0       inactive-port               -
    IGMP           0       inactive-port               -

sysname# show errdisable detect

  Reason      Status                Mode
  ------     -------     ---------------
     ARP      enable       inactive-port
    BPDU      enable     rate-limitation
    IGMP      enable       inactive-port
sysname#
```

This example enables the disabled port recovery function and the recovery timer for the loopguard feature on the Switch. If a port is shut down due to the specified reason, the Switch activates the port 300 seconds (the default value) later. This example also shows the number of the disabled ports and the time left before the ports becomes active.

```
sysname# configure
sysname(config)# errdisable recovery
sysname(config)# errdisable recovery cause loopguard
sysname(config)# exit
sysname# show errdisable recovery
  Errdisable Recovery Status:Enable

  Reason            Timer Status        Time
  ----------        ------------        -------
     loopguard              Enable          300
           ARP             Disable          300
          BPDU             Disable          300
          IGMP             Disable          300
  anti-arpscan             Disable          300
     bpduguard             Disable          300
          zuld             Disable          300

  Interfaces that will be enabled at the next timeout:

  Interface     Reason         Time left(sec)     Mode
  ---------     ----------     --------------     ---------------
sysname#
```

CHAPTER 26
Ethernet OAM Commands

26.1 IEEE 802.3ah Link Layer Ethernet OAM Overview

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.

26.2 Command Summary

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

Table 78 Interface Command Values

COMMAND	DESCRIPTION
port-list	A list of one or more ports, separated by commas with no spaces. The list may also contain ranges of ports signified by a hyphen. For example: 1,3,5–8,10.

The following section lists the commands for this feature.

Table 79 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
ethernet oam	Enables Ethernet OAM on the Switch.	C	13
no ethernet oam	Disables Ethernet OAM on the Switch.	C	13
ethernet oam remote-loopback start <*port*>	Initiates a remote-loopback test from the specified port by sending Enable Loopback Control PDUs to the remote device.	E	13

Table 79 ethernet oam Command Summary (continued)

COMMAND	DESCRIPTION	M	P
ethernet oam remote-loopback stop *<port>*	Terminates a remote-loopback test from the specified port by sending Disable Loopback Control PDUs to the remote device.	E	13
ethernet oam remote-loopback test *<port>* [*<number-of-packets>* [*<packet-size>*]]	Performs a remote-loopback test from the specified port. You can also define the allowable packet number and packet size of the loopback test frames.	E	13
interface port-channel *<port-list>*	Enters config-interface mode for the specified ports.	C	13
ethernet oam	Enables Ethernet OAM on the ports.	C	13
no ethernet oam	Disables Ethernet OAM on the ports.	C	13
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 ignore-rx	Sets the Switch to ignore loopback commands received on the ports.	C	13
ethernet oam remote-loopback supported	Enables the remote loopback feature on the ports.	C	13
no ethernet oam remote-loopback ignore-rx	Sets the Switch to process loopback commands received 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

26.3 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 80 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 80 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 81 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 81 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 82 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.
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.

CHAPTER 27
External Alarm Commands

27.1 Command Summary

Use these commands to configure the external alarm features on the Switch.

The following section lists the commands for this feature.

Table 83 external-alarm Command Summary

COMMAND	DESCRIPTION	M	P
external-alarm <*index*> name <*name_string*>	Sets the name of the specified external alarm. *index*: 1 – 4 *name_string*: Enters a name of up to 32 ASCII characters.	C	13
no external-alarm <*index*>	Removes the name of the specified external alarm.	C	13
no external-alarm all	Removes the name of all external alarms.	C	13
show external-alarm	Displays external alarm settings and status.	E	13

27.2 Command Examples

This example configures and shows the name and status of the external alarms.

```
sysname# configure
sysname(config)# external-alarm 1 name dooropen
sysname(config)# exit
sysname# show external-alarm
External Alarm 1

         Status: Not asserted
         Name: dooropen

External Alarm 2

         Status: Not asserted
         Name:

External Alarm 3

         Status: Not asserted
         Name:

External Alarm 4

         Status: Not asserted
         Name:
sysname#
```

CHAPTER 28
Flex Link Commands

28.1 Flex Link Overview

Use these commands to set up a backup link for a primary link on the Switch.

A flex link pair consists of a primary link and a backup link on a layer-2 interface. A primary link runs on a primary port; a backup link runs on a backup port. The ports have two states: FORWARDING and BLOCKING. When one link is up and running (port state: FORWARDING), the other link is in down or in standby mode (port state: BLOCKING). Only one port is forwarding traffic (FORWARDING) at a time. When the primary link goes down, the backup link automatically goes up and is able to forward traffic.

Preemption

Enable preemption to have the Switch automatically return the primary port to FORWARDING state after the primary port recovers from error state, and the backup port return to BLOCKING. The Switch will wait for the specified `preemption-delay` time before changing the primary port state to FORWARDING and backup port state to BLOCKING.

28.2 Command Summary

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

Table 84 Interface Command Values

COMMAND	DESCRIPTION
port-id	A port number on the Switch.

The following section lists the commands for this feature.

Table 85 flex link Command Summary

COMMAND	DESCRIPTION	M	P
`show flex-link`	Displays the flex link table. The ports in a flex link pair are either in one of the following states: Down: The link is down. Up: The link is up and the port state is FORWARDING. Standby: The link is up and the port state is BLOCKING.	E	3
`flex-link primary-port <port-id> backup-port <port-id> [preemption] [preemption-delay <time>]`	Creates a flex link pair. `preemption`: enables preemption on this flex link pair. When the primary port recovers from error state, the backup port state will change to BLOCKING and the primary port change to FORWARDING after the `preemption-delay` time. `preemption-delay`: sets the time you want the primary port to wait before changing back to FORWARDING state. *time*: 1 – 300 (seconds) Note: A port can only be in one flex link pair. Note: You can only configure up to five pairs of flex links. Note: The Flex Link, STP, Loop Guard, and Link Aggregation features are not allowed to be configured together on the same port.	C	13
`no flex-link primary-port <port-id> preemption`	Disables preemption on a specified flex link pair.	C	13
`no flex-link primary-port <port-id>`	Removes a specified flex link pair.	C	13

28.3 Command Example

In this example, we have **port 1** connected to server 1; **port 2** connected to server 2. We want to set **port 2** as a backup link for **port 1**. This way, we are able to link to server 2 when server 1 link is DOWN.

This example creates a flex link pair on the Switch, sets port 2 to be the backup link of port 1. This example also enables and sets the preemption delay time to 20 seconds on this flex link pair. You can see the primary link (**port 1**) is currently UP; the secondary link (**port 2**) is in standby mode.

```
sysname# config
sysname(config)# flex-link primary-port 1 backup-port 2 preemption
preemption-delay 20
sysname(config)# exit
sysname# show flex-link
  Index  Primary Port  Backup Port                              State
  -----  ------------  -----------  --------------------------------
      1             1            2     Primary Up / Backup Standby
sysname#
```

If primary link (**port 1**) goes DOWN, the secondary link (**port 2**) will automatically go UP.

```
sysname# show flex-link
  Index  Primary Port  Backup Port                              State
  -----  ------------  -----------  --------------------------------
      1             1            2     Primary Down / Backup Up
sysname#
```

When primary link (**port 1**) is again available, the primary link (**port 1**) will first be in standby mode for the preemption delay time (20 secs) interval.

```
sysname# show flex-link
  Index  Primary Port  Backup Port                              State
  -----  ------------  -----------  --------------------------------
      1             1            2     Primary Standby / Backup Up
sysname#
```

After 20 seconds, the primary link (**port 1**) will change to UP, and the secondary link (**port 2**) will go back to standby mode.

```
sysname# show flex-link
  Index  Primary Port  Backup Port                              State
  -----  ------------  -----------  --------------------------------
      1             1            2     Primary Up / Backup Standby
sysname#
```

CHAPTER 29
GARP Commands

29.1 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.

29.2 Command Summary

The following section lists the commands for this feature.

Table 86 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

29.3 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
```

CHAPTER 30
Green Ethernet Commands

30.1 Green Ethernet Overview

Green Ethernet reduces Switch port power consumption in the following ways.

- IEEE 802.3az Energy Efficient Ethernet (EEE)

  If EEE is enabled, both sides of a link support EEE and there is no traffic, the port enters Low Power Idle (LPI) mode. LPI mode turns off some functions of the physical layer (becomes quiet) to save power. Periodically the port transmits a REFRESH signal to allow the link partner keep the link alive. When there is traffic to be sent, a WAKE signal is sent to the link partner to return the link to active mode.
- Auto Power Down

  Auto Power Down turns off almost all functions of the port's physical layer functions when the link is down, so the port only uses power to check for a link up pulse from the link partner. After the link up pulse is detected, the port wakes up from Auto Power Down and operates normally.
- Short Reach

  Traditional Ethernet transmits all data with enough power to reach the maximum cable length. Shorter cables lose less power, so Short Reach saves power by adjusting the transmit power of each port according to the length of cable attached to that port.

Note: Not all Switches supports Green Ethernet completely. Some may only support EEE.

First configure Green Ethernet on the Switch, then configure it on an interface.

30.2 Command Summary

The following section lists the commands for this feature.

Table 87 green-ethernet Command Summary

COMMAND	DESCRIPTION	M	P
`green-ethernet auto-power-down`	Enables automatic power down on the Switch. Note: See Table 8 on page 13 for the products that support this command.	E	13
`no green-ethernet auto-power-down`	Disables automatic power down on the Switch.	E	13
`green-ethernet eee`	Enables IEEE 802.3az Energy Efficient Ethernet on the Switch. Note: See Table 8 on page 13 for the products that support this command.	E	13

Table 87 green-ethernet Command Summary (continued)

COMMAND	DESCRIPTION	M	P
no green-ethernet eee	Disables eee on the Switch.	E	13
green-ethernet short-reach	Enables adjusting the transmission power of each port according to the length of cable attached to a port on the Switch. Note: See Table 8 on page 13 for the products that support this command.	E	13
no green-ethernet short-reach	Disables short-reach on the Switch.	E	13
interface port-channel <*port-list*>	Enters config-interface mode for the specified ports.	C	13
green-ethernet auto-power-down	Enables automatic power down on the specified ports.	C	13
no green-ethernet auto-power-down	Disables automatic power down on the specified ports.	C	13
green-ethernet eee	Enables IEEE 802.3az Energy Efficient Ethernet on the specified ports.	C	13
no green-ethernet eee	Disable IEEE 802.3az Energy Efficient Ethernet on the specified ports.	C	13
green-ethernet short-reach	Enables adjusting the transmit power of the specified ports according to the length of cable attached to the port.	C	13
no green-ethernet short-reach	Disables adjusting the transmit power of the specified ports according to the length of cable attached to the port.	C	13
show green-ethernet auto-power-down	Shows automatic power down information.	E	3
show green-ethernet eee	Shows Energy Efficient Ethernet information.	E	3
show green-ethernet short-reach	Shows short reach information.	E	3

30.3 Green Ethernet Command Example

In this example, the Switch supports EEE and auto power down per port, and short reach globally. The following are explanations of the Status parameters:

EEE

- Active displays when EEE is enabled and the EEE port is up
- Inactive displays when EEE is enabled but the EEE port is down or the device connected to this port does not support EEE
- Unsupported means the Switch cannot display the status
- - means EEE is not enabled

Auto power down

- Normal means auto power down has not reduced the power on this link
- Power down means auto power down has reduced the power on this link
- Unsupported means the Switch cannot display the status
- - means auto power down is not enabled

Short reach

- Normal means short reach has not reduced the power on this link
- Low power means short reach has reduced the power on this link
- Unsupported means the Switch cannot display the status
- - means short reach is not enabled

```
sysname# configure
sysname(config)# green-ethernet eee
sysname(config)# green-ethernet short-reach
sysname(config)# green-ethernet auto-power-down
sysname(config)# interface port-channel 1-4
sysname(config-interface)# green-ethernet eee
sysname(config-interface)# green-ethernet auto-power-down
sysname(config-interface)# exit
sysname(config)# exit
sysname# show green-ethernet eee
  EEE globally configuration : Enable

  Port  Port status      Config   Status
  ----  --------------  -------  ---------
     1         100M/F     Enable       Active
     2           Down     Enable     Inactive
     3         100M/F     Enable  Unsupported
     4           Down    Disable            -

sysname# show green-ethernet auto-power-down
  Auto Power Down globally configuration : Enable

  Port  Config   Status
  ----  -------  ----------
     1   Enable    Power down
     2   Enable        Normal
     3   Enable   Unsupported
     4  Disable             -

sysname# show green-ethernet short-reach
  Short Reach globally configuration : Enable

sysname#
```

The following example shows how to configure short reach if the Switch supports short reach per port

```
sysname# configure
sysname(config)# green-ethernet short-reach

sysname# configure
sysname(config)# interface port-channel  1-4
sysname(config-interface)# green-ethernet short-reach
```

The following example shows the display for short reach if the Switch supports short reach per port and showing the status.

```
sysname# show green-ethernet short-reach
Global configuration : Enable

Port  Config        Status
----  -----------   --------------
   1   Enable         Low power
   2   Disable               -
   3   Enable       Unsupported
   4   Enable            Normal
```

CHAPTER 31
GVRP Commands

31.1 Command Summary

Use these commands to configure GVRP on the Switch.

The following section lists the commands for this feature.

Table 88 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 ports. The list must consist of one or more ports, separated by commas with no spaces. The list may also contain ranges of ports signified by a hyphen. For example: 1,3,5–8,10.	C	13
gvrp	Enables this function to permit VLAN groups beyond the local Switch.	C	13
no gvrp	Disable GVRP on the ports.	C	13

31.2 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

CHAPTER 32
HTTPS Server Commands

32.1 Command Summary

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

The following section lists the commands for this feature.

Table 89 https Command Summary

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

32.2 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 90 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.
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.

Table 90 show https (continued)

LABEL	DESCRIPTION
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 91 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.
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.

CHAPTER 33
Hardware Monitor Commands

33.1 Hardware Monitor Commands Overview

Use these commands to configure the hardware monitor feature on the Switch.

At the time of writing, the Switch only supports the SFP detect feature.

Note: See Table 8 on page 13 for the products that support the Hardware Monitor commands.

SFP Detect

When the SFP transceiver temperature exceeds the temperature threshold defined by the transceiver (see your transceiver documentation), the Switch automatically turns on the fans with maximum fan speed to cool down the system.

Note: The SFP detect feature only functions if at least one of your SFP transceiver(s) support DDMI (Digital Diagnostic Monitoring Interface). See the transceiver documentation.

33.2 Command Summary

Note: Not all models support these commands.

The following section lists the commands for this feature.

Table 92 hardware monitor Command Summary

COMMAND	DESCRIPTION	M	P
`hardware-monitor fan-control sfp-detect`	Enables Fan Control (SFP Detect) on the Switch. Note: The fans do not automatically turn off after the SFP transceiver temperature returns below threshold. To turn off the fans, you have to temporarily disable SFP detect (no `hardware-monitor fan-control sfp-detect`) or reboot the Switch.	C	13
`no hardware-monitor fan-control sfp-detect`	Disables Fan Control (SFP Detect) on the Switch.	C	13
`show hardware-monitor <C|F>`	Displays current hardware monitor information with the specified temperature unit (Celsius **C** or Fahrenheit **F**).	E	0

The following examples look at the current sensor readings from various places in the hardware. The display for your Switch may be different.

```
sysname# show hardware-monitor C

                     Customer Part
 PSU  Serial Number  Number & Revision  Manufacturing   Fan Air Flow
----  -------------  -----------------  ------------  -------------
PSU1    DIYD11M00CN                        20110124  front-to-back
PSU2    DIYD11M00DV                        20110125  front-to-back

Temperature Unit : (C)
Temperature(%c)  Current    Max    Min  Threshold  Status
---------------  -------  -----  -----  ---------  ------
            CPU     45.0   45.0   33.0       80.0  Normal
            MAC     47.0   47.0   32.0       90.0  Normal
           PHY1     45.0   45.0   31.0       90.0  Normal
           PHY2     45.0   45.0   32.0       90.0  Normal

FAN Speed(RPM)  Current    Max   Min  Threshold  Status
--------------  -------  -----  ----  ---------  ------
          FAN1     9360  15960  9360        500  Normal
          FAN2     9360  16320  9360        500  Normal
          FAN3     9360  15720  9360        500  Normal
          FAN4     9480  15240  9360        500  Normal

  FAN TRAY       Air Flow   Status
----------  -------------  -------
FAN TRAY 1  front-to-back  Present
FAN TRAY 2  front-to-back  Present

Voltage(V)  Current     Max     Min  Threshold  Status
----------  -------  ------  ------  ---------  ------
  12V_PSU1   11.737  11.918  11.737     +/-10%  Normal
  12V_PSU2   11.676  11.858  11.676     +/-10%  Normal
sysname#
```

```
sysname# show hardware-monitor C

  Temperature Unit : (C)
  Temperature(%c)  Current    Max    Min  Threshold  Status
  ---------------  -------  -----  -----  ---------  ------
          CPU/MAC     42.0   43.0   39.0       76.0  Normal
            BOARD     43.0   44.0   40.0      113.0  Normal
              PHY     43.0   44.0   39.0       99.0  Normal

  FAN Speed(RPM)  Current   Max   Min  Threshold  Status
  --------------  -------  ----  ----  ---------  ------
            FAN1     6561  6593  6498        500  Normal
            FAN2     6375  6405  6315        500  Normal
            FAN3     6257  6315  6228        500  Normal

   Voltage(V)  Current     Max     Min  Threshold  Status
  -----------  -------  ------  ------  ---------  ------
  1.88V_84887    1.920   1.920   1.920    +4%/-4%  Normal
     1V_84888    1.013   1.013   1.013    +5%/-5%  Normal
        1.88V    1.907   1.907   1.907    +4%/-4%  Normal
         1.0V    1.025   1.037   1.025    +5%/-5%  Normal
         1.8V    1.803   1.803   1.803    +6%/-6%  Normal
      1.0V_H3    1.025   1.025   1.025    +5%/-5%  Normal
      1V5_DDR    1.490   1.490   1.490    +6%/-6%  Normal
      VTT_DDR    0.744   0.744   0.744    +5%/-5%  Normal
         3.3V    3.274   3.274   3.274    +6%/-6%  Normal
         2.5V    2.565   2.565   2.539    +6%/-6%  Normal
          12V   11.656  11.656  11.656  +10%/-20%  Normal

  Power Supply  Status
  ------------  ------
         PSU_1  Active
         PSU_2     N/A
sysname#
```

The following table describes the labels in this screen.

Table 93 show hardware-monitor

LABEL	DESCRIPTION
Customer Part	This displays information on the fan and power module kits installed in the Switch.
PSU	The PSU (Power Supply Unit) is the power module number.
Serial Number	This is a unique number that identifies the inserted power module.
Number & Revision	This is the customer part number and revision.
Manufacturing	This is the date (yyyy-mm-dd) the module was assembled.
Fan Air Flow	This displays the power module fan air flow. All fan air flows within a Switch must be consistent, that is either front-to-back or back-to-front.
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.

Table 93 show hardware-monitor (continued)

LABEL	DESCRIPTION
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.
FAN TRAY	This is the is the fan module number
Air Flow	This displays the fan module fan air flow. All fan air flows within a Switch must be consistent, that is either front-to-back or back-to-front.
Status	This displays whether the fan module is inserted (Present) or not (Absent).
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.
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.
Power Supply	This field lists the power supply modules installed in the Switch.
Status	If the Switch supports two hot-swappable power supply modules and both can supply power to the Switch simultaneously. • **Normal** indicates that the Switch is currently operating from the power source to which the inserted power module is connected. • **Error** indicates that the power module is inserted and connected to a power source but it is not in normal operation. • **Absent** indicates that you did not insert the power module. • **Present** indicates that you inserted the power module, but it is not connected to a power source and there is no available power. If the Switch comes with two built-in power supply modules but only one can supply power to the Switch at a time, • **Active** indicates the Switch is currently operating from the power source to which the power module is connected. • **Standby** indicates the power module is connected to a power source but the Switch is NOT operating from it. • **N/A** is displayed when the power module is not connected to a power source and there is no available power.

CHAPTER 34 IGMP and Multicasting Commands

34.1 IGMP and Multicasting Overview

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.

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.

34.2 Command Summary

The following section lists the commands for this feature.

Table 94 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
`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

Table 94 IGMP Command Summary (continued)

COMMAND	DESCRIPTION	M	P
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 <1-65535>	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
show ip igmp group	Displays the Multicast groups learned by IGMP.	E	3
show ip igmp interface	Displays the IGMP status information per interface.	E	3
show ip igmp multicast	Displays the Multicast traffic information.	E	3
show ip igmp timer	Displays the IGMP timer settings.	E	3
show router igmp	Displays global IGMP settings.	E	3

Table 95 IPMC Command Summary

COMMAND	DESCRIPTION	M	P
interface port-channel *<port-list>*	Enters config-interface mode for the specified ports. The port list must consist of one or more ports, separated by commas with no spaces. The list may also contain ranges of ports signified by a hyphen. For example: 1,3,5–8,10.	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

34.3 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
```

CHAPTER 35
IGMP Snooping Commands

35.1 IGMP Snooping Overview

IGMP snooping allows the Switch to learn about Multicast groups without you having to manually configure them. The Switch inspects IGMP packets sent between IP Multicast routers, switches, and hosts, determines each device's Multicast group, and then creates a map of Multicast groups to switch ports.

After the Switch has created the Multicast map, it only broadcasts Multicast group traffic to ports that are members of that group. This significantly reduces Multicast traffic passing the Switch.

35.2 Command Summary

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

Table 96 Interface Command Values

COMMAND	DESCRIPTION
port-list	A list of one or more ports, separated by commas with no spaces. The list may also contain ranges of ports signified by a hyphen. For example: 1,3,5–8,10.

The following section lists the commands for this feature.

Table 97 igmp-flush Command Summary

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

Table 98 igmp-snooping Command Summary

COMMAND	DESCRIPTION	M	P
`clear igmp-snooping statistics all`	Removes all Multicast statistics of the Switch.	E	3
`clear igmp-snooping statistics port`	Removes the Multicast statistics of the ports.	E	3
`clear igmp-snooping statistics system`	Removes the Multicast statistics of the Switch.	E	3
`clear igmp-snooping statistics vlan`	Removes the Multicast statistics of the Multicast VLANs.	E	3
`igmp-snooping`	Enables IGMP snooping.	C	13
`no igmp-snooping`	Disables IGMP snooping.	C	13

Table 98 igmp-snooping Command Summary (continued)

COMMAND	DESCRIPTION	M	P
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 authentication-timeout <0-3000>	Sets how long the Switch waits before sending the same access request again if the AAA server rejects the host's request to join a Multicast group.	C	13
no igmp-snooping authentication-timeout	Resets the authentication timeout value to its default setting.	C	13
igmp-snooping filtering	Enables IGMP filtering on the Switch. Ports can only join Multicast groups specified in their IGMP filtering profile.	C	13
igmp-snooping filtering profile <*name*> start-address <*ip*> end-address <*ip*>	Sets the range of Multicast addresses in a profile. *name*: 1 – 32 alphanumeric characters	C	13
no igmp-snooping filtering	Disables IGMP filtering on the Switch.	C	13
no igmp-snooping 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-snooping filtering profile <*name*> start-address <*ip*> end-address <*ip*>	Clears the specified rule of the specified IGMP filtering profile.	C	13
igmp-snooping host-timeout <1-16711450>	Sets the host timeout value.	C	13
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
igmp-snooping querier version <v2|v3>	Sets the type of queries that the switch sends when the IGMP snooping querier is enabled. Select **v2** to have the Switch send IGMPv2 queries only. Select **v3** to have the Switch send IGMPv3 queries only. Note: IGMP snooping query works only when both host and Switch support the same IGMP version.	C	13
igmp-snooping querier query-interval <1-65535>	Enter the period in seconds between each IGMP snooping query to hosts in the network to determine whether they still need to receive multicast traffic.	C	13
igmp-snooping report-proxy	Enables IGMP snooping report-proxy mode. In this mode, the Switch acts as an IGMP v1/v2 report proxy. The Switch not only checks IGMP packets between Multicast routers/switches and Multicast hosts to learn the Multicast group membership, but also replaces the source MAC address in an IGMP v1/v2 report with its own MAC address before forwarding to the Multicast router/switch. When the Switch receives more than one IGMP v1/v2 join reports that request to join the same Multicast group, it only sends a new join report with its MAC address. This helps reduce the number of multicast join reports passed to the Multicast router/switch.	C	13

Table 98 igmp-snooping Command Summary (continued)

COMMAND	DESCRIPTION	M	P
no igmp-snooping report-proxy	Disables IGMP snooping report-proxy mode. In this mode, the Switch just snoops on and sends the Multicast router/switch all IGMP join messages without changing their source MAC addresses, and forwards Multicast traffic to the hosts.	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 smart-forward	Enables sending of Multicast frames to querier port and IGMP subscriber groups. Otherwise, the querier port forwards the frames only when it receives a join report and it belongs to the IGMP group.	C	13
no igmp-snooping smart-forward	Disables igmp snooping smart forwarding.	C	13
igmp-snooping unknown-multicast-frame <drop|flooding>	Sets how to treat traffic from unknown Multicast groups.	C	13
igmp-snooping unknown-multicast-frame drop [vlan <*vlan-list*>]	Sets the Switch to discard the frame on all VLANs or on the specified VLANs when it receives an unknown Multicast frame.	C	13
igmp-snooping unknown-multicast-frame flooding	Sets the Switch to send the frame to all ports when it receives an unknown Multicast frame.	C	13
igmp-snooping unknown-multicast-frame querier-port drop	Sets the Switch to not send the frame to any querier port when it receives an unknown Multicast frame. Note: This command works only when the igmp-snooping unknown-multicast-frame drop command is executed to discard the unknown Multicast frames.	C	13
igmp-snooping unknown-multicast-frame querier-port forwarding [vlan <*vlan-list*>]	Sets the Switch to send the frame to all querier ports or the ports which are used as an IGMP query port on the specified VLANs when it receives an unknown Multicast frame. Note: This command works only when the igmp-snooping unknown-multicast-frame drop command is executed to discard the unknown Multicast frames.	C	13
show igmp-snooping	Displays global IGMP snooping settings.	E	3
show igmp-snooping filtering profile	Displays IGMP filtering profile settings.	E	3
show igmp-snooping group all	Displays all Multicast group information.	E	3
show igmp-snooping group client < [vlan <*vlan-list*>] [interface port-channel <*port-list*>] [multicast-group <*group-address*>] >	Displays client IP information for the specified Multicast VLANs, ports and/or Multicast groups.	E	3
show igmp-snooping group client all	Displays client IP information for all Multicast groups on the Switch.	E	3
show igmp-snooping group count	Displays the total number of the Multicast groups on the Switch.	E	3

Table 98 igmp-snooping Command Summary (continued)

COMMAND	DESCRIPTION	M	P
show igmp-snooping group interface port-channel *<port-list>*	Displays the Multicast groups to which the specified ports belongs.	E	3
show igmp-snooping group interface port-channel *<port-list>* count	Displays the number of the Multicast groups to which the specified ports belongs.	E	3
show igmp-snooping group vlan *<vlan-list>*	Displays the Multicast groups for the specified Multicast VLANs.	E	3
show igmp-snooping group vlan *<vlan-list>* count	Displays the number of the Multicast groups for the specified Multicast VLANs.	E	3
show igmp-snooping querier	Displays the IGMP query mode for the ports on the Switch.	E	3
show igmp-snooping statistics interface port-channel *<port-list>*	Displays the Multicast statistics of the specified ports.	E	3
show igmp-snooping statistics system	Displays the Multicast statistics of the Switch.	E	3
show igmp-snooping statistics vlan *<vlan-list>*	Displays the Multicast statistics of the specified Multicast VLANs.	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

Table 99 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 VLANs. 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 100 interface igmp Command Summary

COMMAND	DESCRIPTION	M	P
show interfaces config <*port-list*> igmp-snooping filtering	Displays the names of the IGMP filtering profiles used for the specified ports.	E	3
show interfaces config <*port-list*> igmp-snooping group-limited	Displays whether the group limit is enabled and the maximum number of the Multicast groups the specified ports is allowed to join.	E	3
show interfaces config <*port-list*> igmp-snooping leave-mode	Displays the IGMP leave mode of the specified ports.	E	3
show interfaces config <*port-list*> igmp-snooping query-mode	Displays the IGMP querier mode of the specified ports.	E	3
interface port-channel <*port-list*>	Enters config-interface mode for the specified ports.	C	13
igmp-snooping authentication	Enables IGMP snooping authentication on the ports. When a Multicast host (connected to the specified ports) sends a message to join a Multicast group, the Switch sends an access request (that conatins the host identification information) to an AAA server before forwarding the join message to the Multicast router/switch. The Switch learns the Multicast group membership when the AAA server returns an access-accept. If the AAA server returns an access-reject, the Switch will not learn the Multicast group membership, nor process the packet further. If the Multicast group and port has already been learned, the Switch will not do the authentication again.	C	13
igmp-snooping fast-leave-timeout <200-6348800>	This defines how many seconds the Switch waits for an IGMP report before removing an IGMP snooping membership entry when an IGMP leave message is received on this port from a host.	C	13
igmp-snooping filtering profile <*name*>	Assigns the specified IGMP filtering profile to the ports. If IGMP filtering is enabled on the Switch, the ports can only join the Multicast groups in the specified profile.	C	13
igmp-snooping group-limited	Enables the group limiting feature for IGMP snooping. You must enable IGMP snooping as well.	C	13
igmp-snooping group-limited action <deny|replace>	Sets how the Switch deals with the IGMP reports when the maximum number of the IGMP groups a port can join is reached. deny: The Switch drops any new IGMP join report received on this port until an existing Multicast forwarding table entry is aged out. replace: The Switch replaces an existing entry in the Multicast forwarding table with the new IGMP reports received on this port.	C	13
igmp-snooping group-limited number <*number*>	Sets the maximum number of Multicast groups allowed. *number*: 0 – 255	C	13
igmp-snooping leave-mode <normal|immediate|fast>	Sets the Switch to remove an IGMP snooping membership entry immediately (immediate) or wait for an IGMP report before the normal (normal) or fast (fast) leave timeout when an IGMP leave message is received on this port from a host.	C	13

Table 100 interface igmp Command Summary (continued)

COMMAND	DESCRIPTION	M	P
igmp-snooping leave-timeout <200-6348800>	This defines how many seconds the Switch waits for an IGMP report before removing an IGMP snooping membership entry when an IGMP leave message is received on this port from a host.	C	13
igmp-snooping querier-mode <auto|fixed|edge>	Specifies whether or not and under what conditions the ports is (are) IGMP query ports. 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 ports as IGMP query ports. Select this when you connect an IGMP Multicast server to the ports. 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
no igmp-snooping authentication	Disables IGMP snooping authentication on the ports. The Switch directly forwards the host's join message to the Multicast router without sending an access request to the AAA server for authentication.	C	13
no igmp-snooping filtering profile	Prohibits the ports from joining any Multicast groups if IGMP filtering is enabled on the Switch.	C	13
no igmp-snooping group-limited	Disables Multicast group limits.	C	13

35.3 Command Examples

This example enables IGMP snooping on the Switch, sets the `host-timeout` value to 30 seconds, and sets the Switch to drop packets from unknown Multicast groups on VLAN 1 and VLAN2. The unknown Multicast frames will be forwarded to other VLANs.

```
sysname(config)# igmp-snooping
sysname(config)# igmp-snooping host-timeout 30
sysname(config)# igmp-snooping unknown-multicast-frame drop vlan 1-2
```

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-snooping group-limited
sysname(config-interface)# igmp-snooping group-limited number 5
sysname(config-interface)# exit
sysname(config)# exit
sysname# show interfaces config 1 igmp-snooping 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 101 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
```

This example restricts ports 1 – 4 to Multicast IP addresses 224.255.255.0 through 225.255.255.255.

```
sysname# configure
sysname(config)# igmp-snooping filtering
sysname(config)# igmp-snooping 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-snooping filtering profile example1
sysname(config-interface)# exit
sysname(config)# exit
```

This example enables IGMP Snooping and the IGMP Snooping querier, and then sets the IGMP Snooping Querier version to IGMPv2.

```
sysname# configure
sysname(config)# igmp-snooping
sysname(config)# igmp-snooping querier
sysname(config)# igmp-snooping querier version v2
sysname(config)# igmp-snooping querier query-interval 160
sysname(config)# exit
sysname# show igmp-snooping
  IGMP Snooping                          : Enable
  802.1P Priority                        : No-Change
  Host Timeout                           : 260
  Unknown Multicast Frame                : Flooding
  Unknown Multicast Frame to Querier Port: Drop
  Reserved Multicast Frame               : Flooding
  IGMP Snooping Querier Mode             : Enable
  IGMP Snooping Querier Version          : v2
  IGMP Snooping Querier Query-Interval   : 160
  IGMP Snooping Smart Forward            : Enable
  IGMP Snooping Querier Timer            :
```

CHAPTER 36
Interface Commands

36.1 Command Summary

Use these commands to configure basic port settings.

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

Table 102 Interface Command Values

COMMAND	DESCRIPTION
port-list	A list of one or more ports, separated by commas with no spaces. The list may also contain ranges of ports signified by a hyphen. For example: 1,3,5–8,10.

The following section lists the commands for this feature.

Table 103 interface Command Summary

COMMAND	DESCRIPTION	M	P
`clear interface <port-num>`	Clears all statistics for the specified port.	E	13
`interface port-channel <port-list>`	Enters config-interface mode for the specified ports.	C	13
`bpdu-control <peer|tunnel|discard|network>`	Sets how Bridge Protocol Data Units (BPDUs) are used in STP port states. `peer`: process any BPDU (Bridge Protocol Data Units) received on this port. `tunnel`: forward BPDUs received on this port. `discard`: drop any BPDU received on this port. `network`: process a BPDU with no VLAN tag and forward a tagged BPDU.	C	13
`cx4-length <0.5|1|3|5|10|15>`	Sets the number of meters for the length of the 10GBASE-CX4 cable you use to connect between the Switch and another switch for stacking.	C	13
`flow-control [tx] [rx]`	Enables interface flow control. Flow control regulates transmissions to match the bandwidth of the receiving port. `tx`: Allow the Switch port to send pause signal to the connected device. `rx`: Allow the connected device to send a pause signal to the Switch. The Switch will temporarily stop sending signals.	C	13

Table 103 interface Command Summary (continued)

COMMAND	DESCRIPTION	M	P
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
inactive	Disables the specified ports on the Switch.	C	13
media-type 10g <SFP+|DAC10G>	Sets the media type of the SFP+ module that is attached to the 10 Gigabit interface. On the Switch that has a 10 Gigabit interface, such as the SFP+ slot, you can insert either an SFP+ transceiver or an SFP+ Direct Attach Copper (DAC). An SFP+ Direct Attach Copper (DAC) is an SFP+ housing that has no optical module but uses a fixed-length passive copper cable assembly, which reduces cost and power significantly.	C	13
name <*port-name-string*>	Sets a name for the ports. *port-name-string*: Up to 128 English keyboard characters except [?], [|], ['], ["], [space], or [,].	C	13
no flow-control	Disables flow control on the ports.	C	13
no inactive	Enables the ports on the Switch.	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
qos priority <0-7>	Sets the quality of service priority for an interface.	C	13
speed-duplex <auto|auto-1G|10-half|10-full|10-an|100-half|100-full|100-an|1G-full|2.5G-full|5G-full|10G-full|12G-full|25G-full|25G-an|40G-full|100G-full|100G-an>	Sets the port duplex mode to half or full, and the speed of the port to: 10, 100, 1,000, 2,500, 5,000, 10,000, 12,000, 25,000, 40,000, or 100,000 Mbps. Select auto (auto-negotiation) to let the specified ports negotiate with a peer to obtain the connection speed and duplex mode. Select 10-an, 100-an, 25G-an, 100G-an, or auto-1G to let the specified ports automatically negotiate with an upper limit of 10 Mbps, 100 Mbps, 25,000 Mbps, or 100,000 Mbps respectively. Use these commands if you want to use automatic negotiation while also limiting the port speed. Note: The settings available for each port varies depending on the port type and switch model. Note: The actual speeds that the port can reach depends on the cable type and length. For details, see the Multi-Gigabit section in the Switch User's Guide.	C	13

Table 103 interface Command Summary (continued)

COMMAND	DESCRIPTION	M	P
fec <auto|cl74|cl91|cl108|none>	Set the same FEC (Forward Error Correction) type between the Switch and the connected device to minimize signal degradation of data at high transmission speeds (for example, 25 Gbps or 100 Gbps). Select auto to allow both connected ports to automatically set the FEC type according to the following rules: • For 10G transceivers, the FEC type on the port will automatically be none. • For 25G transceivers, the FEC type on the port will automatically be cl108. • For 100G transceivers, the FEC type on the port will automatically be none if the transceiver type is 100G LR4/ER4; all other types of transceiver will automatically be cl91. Select cl74 when both connected ports support 25 Gbps speed and require low latency in data transmission. Select cl91 when both connected ports support 25 Gbps and 100 Gbps speeds. Select cl108 when both connected ports support 25 Gbps speed but low latency in data transmission is not required. Alternatively, select none when you do not need to set the FEC type.	C	13
no interface <*port-num*>	Resets the port counters for the specified ports.	E	13
show interfaces <*port-list*>	Displays the current interface status for the specified ports.	E	3
show interfaces <*port-list*> | begin <*string*>	Displays the current interface status and statistics for the specified ports, which start from a line with the specified string.	E	3
show interfaces <*port-list*> | begin <*string1*> include <*string2*>	Displays the current interface status and statistics for the specified ports, which start from a line with the first specified string and also contain the second specified string.	E	3
show interfaces <*port-list*> | include <*string*>	Displays the current interface status and statistics for the specified ports, which contain the specified string.	E	3
show interfaces <*port-list*> | refresh	Displays the current interface status and statistics for the specified ports, and updates every second until you press the [ESC] button.	E	3
show interfaces config <*port-list*>	Displays current interface configuration for the specified ports.	E	3
show interfaces utilization	Displays the percentage of actual transmitted and received frames on a port as a percentage of the link speed.	E	3
show interfaces utilization | begin <*string*>	Displays the link speed and percentage of actual transmitted and received frames on a port, which start from a line with the specified string.	E	3
show interfaces utilization | begin <*string1*> include <*string2*>	Displays the link speed and percentage of actual transmitted and received frames on a port, which start from a line with the first specified string and also contain the second specified string.	E	3

Table 103 interface Command Summary (continued)

COMMAND	DESCRIPTION	M	P
show interfaces utilization | include <*string*>	Displays the link speed and percentage of actual transmitted and received frames on a port, which contain the specified string.	E	3
show interfaces utilization | refresh	Displays the link speed and percentage of actual transmitted and received frames on a port, and updates every second until you press the [ESC] button.	E	3

36.2 Command Examples

This example looks at the current status of port 1.

```
sysname# show interfaces config 1-5
Port Configurations:
  Port No       :1
    Active      :Yes
    Name        :
    PVID        :1                    Flow Control    :Rx
    Type        :100M/1G              Speed/Duplex    :auto
    BPDU        :peer                 802.1p Priority :0

  Port No       :2
    Active      :Yes
    Name        :
    PVID        :1                    Flow Control    :Tx
    Type        :100M/1G              Speed/Duplex    :auto
    BPDU        :peer                 802.1p Priority :0

  Port No       :3
    Active      :Yes
    Name        :
    PVID        :1                    Flow Control    :Tx Rx
    Type        :100M/1G              Speed/Duplex    :auto
    BPDU        :peer                 802.1p Priority :0

  Port No       :4
    Active      :Yes
    Name        :
    PVID        :1                    Flow Control    :Tx Rx
    Type        :100M/1G              Speed/Duplex    :auto
    BPDU        :peer                 802.1p Priority :0

  Port No       :5
    Active      :Yes
    Name        :
    PVID        :1                    Flow Control    :Disable
    Type        :100M/1G              Speed/Duplex    :auto
    BPDU        :peer                 802.1p Priority :0
```

The following table describes the labels in this screen.

Table 104 show interfaces

LABEL	DESCRIPTION
Port Info	
Port NO.	This field displays the port number you are viewing.
Link	This field displays the speed (either **10M** for 10 Mbps, **100M** for 100 Mbps, **1G** for 1 Gbps, **2.5G** for 2.5 Gbps, **5G** for 5 Gbps, **10G** for 10 Gbps, **25G** for 25 Gbps, or **100G** for 100 Gbps) 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.	
Unicast	This field shows the number of good unicast packets 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.
Tagged	This field shows the number of packets with VLAN tags transmitted.
Rx Packet The following fields display detailed information about packets received.	
Unicast	This field shows the number of good unicast packets 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.
Control	This field shows the number of control packets received (including those with CRC error) but it does not include the 802.3x Pause packets.
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.

Table 104 show interfaces (continued)

LABEL	DESCRIPTION
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) errors.
Runt	This field shows the number of packets received that were too short (shorter than 64 octets), including the ones with CRC errors.
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 (including bad packets) received that were between 1519 octets and the maximum frame size. The maximum frame size varies depending on your Switch model. See Product Specification chapter in your User's Guide.

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
```

This example enables the CL91 forwarding error correction.

```
sysname (config)# interface port-channel 1
sysname (config-interface)# fec cl91
sysname (config-interface)# exit
sysname (config)# exit
```

This example disables forwarding error correction.

```
sysname (config)# interface port-channel 1
sysname (config-interface)# fec none
sysname (config-interface)# exit
sysname (config)# exit
```

CHAPTER 37
Interface Loopback Mode

37.1 Loopback Interface Overview

Use these commands to configure a loopback interface for the Switch.
The loopback interface is a virtual interface which can be assigned an IP address and used by routing protocols. The loopback interface does not need to be connected to any devices and will always be available if the Switch is functioning normally and connected to a network. You can enable multiple loopback interfaces on the Switch, and each loopback interface must be uniquely identified. The Switch can use a loopback interface address as the source address of all packets that originate from the Switch. Filters can then be applied to the loopback address to protect the system.

37.2 Command Summary

The following section lists the commands for this feature.

Table 105 Interface Loopback Command Summary:

COMMAND	DESCRIPTION	M	P
`interface loopback <0-x>`	Sets a number for this loopback interface configuration. Note: 'x' depends on your Switch model.	C	13
`no interface loopback <0-x>`	Resets the loopback interface configuration for the specified numbers.	C	13
`inactive`	Disables the specified loopback interface.	C	13
`no inactive`	Enables the specified loopback interface.	C	13
`ip address <ip-address> <mask>`	Sets the IP address and subnet mask of the Switch in the specified loopback interface.	C	13
`no ip address <ip-address> <mask>`	Deletes the IP address and subnet mask from this loopback interface.	C	13
`name <name>`	Sets a descriptive name of the loopback interface setting for identification purposes.	C	13
`show interface loopback`	Displays current IPv4 loopback interfaces you configured.	E	3
`show interface loopback <0-x>`	Displays the IPv4 loopback interface configuration for the specified numbers.	E	3

37.3 Command Examples

This example configures IPv4 loopback interface on the Switch with the following settings:

- Enter the configuration mode.
- Create the loopback interface 0 with IP address 192.168.2.1, subnet mask 255.255.255.0, name loopback0 and interface status.

```
sysname# config
sysname(config)# interface loopback 0
sysname(config-if)# inactive
sysname(config-if)# ip address 192.168.2.1 255.255.255.0
sysname(config-if)# name loopback0
sysname(config-if)# exit
sysname(config)# exit
sysname# show interface loopback 0
```

CHAPTER 38 Interface Route-domain Mode

38.1 Command Summary

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

The following section lists the commands for this feature.

Table 106 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 8's together and you get the bit number (24).	C	13
`exit`	Exits from the interface routing-domain configuration mode.	C	13

38.2 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)#
```

CHAPTER 39
IP Commands

39.1 IP Commands Overview

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

Note: See Chapter 86 on page 346 for static route commands.

Note: See Chapter 40 on page 148 for IP source binding commands.

39.2 Command Summary

The following section lists the commands for this feature.

Table 107 ip Command Summary

COMMAND	DESCRIPTION	M	P
`show ip`	Displays current IPv4 interfaces.	E	0
`show ipv6`	Displays current IPv6 interfaces.	E	0
`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

Table 107 ip Command Summary (continued)

COMMAND	DESCRIPTION	M	P
ip iptable hash <crc32l|crc32u|crc16l|crc16u|crc16|lsb>	Sets the hash algorithm that the Switch uses to generate keys for searching the hardware IP table. Certain network configurations might require a specific algorithm to reduce IP address hash collisions. Select from the following algorithms: • **crc32l**: Cyclic redundancy check 32-lower • **crc32u**: Cyclic redundancy check 32-upper • **crc16l**: Cyclic redundancy check 16-lower • **crc16u**: Cyclic redundancy check 16-upper • **crc16**: Cyclic redundancy check 16 (hardware support) • **lsb**: Least significant bit Note: You should not change the default hash algorithm unless you have a specific reason. Note: Supported algorithms vary depending on the switch model. To view which algorithms your switch supports, run the command: ip iptable hash help. Note: After running this command, the CLI might become temporarily unresponsive.	C	13
ip name-server <*ip*|*ipv6*>	Sets the IPv4 and/or IPv6 addresses of the domain name servers.	C	13
no ip name-server <all|*ip*|*ipv6*>	Removes all or the specified DNS server.	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
show ip name-server	Displays the DNS server addresses on the Switch.	E	3

Table 108 tcp and udp Command Summary

COMMAND	DESCRIPTION	M	P
show ip tcp	Displays IP TCP information.	E	3
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 39.3 on page 144 for an example.	E	13

39.3 Command Examples

This example sets the hash algorithm of a XS3800 model switch to crc16l.

```
sysname# configure
sysname(config)# ip iptable hash help

[<crc32l|crc32u|crc16l|crc16u|lsb>]

sysname(config)# ip iptable hash crc16l
```

This example configures two DNS server addresses and displays the settings.

```
sysname# configure
sysname(config)# ip name-server 10.1.2.3 2001::123
sysname# show ip name-server
  Name Server Table:
  Server Address  Source
  --------------  ------
        10.1.2.3  Static
       2001::123  Static
sysname#
```

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

```
sysname# show ip tcp
( 1)tcpRtoAlgorithm              4     ( 2)tcpRtoMin                    30
( 3)tcpRtoMax              6400000     ( 4)tcpMaxConn           4294967295
( 5)tcpActiveOpens               0     ( 6)tcpPassiveOpens              0
( 7)tcpAttemptFails              0     ( 8)tcpEstabResets               0
( 9)tcpCurrEstab                 0     (10)tcpInSegs                    0
(11)tcpOutSegs                   0     (12)tcpRetransSegs               0
(14)tcpInErrs                    0     (15)tcpOutRsts                   0
(17)tcpHcInSegs                  0     (18)tcpHcOutSegs                 0
   &TCB Rcv-Q Snd-Q Rcv-Wnd Snd-Wnd Local socket        Remote socket
State
82ca2290    0    0    128      1  0.0.0.0:22          0.0.0.0:0
Listen
82ca2058    0    0   22400     1  0.0.0.0:443         0.0.0.0:0
Listen (S)
82c92130    0    0   16384     1  0.0.0.0:21          0.0.0.0:0
Listen
82c92014    0    0   16384     1  0.0.0.0:80          0.0.0.0:0
Listen (S)
82c91ef8    0    0    128      1  0.0.0.0:23          0.0.0.0:0
Listen (S)
82e0cb5c    0    0      0      0  :::443              :::0
Listen (S)
82e04b10    0    0      0      0  :::21               :::0
Listen
82e04934    0    0      0      0  :::80               :::0
Listen (S)
82e04758    0    0      0      0  :::23               :::0
Listen (S)
```

The following table describes the labels in this screen.

Table 109 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.
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.

Table 109 show ip tcp (continued)

LABEL	DESCRIPTION
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 in a 32-bit count, including those received in error. This count includes segments received on currently established connections.
tcpOutSegs	This field displays the total number of segments sent in a 32-bit count, 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.
tcpHcInSegs	This field displays the total number of segments received in a 64-bit count, including those received in error. This count includes segments received on currently established connections.
tcpHcOutSegs	This field displays the total number of segments sent in a 64-bit count, including those on current connections but excluding those containing only retransmitted octets.
	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.
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              0     ( 2)udpNoPorts                  0
( 3)udpInErrors                 0     ( 4)udpOutDatagrams             0
( 8)udpHcInDatagrams            0     ( 9)udpHcOutDatagrams           0
    &UCB Rcv-Q  Local socket
82398cac     0  0.0.0.0:68
82398c50     0  0.0.0.0:67
82392d70     0  0.0.0.0:161
822ae07c     0  0.0.0.0:1026
822ae020     0  0.0.0.0:1025
822aa41c     0  0.0.0.0:1024
822aa3c0     0  0.0.0.0:53
822aa364     0  0.0.0.0:69
822a9e5c     0  0.0.0.0:263
82adabf8     0  :::161
```

The following table describes the labels in this screen.

Table 110 show ip udp

LABEL	DESCRIPTION
udpInDatagrams	This field displays the total number of UDP datagrams in a 32-bit count 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 in a 32-bit count sent by the Switch.
udpHcInDatagrams	This field displays the total number of UDP datagrams in a 64-bit count delivered to UDP users.
udpHcOutDatagrams	This field displays the total number of UDP datagrams in a 64-bit count 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.

CHAPTER 40
IP Source Binding Commands

40.1 Command Summary

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

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

Table 111 Interface Command Values

COMMAND	DESCRIPTION
port-list	A list of one or more ports, separated by commas with no spaces. The list may also contain ranges of ports signified by a hyphen. For example: 1,3,5–8,10.

The following section lists the commands for this feature.

Table 112 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 arp-freeze	Create static bindings from any previously learned ARP entries in the Switch's ARP table and add them in the IP source guard static binding table.	C	13
ip source binding arp-freeze interface port-channel <*port-list*>	Create static bindings from previously learned ARP entries containing the specified port number and add them in the IP source guard static binding table.	C	13
ip source binding arp-freeze vlan <*vlan-list*>	Create static bindings from previously learned ARP entries containing the specified VLAN ID and add them in the IP source guard static binding table.	C	13
ip source binding ip <*ip*> vlan <*vlan-id*> [interface port-channel <*interface-id*>]	Creates a static binding that applies to all MAC addresses.	C	13
no ip source binding ip <*ip*>	Removes the specified static binding that applies to all MAC addresses.	C	13

Table 112 ip source binding Command Summary (continued)

COMMAND	DESCRIPTION	M	P
ip source binding ip <*ip*> vlan <*vlan-id*> mac <*mac-addr*> [interface port-channel <*interface-id*>]	Creates a static binding that applies to a specific MAC address.	C	13
no ip source binding ip <*ip*> vlan <*vlan-id*> mac <*mac-addr*>	Removes the specified static binding that applies to a specific MAC address.	C	13

40.2 Command Examples

This example shows the current binding table.

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

The following table describes the labels in this screen.

Table 113 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).
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.

CHAPTER 41
IP Source Guard

41.1 IP Source Guard Overview

IP source guard uses a binding table to distinguish between authorized and unauthorized ARP packets in your network. A binding table entry contains these key attributes:

- MAC address
- VLAN ID
- IP address
- Port number

IP source guard consists of the following features:

- Static bindings. Use this to create static bindings in the binding table.
  For details, see Chapter 40 on page 148.
- DHCP snooping. Use this to filter unauthorized DHCP packets on the network and to build the binding table dynamically.
  For details, see Chapter 21 on page 82.
- ARP inspection. Use this to filter unauthorized ARP packets on the network.
  For details, see Chapter 8 on page 40.

41.2 IP Source Guard Security Mode

When ARP inspection is enabled, a malicious device can avoid detection by not sending any ARP packets. The device can then send malicious non-ARP packets through the Switch.

To prevent this, by default the Switch drops all non-ARP/DHCP packets from a MAC address that is not in the binding table. You can change this default behavior by changing the IP Source Guard security mode.

Table 114 ip source guard security mode Command Summary

COMMAND	DESCRIPTION	M	P
`ip source guard mode <strict|loose>`	Sets the IP Source Guard security mode. **Strict**: The Switch drops all packets from a MAC address that is not in the dynamic or static binding table. This is the default setting. **Loose**: The Switch forwards packets from a MAC address that is not in the dynamic or static binding table.	C	13

In this example, we set the IP Source Guard Security mode to Loose, and then display the setting.

```
sysname# configure
sysname(config)# ip source guard mode loose
sysname# exit
sysname# show run
ip source guard mode loose
```

CHAPTER 42
IPv6 Commands

42.1 IPv6 Overview

IPv6 (Internet Protocol version 6), is designed to enhance IP address size and features. The increase in IPv6 address size to 128 bits (from the 32-bit IPv4 address) allows up to 3.4 x 10^{38} IP addresses. At the time of writing, the Switch supports the following features.

- Static address assignment (see Section 42.1.1 on page 152) and stateless autoconfiguration (see Stateless Autoconfiguration on page 155)
- Neighbor Discovery Protocol (see Neighbor Discovery Protocol (NDP) on page 156)
- Remote Management using SNMP, Telnet, HTTP and FTP services (see Chapter 75 on page 299)
- ICMPv6 (see ICMPv6 on page 156)
- IPv4/IPv6 dual stack; the Switch can run IPv4 and IPv6 at the same time.
- DHCPv6 client and relay (see DHCPv6 on page 155)
- Multicast Listener Discovery (MLD) snooping and proxy (see Multicast Listener Discovery on page 157)

For more information on IPv6 addresses, refer to RFC 2460 and RFC 4291.

42.1.1 IPv6 Addressing

The 128-bit IPv6 address is written as eight 16-bit hexadecimal blocks separated by colons (:). This is an example IPv6 address `2001:0db8:1a2b:0015:0000:0000:1a2f:0000`.

IPv6 addresses can be abbreviated in two ways:

- Leading zeros in a block can be omitted. So `2001:0db8:1a2b:0015:0000:0000:1a2f:0000` can be written as `2001:db8:1a2b:15:0:0:1a2f:0`.
- Any number of consecutive blocks of zeros can be replaced by a double colon. A double colon can only appear once in an IPv6 address. So `2001:0db8:0000:0000:1a2f:0000:0000:0015` can be written as `2001:0db8::1a2f:0000:0000:0015` or `2001:0db8:0000:0000:1a2f::0015`.

42.1.2 IPv6 Terms

IPv6 Prefix and Prefix Length

Similar to an IPv4 subnet mask, IPv6 uses an address prefix to represent the network address. An IPv6 prefix length specifies how many most significant bits (start from the left) in the address compose the network address. The prefix length is written as "/x" where x is a number. For example,

```
2001:db8:1a2b:15::1a2f:0/32
```

means that the first 32 bits (2001:db8) is the subnet prefix.

Interface ID

In IPv6, an interface ID is a 64-bit identifier. It identifies a physical interface (for example, an Ethernet port) or a virtual interface (for example, the management IP address for a VLAN). One interface should have a unique interface ID.

Link-local Address

A link-local address uniquely identifies a device on the local network (the LAN). It is similar to a "private IP address" in IPv4. You can have the same link-local address on multiple interfaces on a device. A link-local unicast address has a predefined prefix of fe80::/10. Link-local unicast address format is as follows.

Table 115 Link-local Unicast Address Format

1111 1110 10	0	Interface ID
10 bits	54 bits	64 bits

Global Address

A global address uniquely identifies a device on the Internet. It is similar to a "public IP address" in IPv4. The global address format as follows.

Table 116 Global Address Format

001	Global ID	Subnet ID	Interface ID
3 bits	45 bits	16 bits	64 bits

The global ID is the network identifier or prefix of the address and is used for routing. This may be assigned by service providers.

The subnet ID is a number that identifies the subnet of a site.

Multicast Addresses

In IPv6, Multicast addresses provide the same functionality as IPv4 broadcast addresses. Broadcasting is not supported in IPv6. A Multicast address allows a host to send packets to all hosts in a Multicast group.

Multicast scope allows you to determine the size of the Multicast group. A Multicast address has a predefined prefix of ff00::/8. The following table describes some of the predefined Multicast addresses.

Table 117 Predefined Multicast Address

MULTICAST ADDRESS	DESCRIPTION
FF01:0:0:0:0:0:0:1	All hosts on a local node.
FF01:0:0:0:0:0:0:2	All routers on a local node.
FF02:0:0:0:0:0:0:1	All hosts on a local connected link.
FF02:0:0:0:0:0:0:2	All routers on a local connected link.
FF05:0:0:0:0:0:0:2	All routers on a local site.
FF05:0:0:0:0:0:1:3	All DHCP severs on a local site.

The following table describes the Multicast addresses which are reserved and cannot be assigned to a Multicast group.

Table 118 Reserved Multicast Address

MULTICAST ADDRESS
FF00:0:0:0:0:0:0:0
FF01:0:0:0:0:0:0:0
FF02:0:0:0:0:0:0:0
FF03:0:0:0:0:0:0:0
FF04:0:0:0:0:0:0:0
FF05:0:0:0:0:0:0:0
FF06:0:0:0:0:0:0:0
FF07:0:0:0:0:0:0:0
FF08:0:0:0:0:0:0:0
FF09:0:0:0:0:0:0:0
FF0A:0:0:0:0:0:0:0
FF0B:0:0:0:0:0:0:0
FF0C:0:0:0:0:0:0:0
FF0D:0:0:0:0:0:0:0
FF0E:0:0:0:0:0:0:0
FF0F:0:0:0:0:0:0:0

Loopback

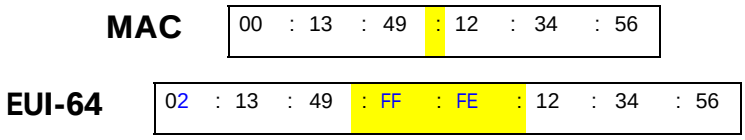
A loopback address (0:0:0:0:0:0:0:1 or ::1) allows a host to send packets to itself. It is similar to “127.0.0.1” in IPv4.

Unspecified

An unspecified address (0:0:0:0:0:0:0:0 or ::) is used as the source address when a device does not have its own address. It is similar to “0.0.0.0” in IPv4.

EUI-64

The EUI-64 (Extended Unique Identifier) defined by the IEEE (Institute of Electrical and Electronics Engineers) is an interface ID format designed to adapt with IPv6. It is derived from the 48-bit (6-byte) Ethernet MAC address as shown next. EUI-64 inserts the hex digits fffe between the third and fourth bytes of the MAC address and complements the seventh bit of the first byte of the MAC address. See the following example.



Stateless Autoconfiguration

With stateless autoconfiguration in IPv6, addresses can be uniquely and automatically generated. Unlike DHCPv6 (Dynamic Host Configuration Protocol version six) which is used in IPv6 stateful autoconfiguration, the owner and status of addresses do not need to be maintained by a DHCP server. Every IPv6 device is able to generate its own and unique IP address automatically when IPv6 is initiated on its interface. It combines the prefix and the interface ID (generated from its own Ethernet MAC address, see Interface ID and EUI-64) to form a complete IPv6 address.

When IPv6 is enabled on a device, its interface automatically generates a link-local address (beginning with fe80).

When the interface is connected to a network with a router and the `ipv6 address autoconfig` command is issued on the Switch, it generates [1]another address which combines its interface ID and global and subnet information advertised from the router. This is a routable global IP address.

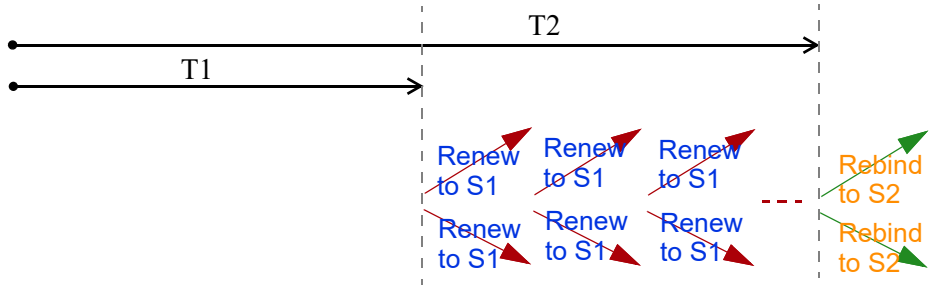
DHCPv6

The Dynamic Host Configuration Protocol for IPv6 (DHCPv6, RFC 3315) is a server-client protocol that allows a DHCP server to assign and pass IPv6 network addresses, prefixes and other configuration information to DHCP clients. DHCPv6 servers and clients exchange DHCP messages using UDP.

Each DHCP client and server has a unique DHCP Unique IDentifier (DUID), which is used for identification when they are exchanging DHCPv6 messages. The DUID is generated from the MAC address, time, vendor assigned ID and/or the vendor's private enterprise number registered with the IANA. It should not change over time even after you reboot the device.

Identity Association

An Identity Association (IA) is a collection of addresses assigned to a DHCP client, through which the server and client can manage a set of related IP addresses. Each IA must be associated with exactly one interface. The DHCP client uses the IA assigned to an interface to obtain configuration from a DHCP server for that interface. Each IA consists of a unique IAID and associated IP information.
The IA type is the type of address in the IA. Each IA holds one type of address. IA_NA means an identity association for non-temporary addresses and IA_TA is an identity association for temporary addresses. An IA_NA option contains the T1 and T2 fields, but an IA_TA option does not. The DHCPv6 server uses T1 and T2 to control the time at which the client contacts with the server to extend the lifetimes on any addresses in the IA_NA before the lifetimes expire. After T1, the client sends the server (**S1**) (from which the addresses in the IA_NA were obtained) a Renew message. If the time T2 is reached and the server does not respond, the client sends a Rebind message to any available server (**S2**). For an IA_TA, the client may send a Renew or Rebind message at the client's discretion.



1. In IPv6, all network interfaces can be associated with several addresses.

DHCP Relay Agent

A DHCP relay agent is on the same network as the DHCP clients and helps forward messages between the DHCP server and clients. When a client cannot use its link-local address and a well-known multicast address to locate a DHCP server on its network, it then needs a DHCP relay agent to send a message to a DHCP server that is not attached to the same network.

The DHCP relay agent can add the remote identification (remote-ID) option and the interface-ID option to the Relay-Forward DHCPv6 messages. The remote-ID option carries a user-defined string, such as the system name. The interface-ID option provides slot number, port information and the VLAN ID to the DHCPv6 server. The remote-ID option (if any) is stripped from the Relay-Reply messages before the relay agent sends the packets to the clients. The DHCP server copies the interface-ID option from the Relay-Forward message into the Relay-Reply message and sends it to the relay agent. The interface-ID should not change even after the relay agent restarts.

ICMPv6

Internet Control Message Protocol for IPv6 (ICMPv6 or ICMP for IPv6) is defined in RFC 4443. ICMPv6 has a preceding Next Header value of 58, which is different from the value used to identify ICMP for IPv4. ICMPv6 is an integral part of IPv6. IPv6 nodes use ICMPv6 to report errors encountered in packet processing and perform other diagnostic functions, such as "ping".

Neighbor Discovery Protocol (NDP)

The Neighbor Discovery Protocol (NDP) is a protocol used to discover other IPv6 devices and track neighbor's reachability in a network.

An IPv6 device uses the following ICMPv6 messages types:

- Neighbor solicitation: A request from a host to determine a neighbor's link-layer address (MAC address) and detect if the neighbor is still reachable. A neighbor being "reachable" means it responds to a neighbor solicitation message (from the host) with a neighbor advertisement message.
- Neighbor advertisement: A response from a node to announce its link-layer address.
- Router solicitation: A request from a host to locate a router that can act as the default router and forward packets.
- Router advertisement: A response to a router solicitation or a periodical Multicast advertisement from a router to advertise its presence and other parameters.

IPv6 Cache

An IPv6 host is required to have a neighbor cache, destination cache, prefix list and default router list. The Switch maintains and updates its IPv6 caches constantly using the information from response messages. In IPv6, the Switch configures a link-local address automatically, and then sends a neighbor solicitation message to check if the address is unique. If there is an address to be resolved or verified, the Switch also sends out a neighbor solicitation message. When the Switch receives a neighbor advertisement in response, it stores the neighbor's link-layer address in the neighbor cache. When the Switch uses a router solicitation message to query for a router and receives a router advertisement message, it adds the router's information to the neighbor cache, prefix list and destination cache. The Switch creates an entry in the default router list cache if the router can be used as a default router.

When the Switch needs to send a packet, it first consults the destination cache to determine the next hop. If there is no matching entry in the destination cache, the Switch uses the prefix list to determine

whether the destination address is on-link and can be reached directly without passing through a router. If the address is on-link, the address is considered as the next hop. Otherwise, the Switch determines the next-hop from the default router list or routing table. Once the next hop IP address is known, the Switch looks into the neighbor cache to get the link-layer address and sends the packet when the neighbor is reachable. If the Switch cannot find an entry in the neighbor cache or the state for the neighbor is not reachable, it starts the address resolution process. This helps reduce the number of IPv6 solicitation and advertisement messages.

Multicast Listener Discovery

The Multicast Listener Discovery (MLD) protocol (defined in RFC 2710) is derived from IPv4's Internet Group Management Protocol version 2 (IGMPv2). MLD uses ICMPv6 message types, rather than IGMP message types. MLDv1 is equivalent to IGMPv2 and MLDv2 is equivalent to IGMPv3.

MLD allows an IPv6 switch or router to discover the presence of MLD listeners who wish to receive Multicast packets and the IP addresses of Multicast groups the hosts want to join on its network.

MLD snooping and MLD proxy are analogous to IGMP snooping and IGMP proxy in IPv4.

MLD filtering controls which Multicast groups a port can join.

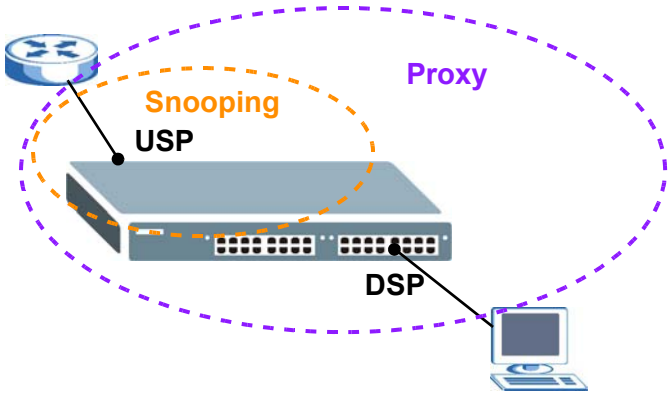
MLD Messages

A Multicast router or switch periodically sends general queries to MLD hosts to update the Multicast forwarding table. When an MLD host wants to join a Multicast group, it sends an MLD Report message for that address.

An MLD Done message is equivalent to an IGMP Leave message. When an MLD host wants to leave a Multicast group, it can send a Done message to the router or switch. If the leave mode is not set to `immediate`, the router or switch sends a group-specific query to the port on which the Done message is received to determine if other devices connected to this port should remain in the group.

MLD Port Role

A port on the Switch can be either a downstream port or upstream port in MLD. A downstream port (**DSP** in the figure) connects to MLD hosts and acts as a Multicast router to send MLD queries and listen to the MLD host's Report and Done messages. An upstream port (**USP** in the figure) connects to a Multicast router and works as a host to send Report or Done messages when receiving queries from a Multicast router.

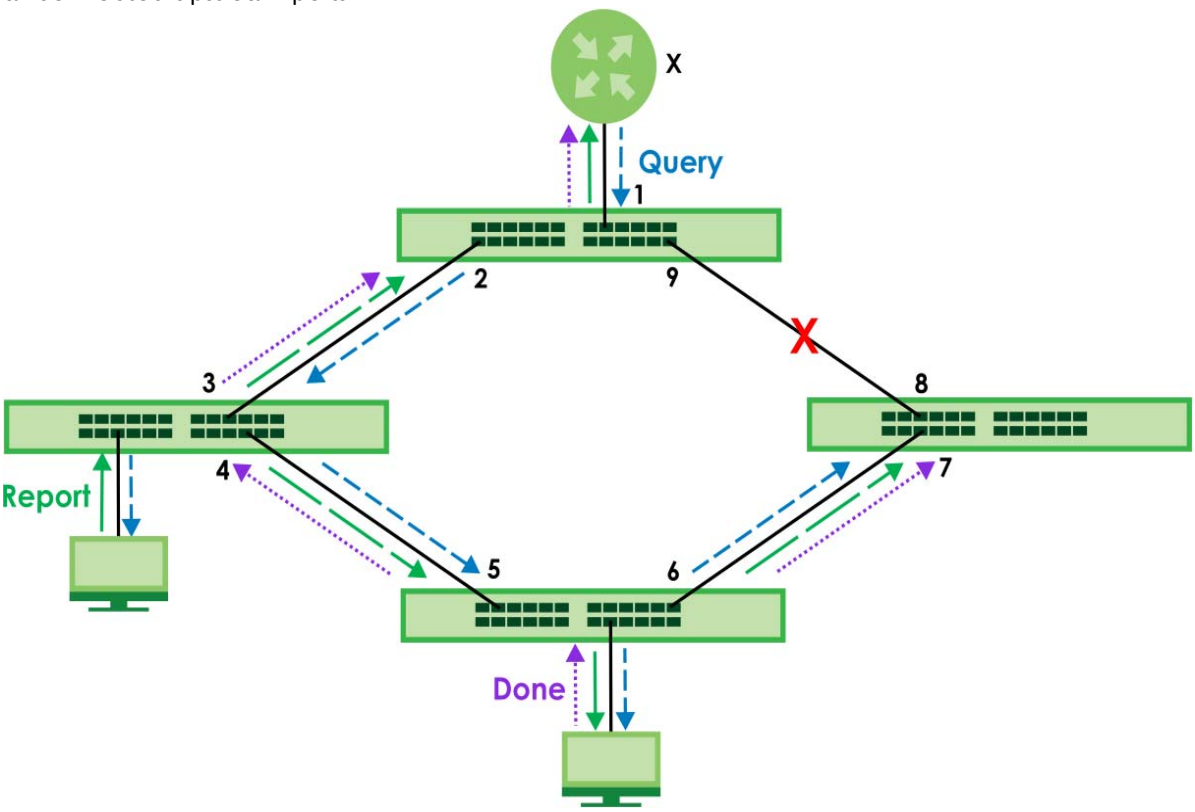


MLD Snooping-Proxy

MLD snooping-proxy is a Zyxel-proprietary feature. IPv6 MLD proxy allows only one upstream interface on a switch, while MLD snooping-proxy supports more than one upstream port on a switch. The upstream port in MLD snooping-proxy can report group changes to a connected Multicast router and forward MLD messages to other upstream ports. This helps especially when you want to have a network that uses STP to provide backup links between switches and also performs MLD snooping and proxy functions. MLD snooping-proxy, like MLD proxy, can minimize MLD control messages and allow better network performance.

In MLD snooping-proxy, if one upstream port is learned through snooping, all other upstream ports on the same device will be added to the same group. If one upstream port requests to leave a group, all other upstream ports on the same device will also be removed from the group.

In the following MLD snooping-proxy example, all connected upstream ports (1 – 7) are treated as one interface. The connection between ports 8 and 9 is blocked by STP to break the loop. If there is one query from a router (**X**) or MLD Done or Report message from any upstream port, it will be broadcast to all connected upstream ports.



42.2 Command Summary

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

Table 119 ipv6 User-input Values

COMMAND	DESCRIPTION
interface-type	VLAN. The Switch supports only the VLAN interface type at the time of writing.
interface-number	A VLAN ID number.
port-list	A list of one or more ports, separated by commas with no spaces. The list may also contain ranges of ports signified by a hyphen. For example: 1,3,5–8,10.

The following section lists the commands for this feature.

Table 120 ipv6 address Command Summary

COMMAND	DESCRIPTION	M	P
vlan <1-4094> interface vlan <1-4094>	Enters config-vlan mode config-route-domain mode for the specified VLAN. Creates the VLAN, if necessary.	C	13
ipv6	Globally enables IPv6 in this VLAN. The Switch then creates a link-local address automatically. Use "show ipv6" to see the generated address.	C	13
ipv6 address <*ipv6-address*>/<*prefix*>	Manually configures a static IPv6 global address for the VLAN.	C	13
ipv6 address <*ipv6-address*>/<*prefix*> eui-64	Manually configures a static IPv6 global address for the VLAN and have the interface ID be generated automatically using the EUI-64 format.	C	13
ipv6 address <*ipv6-address*>/<*prefix*> link-local	Manually configures a static IPv6 link-local address for the VLAN.	C	13
ipv6 address autoconfig	Use the command to have the Switch generate an IPv6 global address automatically in this VLAN after the Switch obtains the VLAN network information from a router. Note: Make sure an IPv6 router is available in the VLAN network before using this command on the Switch.	C	13
ipv6 address default-gateway <*gateway-ipv6-address*>	Sets the default gateway for the VLAN. When an interface cannot find a routing information for a frame's destination, it forwards the packet to the default gateway.	C	13
ipv6 address dhcp client <ia-na>	Sets the Switch to get a non-temporary IP address from the DHCP server.	C	13
ipv6 address dhcp client <ia-na> [rapid-commit]	Sets the Switch to get a non-temporary IP address from the DHCP server for this VLAN. Optionally, sets the Switch to send its DHCPv6 Solicit message with a Rapid Commit option to obtain information from the DHCP server by a rapid two-message exchange. The Switch discards any Reply messages that do not include a Rapid Commit option. The DHCPv6 server should also support the Rapid Commit option to have it work well.	C	13
ipv6 address dhcp client information refresh minimum <600-4294967295>	Sets the time interval (in seconds) at which the Switch exchanges other configuration information with a DHCPv6 server again.	C	13

Table 120 ipv6 address Command Summary (continued)

COMMAND	DESCRIPTION	M	P
ipv6 address dhcp client option <dns>	Sets the Switch to obtain DNS server information from the DHCP server.	C	13
ipv6 address dhcp client option <[dns][domain-list]>	Sets the Switch to obtain DNS server IPv6 addresses or a list of domain names from the DHCP server.	C	13
ipv6 mtu <*bytes*>	Sets the Maximum Transmission Unit (MTU) size (from 1280 to 1500) for IPv6 packets in this VLAN.	C	13
no ipv6	Disables IPv6 in this VLAN.	C	13
no ipv6 address <*ipv6-address*>/<*prefix*>	Removes a specified static global address.	C	13
no ipv6 address <*ipv6-address*>/<*prefix*> eui-64	Removes a specified static global address whose interface ID was generated using the EUI-64 format.	C	13
no ipv6 address <*ipv6-address*>/<*prefix*> link-local	Removes a specified static link-local address.	C	13
no ipv6 address autoconfig	Disables IPv6 address autoconfiguration in this VLAN.	C	13
no ipv6 address default-gateway	Removes the default gateway address for this VLAN.	C	13
no ipv6 address dhcp client	Disables the DHCP client feature in this VLAN.	C	13
no ipv6 address dhcp client [rapid-commit]	sets the Switch to not include a Rapid Commit option in its DHCPv6 Solicit message for this VLAN.	C	13
no ipv6 address dhcp client option	Sets the Switch to not obtain the DNS server information from the DHCP server.	C	13
no ipv6 address dhcp client option <[dns][domain-list]>	Sets the Switch to not obtain DNS server IPv6 addresses or a list of domain names from the DHCP server.	C	13
restart ipv6 dhcp client vlan <1-4094>	Sets the Switch to send a Release message for the assigned IPv6 address to the DHCP server and start DHCP message exchange again.	E	13
show ipv6	Displays IPv6 settings in all VLANs on the Switch.	E	3
show ipv6 dhcp6 show ipv6 dhcp	Displays the Switch's DHCPv6 DUID.	E	3
show ipv6 dhcp6 vlan <1-4094> show ipv6 dhcp vlan <1-4094>	Displays the DHCPv6 settings for the specified VLAN, including DHCPv6 mode, the IA type and the IAID.	E	3
show ipv6 vlan <1-4094>	Displays IPv6 settings in a specified VLAN on the Switch.	E	3
show ipv6 <*interface-type*> <*interface-number*>	Displays IPv6 settings for a specified interface on the Switch.	E	3

Table 121 ipv6 dhcp relay Command Summary

COMMAND	DESCRIPTION	M	P
ipv6 dhcp relay vlan <1-4094> helper-address <*remote-dhcp-server*>	Enables DHCPv6 relay agent and configures the remote DHCP server address for the specified VLAN.	C	13
ipv6 dhcp relay vlan <1-4094> option interface-id	Sets the Switch to add the interface-ID option in the DHCPv6 requests from the clients in the specified VLAN before the Switch forwards them to a DHCP server.	C	13

Table 121 ipv6 dhcp relay Command Summary (continued)

COMMAND	DESCRIPTION	M	P
ipv6 dhcp relay vlan <1-4094> option remote-id <*remote-id*>	Sets the Switch to add the remote-ID option in the DHCPv6 requests from the clients in the specified VLAN before the Switch forwards them to a DHCP server. This also specifies a string (up to 64 printable ASCII characters) to be carried in the remote-ID option.	C	13
no ipv6 dhcp6 relay vlan <1-4094> no ipv6 dhcp relay vlan <1-4094>	Disables DHCPv6 relay agent in the specified VLAN.	C	13
no ipv6 dhcp6 relay vlan <1-4094> option interface-id no ipv6 dhcp relay vlan <1-4094> option interface-id	Sets the Switch to not add the interface-ID option in the DHCPv6 requests from the clients in the specified VLAN before the Switch forwards them to a DHCP server.	C	13
no ipv6 dhcp6 relay vlan <1-4094> option remote-id no ipv6 dhcp relay vlan <1-4094> option remote-id	Sets the Switch to not add the remote-ID option in the DHCPv6 requests from the clients in the specified VLAN before the Switch forwards them to a DHCP server.	C	13

Table 122 ipv6 dhcp trust Command Summary

COMMAND	DESCRIPTION	M	P
ipv6 dhcp trust	Enables IPv6 DHCP trust to set whether ports are trusted or untrusted ports for DHCP snooping. All ports are untrusted ports by default.	C	13
no ipv6 dhcp trust	Disables IPv6 DHCP trust. All ports are automatically trusted.	C	13
interface port-channel <*port-list*>	Enters config-interface mode for the specified ports.	C	13
ipv6 dhcp trust	Configures this port as a trusted port. Trusted ports are connected to DHCPv6 servers or other switches.	C	13
no ipv6 dhcp trust	Configures this port as an untrusted port. Untrusted ports are connected to subscribers, and the Switch discards DHCPv6 packets from untrusted ports in the following situations: • The packet is a DHCPv6 server packet (for example, ADVERTISE, REPLY, or RELAY-REPLY). • The source MAC address and source IP address in the packet do not match any of the current bindings.	C	13

Table 123 ipv6 icmp and ping6 Command Summary

COMMAND	DESCRIPTION	M	P
ipv6 icmp error-interval <0-2147483647> [bucket-size <1-200>]	Sets the average transmission rate of ICMPv6 error messages the Switch generates, such as Destination Unreachable message, Packet Too Big message, Time Exceeded message and Parameter Problem message. error-interval: specifies a time period (in milliseconds) during which packets of up to the bucket size (10 by default) can be transmitted. 0 means no limit. Note: The Switch applies the time interval in increments of 10. For example, if you set a time interval from 1280 to 1289 milliseconds, the Switch uses the time interval of 1280 milliseconds. bucket-size: Defines the maximum number of packets which are allowed to transmit in a given time interval. If the bucket is full, subsequent error messages are suppressed.	C	13
ping6 <*ipv6-address*> vlan <1-4094> [-t] [size <1-1452>] [count <1~65535>]	Sends IPv6 ping packets to the specified Ethernet device. *vlan-id*: Specifies the VLAN ID to which the Ethernet device belongs. size <0-1452>: 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
ping6 <*ipv6-address*> <[-i <*interface-type*> <*interface-number*>] [-t] [-l <1-1452>] [-n <1-65535>] [-s <*ipv6-address*>]	Sends IPv6 ping packets to the specified Ethernet device. *interface-type*: the Switch supports only the VLAN interface type at the time of writing. *interface-number*: The VLAN ID to which the Ethernet device belongs. -l <1-1452>: Specifies the size of the ping packet. -t: Sends ping packets to the Ethernet device indefinitely. Press [CTRL]+C to terminate the Ping process. -n <1-65535>: Specifies how many times the Switch sends the ping packets. -s <*ipv6-address*>: Specifies the source IPv6 address of the pin packets.	E	0
show ipv6 mtu	The Switch uses Path MTU Discovery to discover Path MTU (PMTU), that is, the minimum link MTU of all the links in a path to the destination. If the Switch receives an ICMPv6 Packet Too Big error message after sending a packet, it adjusts the next packet size according to the suggested MTU in the error message. Displays IPv6 path MTU information on the Switch.	E	3

Table 124 ipv6 mld snooping-proxy Command Summary

COMMAND	DESCRIPTION	M	P
clear ipv6 mld snooping-proxy statistics all	Removes all MLD snooping-proxy statistics of the Switch.	E	13
clear ipv6 mld snooping-proxy statistics port	Removes the MLD snooping-proxy statistics of the ports.	E	13
clear ipv6 mld snooping-proxy statistics system	Removes the MLD snooping-proxy statistics of the Switch.	E	13
clear ipv6 mld snooping-proxy statistics vlan	Removes the MLD snooping-proxy statistics of the Multicast VLANs.	E	13
interface port-channel <*port-list*>	Enters config-interface mode for the specified ports.	C	13
ipv6 mld snooping-proxy filtering group-limited	Enables Multicast group limits for MLD snooping-proxy.	C	13
ipv6 mld snooping-proxy filtering group-limited number <*number*>	Sets the maximum number of the Multicast groups the ports is allowed to join. *number*: 0 – 255	C	13
ipv6 mld snooping-proxy filtering profile <*name*>	Assigns the specified MLD filtering profile to the ports. If MLD filtering is enabled on the Switch, the ports can only join the Multicast groups in the specified profile.	C	13
no ipv6 mld snooping-proxy filtering group-limited	Disables Multicast group limits for MLD snooping.	C	13
no ipv6 mld snooping-proxy filtering profile	Disables MLD filtering on the ports and allows the ports to join any group.	C	13
ipv6 mld snooping-proxy	Enables IPv6 MLD snooping-proxy on the Switch.	C	13
ipv6 mld snooping-proxy 8021p-priority <0-7>	Sets the default IEEE 802.1p priority in the MLD messages.	C	13
ipv6 mld snooping-proxy filtering	Enables MLD filtering on the Switch.	C	13
ipv6 mld snooping-proxy filtering profile <*name*> start-address <*ip*> end-address <*ip*>	Adds an MLD filtering profile and sets the range of the Multicast addresses.	C	13
ipv6 mld snooping-proxy vlan <*vlan-id*>	Enables MLD snooping-proxy on the specified VLAN.	C	13
ipv6 mld snooping-proxy vlan <*vlan-id*> downstream interface port-channel <*port-list*>	Specifies the downstream ports on the Switch. The ports will work as a Multicast router to send MLD queries and listen to the MLD host's join and leave messages.	C	13
ipv6 mld snooping-proxy vlan <*vlan-id*> downstream interface port-channel <*port-list*> fast-leave-timeout <2-16775168>	Sets the fast leave timeout (in milliseconds) for the specified downstream ports. This defines how many seconds the Switch waits for an MLD report before removing an MLD snooping membership entry (learned on a downstream port) when an MLD Done message is received on this port from a host.	C	13
ipv6 mld snooping-proxy vlan <*vlan-id*> downstream interface port-channel <*port-list*> leave-timeout <2-16775168>	Set the MLD snooping normal leave timeout (in milliseconds) the Switch uses to update the forwarding table for the specified downstream ports. This defines how many seconds the Switch waits for an MLD report before removing an MLD snooping membership entry (learned on a downstream port) when an MLD Done message is received on this port from a host.	C	13

Table 124 ipv6 mld snooping-proxy Command Summary (continued)

COMMAND	DESCRIPTION	M	P
ipv6 mld snooping-proxy vlan <*vlan-id*> downstream interface port-channel <*port-list*> mode <immediate | normal | fast>	Sets the leave mode for the specified downstream ports in a specified VLAN. This specifies whether Switch removes an MLD snooping membership entry (learned on a downstream port) immediately (immediate) or wait for an MLD report before the normal (normal) or fast (fast) leave timeout when an MLD leave message is received on this port from a host.	C	13
ipv6 mld snooping-proxy vlan <*vlan-id*> downstream query-interval <1000-31744000>	Sets the amount of time (in milliseconds) between general query messages sent by the downstream port.	C	13
ipv6 mld snooping-proxy vlan <*vlan-id*> downstream query-max-response-time <1000-25000>	Sets the maximum time (in milliseconds) that the Switch waits for a response to a general query message sent by the downstream port.	C	13
ipv6 mld snooping-proxy vlan <*vlan-id*> upstream interface port-channel <*port-list*>	Specifies the upstream (host) ports on the Switch. The ports will work as an MLD host to send join or leave messages when receiving queries from the Multicast router.	C	13
ipv6 mld snooping-proxy vlan <*vlan-id*> upstream last-listener-query-interval <1-8387584>	Sets the amount of time (in milliseconds) between the MLD group-specific queries sent by an upstream port when an MLD Done message is received. This value should be exactly the same as what's configured in the connected Multicast router. This value is used to calculate the amount of time an MLD snooping membership entry (learned only on the upstream port) can remain in the forwarding table after a Done message is received. When an MLD Done message is received, the Switch sets the entry's lifetime to be: last-listener-query-interval x robustness-variable.	C	13
ipv6 mld snooping-proxy vlan <*vlan-id*> upstream query-interval <1000-31744000>	Sets the amount of time (in milliseconds) between general query messages sent by the router connected to the upstream port. This value should be exactly the same as what's configured in the connected Multicast router. This value is used to calculate the amount of time an MLD snooping membership entry (learned only on the upstream port) can remain in the forwarding table. When an MLD Report message is received, the Switch sets the timeout period of the entry to be: query-interval x robustness-variable + query-max-response-time	C	13

Table 124 ipv6 mld snooping-proxy Command Summary (continued)

COMMAND	DESCRIPTION	M	P
ipv6 mld snooping-proxy vlan <*vlan-id*> upstream query-max-response-time <1000-25000>	Sets the amount of time (in milliseconds) the router connected to the upstream port waits for a response to an MLD general query message. This value should be exactly the same as what is configured in the connected Multicast router. This value is used to calculate the amount of time an MLD snooping membership entry (learned only on the upstream port) can remain in the forwarding table. When an MLD Report message is received, the Switch sets the timeout period of the entry to be: query-interval x robustness-variable + query-max-response-time When an MLD Done message is received, the Switch sets the entry's lifetime to be: last-listener-query-interval x robustness-variable	C	13
ipv6 mld snooping-proxy vlan <*vlan-id*> upstream robustness-variable <1-25>	Sets the number of queries. A Multicast address entry (learned only on an upstream port by snooping) is removed from the forwarding table when there is no response to the configured number of queries sent by the router connected to the upstream port. This value should be exactly the same as what's configured in the connected Multicast router. This value is used to calculate the amount of time an MLD snooping membership entry (learned only on the upstream port) can remain in the forwarding table.	C	13
no ipv6 mld snooping-proxy	Disables IPv6 MLD snooping-proxy on the Switch.	C	13
no ipv6 mld snooping-proxy filtering	Disables IPv6 MLD filtering on the Switch.	C	13
no ipv6 mld snooping-proxy filtering profile <*name*>	Removes the specified MLD filtering profile.	C	13
no ipv6 mld snooping-proxy filtering profile <*name*> start-address <*ip*> end-address <*ip*>	Removes the range of Multicast addresses from the specified filtering profile.	C	13
no ipv6 mld snooping-proxy vlan <*vlan-id*>	Disables MLD snooping-proxy on the specified VLAN.	C	13
no ipv6 mld snooping-proxy vlan <*vlan-id*> downstream interface port-channel <*port-list*>	Sets the specified ports to not be a downstream ports for the specified VLAN.	C	13
no ipv6 mld snooping-proxy vlan <*vlan-id*> upstream interface port-channel <*port-list*>	Sets the specified ports to not be an upstream ports for the specified VLAN.	C	13
show interfaces config <*port-list*> mld snooping-proxy filtering group-limited	Displays whether MLD filtering is enabled and the maximum MLD group number for the specified ports.	E	3
show interfaces config <*port-list*> mld snooping-proxy filtering profile	Displays the name of the filtering profile for the specified ports.	E	3
show ipv6 mld snooping-proxy	Displays whether MLD snooping-proxy is enabled on the Switch and on which VLANs.	E	3

Table 124 ipv6 mld snooping-proxy Command Summary (continued)

COMMAND	DESCRIPTION	M	P
show ipv6 mld snooping-proxy filtering profile	Displays whether MLD filtering is enabled on the Switch and the filtering profile settings.	E	3
show ipv6 mld snooping-proxy group	Displays the Multicast group addresses learned on the Switch's ports.	E	3
show ipv6 mld snooping-proxy statistics interface port-channel <*port-list*>	Displays the MLD snooping-proxy statistics of the specified ports.	E	3
show ipv6 mld snooping-proxy statistics system	Displays the MLD snooping-proxy statistics of the Switch.	E	3
show ipv6 mld snooping-proxy statistics vlan <*vlan-list*>	Displays the MLD snooping-proxy statistics of the specified Multicast VLANs.	E	3
show ipv6 mld snooping-proxy vlan <*vlan-id*>	Displays MLD proxy settings for the specified VLAN.	E	3
show ipv6 multicast	Displays the Multicast group addresses learned on the Switch's ports and the timeout values.	E	3

Table 125 ipv6 nd Command Summary

COMMAND	DESCRIPTION	M	P
interface vlan <1-4094>	Enters config-route-domain mode for the specified VLAN. Creates the VLAN, if necessary.	C	13
ipv6 nd dad-attempts <0-600>	Sets the number of consecutive neighbor solicitations the Switch sends for this VLAN. The Switch uses Duplicate Address Detection (DAD) with neighbor solicitation and advertisement messages to check whether an IPv6 address is already in use before assigning it to an interface, such as the link-local address it creates through stateless address autoconfiguration for this VLAN. To turn off the DAD for this VLAN, set the number of DAD attempts to 0.	C	13
ipv6 nd managed-config-flag	Configures the Switch to set the "managed address configuration" flag (the M flag) to 1 in IPv6 router advertisements, which means hosts use DHCPv6 to obtain IPv6 stateful addresses.	C	13
ipv6 nd ns-interval <1000-3600000>	Specifies the time interval (in milliseconds) at which neighbor solicitations are re-sent for this VLAN.	C	13
ipv6 nd other-config-flag	Configures the Switch to set the "Other stateful configuration" flag (the O flag) to 1 in IPv6 router advertisements, which means hosts use DHCPv6 to obtain additional configuration settings, such as DNS information.	C	13

Table 125 ipv6 nd Command Summary (continued)

COMMAND	DESCRIPTION	M	P
ipv6 nd prefix <*ipv6-prefix*>/<*prefix-length*> <[valid-lifetime <0-4294967295>] [preferred-lifetime <0-4294967295>] [no-autoconfig] [no-onlink] [no-advertise]>	Sets the Switch to include the specified IPv6 prefix, prefix length and optional parameters in router advertisements for this VLAN. valid-lifetime: sets how long in seconds the prefix is valid for on-link determination. preferred-lifetime: sets how long (in seconds) that addresses generated from the prefix through stateless address autoconfiguration remain preferred. no-autoconfig: indicates the hosts cannot use this prefix for stateless address autoconfiguration. no-onlink: indicates this prefix cannot be used for on-link determination. no-advertise: sets the Switch to not include the specified IPv6 prefix, prefix length and optional parameters in router advertisements for this VLAN.	C	13
ipv6 nd prefix <*ipv6-prefix*>/<*prefix-length*>	Sets the Switch to include the specified IPv6 prefix and prefix length in router advertisements for this VLAN.	C	13
ipv6 nd ra interval minimum <3-1350> maximum <4-1800>	Specifies the minimum and maximum time intervals at which the Switch sends router advertisements for this VLAN.	C	13
ipv6 nd ra lifetime <0-9000>	Sets how long (in seconds) the router in router advertisements can be used as a default router for this VLAN.	C	13
ipv6 nd ra suppress	Sets the Switch to not send router advertisements and responses to router solicitations for this VLAN.	C	13
ipv6 nd reachable-time <1000-3600000>	Specifies how long (in milliseconds) a neighbor is considered reachable for this VLAN.	C	13
no ipv6 nd dad-attempts	Resets the number of the DAD attempts to the default settings (3).	C	13
no ipv6 nd managed-config-flag	Configures the Switch to set the “managed address configuration” flag (the M flag) to 0 in IPv6 router advertisements, which means hosts do not use DHCPv6 to obtain IPv6 stateful addresses.	C	13
no ipv6 nd ns-interval	Resets the time interval between retransmissions of neighbor solicitations to the default setting (1000 milliseconds).	C	13
no ipv6 nd other-config-flag	Configures the Switch to set the “Other stateful configuration” flag (the O flag) to 0 in IPv6 router advertisements, which means hosts do not use DHCPv6 to obtain additional configuration settings, such as DNS information.	C	13
no ipv6 nd prefix <*ipv6-prefix*>/<*prefix-length*>	Sets the Switch to not include the specified IPv6 prefix and prefix length in router advertisements for this VLAN.	C	13
no ipv6 nd ra interval	Resets the minimum and maximum time intervals between retransmissions of router advertisements for this VLAN to the default settings.	C	13
no ipv6 nd ra lifetime	Resets the lifetime of a router in router advertisements to the default setting (1800 seconds).	C	13
no ipv6 nd ra suppress	Enables the sending of router advertisements and responses to router solicitations on this interface.	C	13

Table 125 ipv6 nd Command Summary (continued)

COMMAND	DESCRIPTION	M	P
no ipv6 nd reachable-time	Resets the reachable time of a neighbor to the default setting (30000 milliseconds).	C	13
ipv6 hop-limit <1-255>	Sets the maximum number of hops on which an IPv6 packet is allowed to transmit before it is discarded by an IPv6 router, which is similar to the TTL field in IPv4.	C	13
ipv6 route <*ipv6-prefix*>/<*prefix-length*> <*next-hop*>	Creates a static route to forward packets with the specified IPv6 prefix and prefix length to a specific gateway.	C	13
ipv6 route <*ipv6-prefix*>/<*prefix-length*> <*next-hop*> <*interface-type*> <*interface-number*>	Creates a static route to forward packets with the specified IPv6 prefix and prefix length to a specific gateway in a VLAN.	C	13
no ipv6 hop-limit	Resets the maximum number of hops in router advertisements to the default setting.	C	13
no ipv6 route <*ipv6-prefix*>/<*prefix-length*>	Removes an IPv6 static route.	C	13
show ipv6 route	Displays IPv6 routing information on the Switch.	E	3
show ipv6 route static	Displays static IPv6 routing information on the Switch.	E	3
show ipv6 prefix	Displays all IPv6 prefix information on the Switch.	E	3
show ipv6 prefix <*interface-type*> <*interface-number*>	Displays IPv6 prefix information for the specified interface (VLAN).	E	3

Table 126 ipv6 neighbor Command Summary

COMMAND	DESCRIPTION	M	P
clear ipv6 neighbor	Removes all IPv6 neighbor information on the Switch.	E	13
clear ipv6 neighbor <*interface-type*> <*interface-number*>	Removes IPv6 neighbor information for a specified interface on the Switch.	E	13
ipv6 neighbor <*interface-type*> <*interface-number*> <*ipv6-address*> <*mac-address*>	Creates a static IPv6 neighbor entry in the IPv6 cache for this VLAN.	C	13
no ipv6 neighbor <*interface-type*> <*interface-number*> <*ipv6-address*>	Removes a static IPv6 neighbor entry from the IPv6 cache.	C	13
show ipv6 neighbor	Displays the IPv6 neighbor devices on the Switch	E	3
show ipv6 neighbor <*interface-type*> <*interface-number*>	Displays IPv6 neighbor devices for a specified interface on the Switch.	E	3
show ipv6 router	Displays all IPv6 router advertisement information on the Switch.	E	3
show ipv6 router <*interface-type*> <*interface-number*>	Displays IPv6 router advertisement information for a specified interface on the Switch.	E	3
show ipv6 neighbor address	Displays and arranges the data according to IPv6 address of the neighboring device.	E	3
show ipv6 neighbor count	Displays the number of the neighboring devices.	E	3

Table 126 ipv6 neighbor Command Summary (continued)

COMMAND	DESCRIPTION	M	P
show ipv6 neighbor interface	Displays and arranges the data according to IPv6 interface on which the IPv6 address is created or through which the neighboring device can be reached.	E	3
show ipv6 neighbor mac	Displays and arranges the data according to MAC address of the IPv6 interface on which the IPv6 address is configure or the MAC address of the neighboring device.	E	3

Table 127 IPv6 NS tracking Command Summary

COMMAND	DESCRIPTION	M	P
ipv6 icmp ns tracking aging-time <120-86400>	Sets the aging time for stale (unreachable) devices. When a device becomes unreachable, its record in the Neighbor Solicitation (NS) table starts aging. When the age reaches the value set by this command, the Switch deletes the device from the NS table. Note: For information on Neighbor Solicitation, see page 156.	C	13
clear ipv6 ns tracking	Clears all IPv6 Neighbor Solicitation (NS) tracking information.	E	13
show ipv6 ns tracking	Displays all devices currently being tracked using Neighbor Solicitation (NS), as a table. The table includes each device's network settings, MAC address, and current network status.	E	3
show ipv6 ns tracking count	Displays how many devices are currently being tracked using Neighbor Solicitation (NS).	E	3

Table 128 ipv6 snooping policy Command Summary

COMMAND	DESCRIPTION	M	P
ipv6 snooping policy <*name*>	Enters sub-command mode for creating an IPv6 snooping policy.	C	13
limit address-count <*number*>	Sets the number of IPv6 addresses and prefixes learned using the IPv6 snooping policy. The maximum limit address count is the maximum size of the IPv6 source guard binding table.	C	13
no limit address-count	Removes the maximum limit address count setting.	C	13
prefix-glean	Allows the Switch to learn the IPv6 prefix and length from DHCPv6 sniffed packets.	C	13
no prefix-glean	Disables IPv6 prefix gleaning.	C	13
protocol dhcp	Enables DHCP snooping to have the Switch sniff DHCPv6 packets sent from a DHCPv6 server to a DHCPv6 client.	C	13
no protocol dhcp	Disables DHCP snooping.	C	13
no ipv6 snooping policy <*name*>	Removes the specified IPv6 snooping policy.	C	13
interface vlan <1-4094>	Enters config-route-domain mode for the specified VLAN. Creates the VLAN, if necessary.	C	13
ipv6 snooping attach-policy <*name*>	Enables a IPv6 snooping policy on the specified VLAN interface.	C	13

Table 128 ipv6 snooping policy Command Summary (continued)

COMMAND	DESCRIPTION	M	P
no ipv6 snooping attach-policy	Disables the IPv6 snooping policy on the VLAN interface.	C	13
show ipv6 snooping policy [<*name*>]	Displays all or the specified IPv6 snooping policy settings.	E	3

Table 129 ipv6 source binding Command Summary

COMMAND	DESCRIPTION	M	P
clear ipv6 source binding [address <*ipv6-address*> | prefix <*ipv6-address/prefix-length*>]	Removes all or the dynamic IPv6 source binding entries snooped with the specified IPv6 address and/or prefix address.	E	13
ipv6 source binding <*ipv6-address*|*ipv6-address/prefix-length*> [mac <*mac-addr*>] [vlan <*vlan-id*>] [interface port-channel <*port-list*>]	Creates an IPv6 source binding table entry.	C	13
no ipv6 source binding <*ipv6-address*|*ipv6-address/prefix-length*>	Removes a static IPv6 source binding entry with the specified IPv6 address and/or prefix address.	C	13
show ipv6 source binding	Displays all the current bindings on the Switch. The table contains bindings discovered using DHCP Snooping (dynamic) and bindings that were manually added (static).	E	3
show ipv6 source binding [*ipv6-address*|*ipv6-address/prefix-length*] [mac <*mac-address*>] [vlan <*vlan-id*>] [interface port-channel <*port-list*>] [dhcpv6-snooping |static]>	Displays the IPv6 source binding table, based on the specified parameters.	E	3
show ipv6 source binding count	Displays the number of IPv6 source binding entries.	E	3

Table 130 ipv6 source guard Command Summary

COMMAND	DESCRIPTION	M	P
ipv6 source-guard policy <*name*>	Enters sub-command mode for creating an IPv6 source guard policy.	C	13
permit link-local	Allows data traffic from all link-local addresses.	C	13
no permit link-local	Blocks data traffic from all link-local addresses.	C	13
validate address	Sets IPv6 source guard to forward valid IPv6 addresses that are stored in the binding table.	C	13
no validate address	Sets IPv6 source guard to not forward valid IPv6 addresses that are stored in the binding table.	C	13
validate prefix	Sets IPv6 source guard to forward valid IPv6 prefixes that are stored in the binding table.	C	13
no validate prefix	Sets IPv6 source guard to not forward valid IPv6 prefixes that are stored in the binding table.	C	13
show ipv6 source-guard policy [<*name*>]	Displays information of all IPv6 source guard policies on the Switch or the specified IPv6 source guard policy.	E	3

42.3 Command Examples

This example shows how to enable IPv6 in VLAN 1 and display the link-local address the Switch automatically generated for the VLAN.

```
sysname# config
sysname(config)# vlan 1
sysname(config-vlan)# ipv6
sysname(config-vlan)# exit
sysname(config)# exit
sysname# show ipv6

VLAN ID     : 1
IPv6 Status : Enable

Origin    IP Address/PrefixLength                      Status     Expire
--------- ------------------------------------------- ---------- -----------
manual    fe80::219:cbff:fe00:1/64                     preferred   permanent
```

The following table describes the labels in the `show ipv6` command output.

Table 131 show ipv6

LABEL	DESCRIPTION
VLAN ID	This field displays a configured VLAN identifier.
IPv6 Status	This field displays the current IPv6 status in a VLAN. You can use the command "ipv6" to enable IPv6 in a VLAN if it displays Disable.
Origin	This field displays the origin of an IPv6 address. The available options for this field are: • manual: The IP address was automatically generated by the interface itself or configured manually. • linklayer: The IP address was generated by stateless autoconfiguration. • other: The IP address was assigned by a DHCP server.
IP Address / Prefix Length	This field displays the configured IPv6 address and prefix.
Status	This field displays the current status of an IPv6 address. The available options for this field are: • preferred: This is a valid address and it can be used as a sender or receiver address. • deprecated: This is a valid address but should not be used as a sender address in new session. • invalid: This is not a valid address and it should not be used as a sender or receiver address. • inaccessible: The address is not accessible because the interface to which this address is assigned is not operational. • unknown: The status of the IP address cannot be determined for some reason. • tentative: The Switch is verifying the uniqueness of the IP address. • duplicate: The address is not unique in your network and can not be used.
Expire	This displays how long (hh:mm:ss) an address can be used before it expires. When an address is manually configured, it displays permanent (never expires).

This example shows how to enable IPv6 in VLAN 1 and display the link-local address the Switch automatically generated and other IPv6 information for the VLAN.

```
sysname# config
sysname(config)# interface vlan 1
sysname(config-vlan)# ipv6
sysname(config-vlan)# exit
sysname(config)# exit
sysname# show ipv6 vlan 1
VLAN : 1 (VLAN1)
  IPv6 is enabled.
  MTU is 1500 bytes.
  ICMP error messages limited to 10 every 100 milliseconds.
  Stateless Address Autoconfiguration is disabled.
  Link-Local address is fe80::219:cbff:fe6f:9159 [preferred]
  Global unicast address(es):
  Joined group address(es):
    ff02::2
    ff01::1
    ff02::1
    ff02::1:ff6f:9159
  ND DAD is enabled, number of DAD attempts: 1
  ND NS-interval is 1000 milliseconds
  ND reachable time is 30000 milliseconds
  ND router advertised managed config flag is disable
  ND router advertised other config flag is disable
  ND router advertisements are sent every 200 to 600 seconds
  ND router advertisements lifetime 1800 seconds
```

This example shows how to manually configure two IPv6 addresses (one uses the EUI-64 format, one doesn't) in VLAN 1, and then display the result. Before using `ipv6 address` commands, you have to enable IPv6 in the VLAN and this has the Switch generate a link-local address for the interface.

There are three addresses created in total for VLAN 1. The address "2001:db8:c18:1:219:cbff:fe00:1/64" is created with the interface ID "219:cbff:fe00:1" generated using the EUI-64 format. The address "2001:db8:c18:1::12b/64" is created exactly the same as what you entered in the command.

```
sysname# config
sysname(config)# vlan 1
sysname(config-vlan)# ipv6
sysname(config-vlan)# ipv6 address 2001:db8:c18:1::127/64 eui-64
sysname(config-vlan)# ipv6 address 2001:db8:c18:1::12b/64
sysname(config-vlan)# exit
sysname(config)# exit
sysname# show ipv6

VLAN ID     : 1
IPv6 Status : Enable

Origin    IP Address/PrefixLength                    Status     Expire
--------- ------------------------------------------ ---------- -----------
manual    fe80::219:cbff:fe00:1/64                    preferred   permanent
manual    2001:db8:c18:1:219:cbff:fe00:1/64           preferred   permanent
manual    2001:db8:c18:1::12b/64                      preferred   permanent
```

```
sysname# config
sysname(config)# interface vlan 1
sysname(config-vlan)# ipv6
sysname(config-vlan)# ipv6 address 2001:db8:c18:1::127/64 eui-64
sysname(config-vlan)# ipv6 address 2001:db8:c18:1::12b/64
sysname(config-vlan)# exit
sysname(config)# exit
sysname# show ipv6
VLAN : 1 (VLAN1)
  IPv6 is enabled.
  MTU is 1500 bytes.
  ICMP error messages limited to 10 every 100 milliseconds.
  Stateless Address Autoconfiguration is disabled.
  Link-Local address is fe80::219:cbff:fe00:1 [preferred]
  Global unicast address(es):
    2001:db8:c18:1::12b/64 [preferred]
    2001:db8:c18:1:219:cbff:fe00:1/64 [preferred]
  Joined group address(es):
    ff02::1:ff00:12b
    ff02::2
    ff01::1
    ff02::1
    ff02::1:ff6f:9159
  ND DAD is enabled, number of DAD attempts: 1
  ND NS-interval is 1000 milliseconds
  ND reachable time is 30000 milliseconds
  ND router advertised managed config flag is disable
  ND router advertised other config flag is disable
  ND router advertisements are sent every 200 to 600 seconds
  ND router advertisements lifetime 1800 seconds
```

This example shows the Switch owns (L displays in the **T** field) two manually configured (permanent) IP addresses, 2001::1234 and fe80::219:cbff:fe00:1. It also displays a neighbor fe80::2d0:59ff:feb8:103c in VLAN 1 is reachable from the Switch.

```
sysname# show ipv6 neighbor
Address                                 MAC               VLAN S  T Expire
--------------------------------------- ----------------- ---- -- - ----------
2001::1234                              0:19:cb:0:0:1     1    R  L permanent
fe80::219:cbff:fe00:1                   0:19:cb:0:0:1     1    R  L permanent
fe80::2d0:59ff:feb8:103c                0:d0:59:b8:10:3c  1    R  D 23h53m34s

S: reachable(R),stale(S),delay(D),probe(P),invalid(IV),incomplete(I),unknown(?)
T: local(L),dynamic(D),static(S),other(O)
```

```
sysname# show ipv6 neighbor
Address                                 MAC               S  T Interface
--------------------------------------- ----------------- -- - ------------
2001::1234                              00:19:cb:0:0:0:1  R  L vlan 1
fe80::219:cbff:fe00:1                   00:19:cb:0:0:0:1  R  L vlan 1
fe80::2d0:59ff:feb8:103c                00:d0:59:b8:10:3c R  D vlan 1

S: reachable(R),stale(S),delay(D),probe(P),invalid(IV),incomplete(I),unknown(?)
T: local(L),dynamic(D),static(S),other(O)
```

The following table describes the labels in this screen.

Table 132 show ipv6 neighbor

LABEL	DESCRIPTION
Address	This is the IPv6 address of the Switch or a neighboring device.
MAC	This is the MAC address of the neighboring device or itself.
VLAN	This is the VLAN of which an IPv6 interface is a member.
S	This field displays whether the neighbor IPv6 interface is reachable. In IPv6, "reachable" means an IPv6 packet can be correctly forwarded to a neighbor node (host or router) and the neighbor can successfully receive and handle the packet. The available options in this field are: • reachable(R): The interface of the neighboring device is reachable. (The Switch has received a response to the initial request.) • stale(S): The last reachable time has expired and the Switch is waiting for a response to another initial request. The field displays this also when the Switch receives an unrequested response from the neighbor's interface. • delay(D): The neighboring interface is no longer known to be reachable, and traffic has been sent to the neighbor recently. The Switch delays sending request packets for a short to give upper-layer protocols a chance to determine reachability. • probe(P): The Switch is sending request packets and waiting for the neighbor's response. • invalid(IV): The neighbor address is with an invalid IPv6 address. • unknown(?): The status of the neighboring interface can not be determined for some reason. • incomplete(I): Address resolution is in progress and the link-layer address of the neighbor has not yet been determined (see RFC 2461). The interface of the neighboring device did not give a complete response.
T	This field displays the type of an address mapping to a neighbor interface. The available options in this field are: • other(O): none of the following type. • dynamic(D): The IP address to MAC address can be successfully resolved using IPv6 Neighbor Discovery protocol (See Neighbor Discovery Protocol (NDP)). It is similar as IPv4 ARP (Address Resolution protocol). • static(S): The interface address is statically configured. • local(L): A Switch interface is using the address.
Interface	This field displays the IPv6 interface.
Expire	This displays how long (*hhhmmmsss*) an address can be used before it expires. If an address is manually configured, it displays permanent (never expires).

This example shows the ipv6 NS tracking table and tracking count.

```
sysname# show ipv6 neighbor
  Address                                 MAC               S  T Interface
  --------------------------------------- ----------------- -- - -----------
-
  fe80::219:caff:fe01:b0d                 00:19:ca:01:0b:0d R  L vlan 1
  fe80::a26:97ff:fede:2177                08:26:97:de:21:77 S  D vlan 1
  fe80::298b:84cb:28aa:9cbe               00:00:e8:88:e7:52 S  D vlan 1
  fe80::2cd9:f633:775b:418d               98:fa:9b:5f:ef:6d S  D vlan 1
  fe80::39ff:cf44:b86:78e3                90:2b:34:bb:7a:a4 S  D vlan 1
  fe80::4087:e9cd:15e7:221e               dc:4a:3e:40:ec:67 S  D vlan 1

  S:
reachable(R),stale(S),delay(D),probe(P),invalid(IV),incomplete(I),unknown(?
)
  T: local(L),dynamic(D),static(S),other(O)
sysname# show ipv6 ns tracking count
No : 6
```

This example sends ping requests to an Ethernet device with IPv6 address fe80::2d0:59ff:feb8:103c in VLAN 1. The device also responds the pings.

```
sysname# ping6 fe80::2d0:59ff:feb8:103c vlan 1
PING6(56=40+8+8 bytes) fe80::219:cbff:fe00:1 --> fe80::2d0:59ff:feb8:103c
16 bytes from fe80::2d0:59ff:feb8:103c, icmp_seq=0 hlim=128 time=1.0  ms
16 bytes from fe80::2d0:59ff:feb8:103c, icmp_seq=1 hlim=128 time=1.0  ms
16 bytes from fe80::2d0:59ff:feb8:103c, icmp_seq=2 hlim=128 time=1.0  ms

--- fe80::2d0:59ff:feb8:103c ping6 statistics ---
3 packets transmitted, 3 packets received, 0.0 % packet loss
round-trip min/avg/max = 1.0 /1.0 /1.0  ms
sysname#
```

```
sysname# ping6 ffe80::2d0:59ff:feb8:103c -i vlan 1
PING6(56=40+8+8 bytes) fe80::219:cbff:fe00:1 --> fe80::2d0:59ff:feb8:103c
16 bytes from fe80::2d0:59ff:feb8:103c, icmp_seq=0 hlim=64 time=1.0  ms
16 bytes from fe80::2d0:59ff:feb8:103c, icmp_seq=1 hlim=64 time=1.0  ms
16 bytes from fe80::2d0:59ff:feb8:103c, icmp_seq=2 hlim=64 time=1.0  ms

--- fe80::2d0:59ff:feb8:103c ping6 statistics ---
3 packets transmitted, 3 packets received, 0.0 % packet loss
round-trip min/avg/max = 1.0 /1.0 /1.0  ms
sysname#
```

This example configures a static IPv6 route to forward packets with IPv6 prefix 2100:: and prefix length 64 to the gateway with IPv6 address fe80::219:cbff:fe01:101 in VLAN 1.

```
sysname# config
sysname(config)# ipv6 route 2100::/64 fe80::219:cbff:fe01:101 vlan 1
sysname(config)# exit
sysname# show ipv6 route
  Terminology:
    C - Connected, S - Static
Destination/Prefix Length                          Type
Next Hop                                           Interface
-------------------------------------------------------------
2001:db8:c18:1::/64                                C
::                                                 VLAN1
2100::/64                                          S
fe80::219:cbff:fe01:101                            VLAN1
sysname#
```

IPv6 is installed and enabled by default in Windows 8, 8.1, 10, 11 and on Windows Server 2012, 2016, 2019, 2020, and later. Use the “ipconfig” command to check your automatic configured IPv6 address.

CHAPTER 43
Layer 2 Protocol Tunnel (L2PT) Commands

43.1 Command Summary

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

Table 133 Interface Command Values

COMMAND	DESCRIPTION
port-list	A list of one or more ports, separated by commas with no spaces. The list may also contain ranges of ports signified by a hyphen. For example: 1,3,5–8,10.

The following section lists the commands for this feature.

Table 134 l2pt Command Summary

COMMAND	DESCRIPTION	M	P
`clear l2protocol-tunnel`	Removes all layer 2 protocol tunneling counters.	E	13
`interface port-channel <port-list>`	Enters config-interface mode for configuring the specified ports.	C	13
`l2protocol-tunnel`	Enables layer 2 protocol tunneling for CDP (Cisco Discovery Protocol), STP (Spanning Tree Protocol) and VTP (VLAN Trunking Protocol) packets on the specified ports.	C	13
`l2protocol-tunnel cdp`	Enables layer 2 protocol tunneling for CDP packets on the specified ports.	C	13
`l2protocol-tunnel mode <access|tunnel>`	Sets the L2PT mode for the specified ports access: for ingress ports at the edge of the service provider's network. The Switch encapsulates the incoming layer 2 protocol packets and forward them to the tunnel ports. Note: You can enable L2PT services for STP, LACP, VTP, LLDP, CDP, UDLD, and PAGP on the access ports only. tunnel: for egress ports at the edge of the service provider's network. The Switch decapsulates the encapsulated layer 2 protocol packets received on a tunnel port by changing the destination MAC address to the original one, and then forward them to an access port. If the services is not enabled on an access port, the protocol packets are dropped.	C	13

Table 134 l2pt Command Summary (continued)

COMMAND	DESCRIPTION	M	P
l2protocol-tunnel point-to-point	Enables point-to-point layer 2 protocol tunneling for LACP (Link Aggregation Control Protocol), PAgP (Port Aggregation Protocol) and UDLD (UniDirectional Link Detection) packets on the specified ports.	C	13
l2protocol-tunnel point-to-point lacp	Enables point-to-point layer 2 protocol tunneling for LACP packets on the specified ports.	C	13
l2protocol-tunnel point-to-point pagp	Enables point-to-point layer 2 protocol tunneling for PAgP packets on the specified ports.	C	13
l2protocol-tunnel point-to-point udld	Enables point-to-point layer 2 protocol tunneling for UDLD packets on the specified ports.	C	13
l2protocol-tunnel stp	Enables layer 2 protocol tunneling for STP packets on the specified ports.	C	13
l2protocol-tunnel vtp	Enables layer 2 protocol tunneling for CDP packets on the specified ports.	C	13
l2protocol-tunnel lldp	Enables layer 2 protocol tunneling for Link Layer Discovery Protocol (LLDP) packets on the specified ports.	C	13
no l2protocol-tunnel	Disables layer 2 protocol tunneling for CDP, VTP and STP packets on the specified ports.	C	13
no l2protocol-tunnel cdp	Disables layer 2 protocol tunneling for CDP packets on the specified ports.	C	13
no l2protocol-tunnel point-to-point	Disables point-to-point layer 2 protocol tunneling for LACP, PAgP and UDLD packets on the specified ports.	C	13
no l2protocol-tunnel point-to-point lacp	Disables point-to-point layer 2 protocol tunneling for LACP packets on the specified ports.	C	13
no l2protocol-tunnel point-to-point pagp	Disables point-to-point layer 2 protocol tunneling for PAgP packets on the specified ports.	C	13
no l2protocol-tunnel point-to-point udld	Enables point-to-point layer 2 protocol tunneling for UDLD packets on the specified ports.	C	13
no l2protocol-tunnel stp	Disables layer 2 protocol tunneling for STP packets on the specified ports.	C	13
no l2protocol-tunnel vtp	Disables layer 2 protocol tunneling for VTP packets on the specified ports.	C	13
no l2protocol-tunnel lldp	Disables layer 2 protocol tunneling for Link Layer Discovery Protocol (LLDP) packets on the specified ports.	C	13
l2protocol-tunnel	Enables layer 2 protocol tunneling on the Switch.	C	13
l2protocol-tunnel mac <mac-addr>	Sets the destination MAC address used for encapsulating layer 2 protocol packets received on an access port.	C	13
no l2protocol-tunnel	Disables layer 2 protocol tunneling on the Switch.	C	13
show l2protocol-tunnel	Displays layer 2 protocol tunneling settings and counters for all ports.	E	13
show l2protocol-tunnel interface port-channel *<port-list>*	Displays layer 2 protocol tunneling settings and counters for the specified ports.	E	13

43.2 Command Examples

This example enables L2PT on the Switch and sets the destination MAC address for encapsulating layer 2 protocol packets received on an access port.

```
sysname# configure
sysname(config)# l2protocol-tunnel
sysname(config)# l2protocol-tunnel mac 00:10:23:45:67:8e
sysname(config)#
```

This example enables L2PT for STP, CDP and VTP packets on port 3. It also sets L2PT mode to **access** for this port.

```
sysname(config)# interface port-channel 3
sysname(config-interface)# l2protocol-tunnel
sysname(config-interface)# l2protocol-tunnel mode access
sysname(config-interface)# exit
sysname(config)# exit
```

This example sets L2PT mode to **tunnel** for port 4.

```
sysname(config)# interface port-channel 4
sysname(config-interface)# l2protocol-tunnel mode tunnel
sysname(config-interface)# exit
sysname(config)# exit
```

This example displays L2PT settings and status on port 3. You can also see how many CDP, STP, VTP, LACP, PAgP and UDLD packets received on this port are encapsulated, decapsulated or dropped.

```
sysname# show l2protocol-tunnel interface port-channel 3

Status : Running
Layer 2 Protocol Tunneling: Enable
Destination MAC Address: 00:10:23:45:67:8e

Port  Protocol   State  Encapsulation  Decapsulation     Drop
                            Counter        Counter  Counter
----  --------  ------  -------------  -------------  -------
   3       cdp  Enable              0              0        0
           stp  Enable           1280           2548        0
           vtp  Enable              0              0        0
          lldp  Enable              0              0        0
          lacp  Disable             0              0        0
          pagp  Disable             0              0        0
          udld  Disable             0              0        0
sysname#
```

CHAPTER 44
Link Layer Discovery Protocol (LLDP) Commands

44.1 LLDP Overview

The LLDP (Link Layer Discovery Protocol) is a layer 2 protocol. It allows a network device to advertise its identity and capabilities on the local network. It also allows the device to maintain and store information from adjacent devices which are directly connected to the network device. This helps an administrator discover network changes and perform necessary network reconfiguration and management. The device information is encapsulated in the LLDPDUs (LLDP data units) in the form of TLV (Type, Length, Value). Device information carried in the received LLDPDUs is stored in the standard MIB.

The Switch supports these basic management TLVs.

- End of LLDPDU (mandatory)
- Chassis ID (mandatory)
- Port ID (mandatory)
- Time to Live (mandatory)
- Port Description (optional)
- System Name (optional)
- System Description (optional)
- System Capabilities (optional)
- Management Address (optional)

The Switch also supports the IEEE 802.1 and IEEE 802.3 organizationally-specific TLVs.

Annex F of the LLDP specification defines the following set of IEEE 802.1 organizationally specific TLVs:

- Port VLAN ID TLV (optional)
- Port and Protocol VLAN ID TLV (optional)

Annex G of the LLDP specification defines the following set of IEEE 802.3 Organizationally Specific TLVs:

- MAC/PHY Configuration/Status TLV (optional)
- Power via MDI TLV (optional)
- Link Aggregation TLV (optional)
- Maximum Frame Size TLV (optional)

The optional TLVs are inserted between the Time To Live TLV and the End of LLDPDU TLV.

LLDP-MED (Link Layer Discovery Protocol for Media Endpoint Devices) is an enhanced extension to LLDP especially for voice applications. You can use LLDP-MED to advertise location-based information of emergency calls and/or network policies for voice/video streaming.

44.2 Command Summary

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

Table 135 Interface Command Values

COMMAND	DESCRIPTION
port-list	A list of one or more ports, separated by commas with no spaces. The list may also contain ranges of ports signified by a hyphen. For example: 1,3,5–8,10.

The following section lists the commands for this feature.

Table 136 lldp Command Summary

COMMAND	DESCRIPTION	M	P
`interface port-channel <port-list>`	Enters config-interface mode for configuring the specified ports.	C	13
`lldp admin-status <disabled|tx-only|rx-only|tx-rx>`	Sets LLDP operating mode. `disabled`: the ports cannot send or receive LLDP packets. `tx-only`: the ports can only send LLDP packets. `rx-only`: the ports can only receive LLDP packets. `tx-rx`: the ports can send or receive LLDP packets.	C	13
`lldp basic-tlv management-address`	Enables the sending of Management Address TLVs on the ports.	C	13
`lldp basic-tlv port-description`	Enables the sending of Port Description TLVs on the ports.	C	13
`lldp basic-tlv system-capabilities`	Enables the sending of System Capabilities TLVs on the ports.	C	13
`lldp basic-tlv system-description`	Enables the sending of System Description TLVs on the ports.	C	13
`lldp basic-tlv system-name`	Enables the sending of System Name TLVs on the ports.	C	13

Table 136 lldp Command Summary (continued)

COMMAND	DESCRIPTION	M	P
lldp med location civic [county <*county*>] [city <*city*>] [division <*division*>] [neighbor <*neighbor*>] [street <*street*>] [leading-street-direction <*value*>] [trailing-street-suffix <*value*>] [street-suffix <*value*>] [house-number <*num*>] [house-number-suffix <*value*>] [landmark <*landmark*>] [additional-location <*value*>] [name <*value*>] [zip-code <*value*>] [building <*value*>] [unit <*value*>] [floor <*value*>] [room-number <*value*>] [place-type <*value*>] [postal-community-name <*value*>] [post-office-box <*value*>] [additional-code <*value*>]	Sets civic location information, such as street address and city name.	C	13
lldp med location coordinate [latitude <north|south> <*value*>][longitude <west|east > <*value*>][altitude <meters|floor> <*value*>][datum <WGS84|NAD83-NAVD88|NAD83-MLLW>]	Sets coordinate location information. Latitude *value*: –90º to 90º Longtitude *value*: –180º to 180º Altitude *value*: –2097151 to 2097151 in meters or –2097151 to 2097151 in the number of floors	C	13
lldp med location elin <*number*>	Sets location information of a caller by its ELIN (Emergency Location Identifier Number). *number*: a ten-digit phone number	C	13
lldp med network-policy <voice|voice-signaling|guest-voice|guest-voice-signaling|softphone-voice|video-conferencing|streaming-video|video-signaling> [tagged|untagged][vlan <*vlan-id*>][priority <*priority*>][dscp <*dscp*>]	Sets a network policy for the specified application.	C	13
lldp med topology-change-notification	Enables the sending of LLDP-MED topology change traps when devices are connected to or disconnected from the specified ports.	C	13
lldp notification	Enables the sending of LLDP traps.	C	13
lldp org-specific-tlv dot1 port-protocol-vlan-id	Enables the sending of IEEE 802.1 Port and Protocol VLAN ID TLVs, which contains the VLAN ID and indicates whether the VLAN is enabled and supported.	C	13
lldp org-specific-tlv dot1 port-vlan-id	Enables the sending of IEEE 802.1 Port VLAN ID TLVs, which contains the port's VLAN ID.	C	13

Table 136 lldp Command Summary (continued)

COMMAND	DESCRIPTION	M	P
lldp org-specific-tlv dot3 link-aggregation	Enables the sending of IEEE 802.3 Link Aggregation TLVs, which shows the link aggregation status of the ports.	C	13
lldp org-specific-tlv dot3 mac-phy	Enables the sending of IEEE 802.3 MAC/PHY Configuration/Status TLV, which shows duplex and rate settings and indicates whether auto negotiation is supported on the port.	C	13
lldp org-specific-tlv dot3 max-frame-size	Enables the sending of IEEE 802.3 Maximum Frame Size TLVs on the ports.	C	13
lldp org-specific-tlv dot3 power-via-mdi	Enables the sending of IEEE 802.3 Power via MDI TLVs, which indicates whether power can be supplied through a media dependent interface (MDI) on the ports.	C	13
lldp org-specific-tlv med location	Enables the sending of location TLVs on the ports.	C	13
lldp org-specific-tlv med network-policy	Enables the sending of network policy TLVs on the ports.	C	13
no lldp admin-status	Resets the ports to default setting on sending or receiving LLDP packets.	C	13
no lldp basic-tlv management-address	Disables the sending of Management Address TLVs on the ports.	C	13
no lldp basic-tlv port-description	Disables the sending of Port Description TLVs on the ports.	C	13
no lldp basic-tlv system-capabilities	Disables the sending of System Capabilities TLVs on the ports.	C	13
no lldp basic-tlv system-description	Disables the sending of System Description TLVs on the ports.	C	13
no lldp basic-tlv system-name	Disables the sending of System Name TLVs on the ports.	C	13
no lldp med location	Deletes all location identification.	C	13
no lldp med location <civic|coordinate|elin>	Deletes location identification of the specified type.	C	13
no lldp med network-policy	Deletes network policies for all connected media endpoint devices.	C	13
no lldp med network-policy <voice|voice-signaling|guest-voice|guest-voice-signaling|softphone-voice|video-conferencing|streaming-video|video-signaling>	Deletes network policies for the specified applications.	C	13
no lldp med topology-change-notification	Disables the sending of LLDP-MED topology change traps.	C	13
no lldp notification	Disables the sending of LLDP traps.	C	13
no lldp org-specific-tlv dot1 port-protocol-vlan-id	Disables the sending of IEEE 802.1 Port and Protocol VLAN ID TLVs on the ports.	C	13
no lldp org-specific-tlv dot1 port-vlan-id	Disables the sending of IEEE 802.1 Port VLAN ID TLVs on the ports.	C	13

Table 136 lldp Command Summary (continued)

COMMAND	DESCRIPTION	M	P
no lldp org-specific-tlv dot3 link-aggregation	Disables the sending of IEEE 802.3 Link Aggregation TLVs on the ports.	C	13
no lldp org-specific-tlv dot3 mac-phy	Disables the sending of IEEE 802.3 MAC/PHY Configuration/Status TLVs on the ports.	C	13
no lldp org-specific-tlv dot3 max-frame-size	Disables the sending of IEEE 802.3 Maximum Frame Size TLVs on the ports.	C	13
no lldp org-specific-tlv dot3 power-via-mdi	Disables the sending of IEEE 802.3 Power via MDI TLVs on the ports.	C	13
lldp	Enables the LLDP feature on the Switch.	C	13
lldp reinitialize-delay <1-10>	Sets a number of seconds for LLDP wait to initialize on a port.	C	13
lldp transmit-delay <1-8192>	Sets the delay (in seconds) between the successive LLDPDU transmissions initiated by value or status changes in the Switch MIB.	C	13
lldp transmit-hold <2-10>	Sets the time-to-live (TTL) multiplier of the LLDP packets. The device information on the neighboring devices ages out and is discarded when its corresponding TTL expires. The TTL value is to multiply the TTL multiplier by the LLDP packets transmitting interval. Note: Make sure the LLDP packet transmitting interval is shorter than its TTL to have the Switch's device information being updated in the neighboring devices before it ages out.	C	13
lldp transmit-interval <5-32768>	Sets the interval (in seconds) the Switch waits before sending LLDP packets.	C	13
no lldp	Disables the LLDP feature on the Switch.	C	13
show lldp config	Displays the global LLDP settings on the Switch.	E	3
show lldp config interface port-channel <*port-list*>	Displays the LLDP settings on the specified ports.	E	3
show lldp info local	Displays the Switch's device information.	E	3
show lldp info local interface port-channel <*port-list*>	Displays the LLDP information for the specified ports.	E	3
show lldp info remote	Displays the device information from the neighboring devices.	E	3
show lldp info remote interface port-channel <*port-list*>	Displays the neighboring device information received on the specified ports.	E	3
show lldp statistic	Displays LLDP statistics on the Switch.	E	3
show lldp statistic interface port-channel <*port-list*>	Displays LLDP statistics of the specified ports.	E	3
clear lldp statistic	Resets the LLDP statistics counters to zero.	E	13
clear lldp remote_info	Deletes all device information from the neighboring devices.	E	13
clear lldp remote_info interface port-channel <*port-list*>	Deletes remote device information on the specified ports.	E	13

44.3 Command Examples

This example enables LLDP on the Switch, sets port 2 to send and receive LLDP packets and allows the Switch to send optional basic management TLVs (such as management-address, port-description and system-description TLVs) on port 2. This example also shows the LLDP settings on port 2 and global LLDP settings on the Switch.

```
sysname# configure
sysname(config)# lldp
sysname(config)# interface port-channel 2
sysname(config-interface)# lldp admin-status tx-rx
sysname(config-interface)# lldp basic-tlv management-address
sysname(config-interface)# lldp basic-tlv port-description
sysname(config-interface)# lldp basic-tlv system-description
sysname(config-interface)# exit
sysname(config)# exit
sysname# show lldp config interface port-channel 2
LLDP Port Configuration:
Port    AdminStatus     Notification    BasicTLV   Dot1TLV      Dot3TLV
  2        tx-rx         Disable          P-D-M      --          ----
Basic TLV Flags: (P)Port Description, (N)System Name, (D)System
Description
                (C)System Capabilities, (M)Management Address
802.1 TLV Flags: (P)Port & Protocol VLAN ID, (V)Port VLAN ID
802.3 TLV Flags: (L)Link Aggregation, (M)MAC/PHY Configuration/Status
                (F)Maximun Frame Size, (P)Power Via MDI
sysname# show lldp config
LLDP Global Configuration:
         Active: Yes
Transmit Interval: 30 seconds
  Transmit Hold: 4
 Transmit Delay: 2 seconds
Reinitialize Delay: 2 seconds

sysname#
```

This example shows global Switch LLDP settings.

```
sysname# show lldp config
LLDP Global Configuration:
         Active: No
Transmit Interval: 30 seconds
  Transmit Hold: 4
 Transmit Delay: 2 seconds
Reinitialize Delay: 2 seconds

sysname#
```

The following table describes the labels in this screen.

Table 137 Switch LLDP settings

LABEL	DESCRIPTION
Active	This displays whether LLDP is enabled on the Switch. It is disabled by default.
Transmit Interval	This displays how long the Switch waits before sending LLDP packets.
Transmit Hold	This displays the time-to-live (TTL) multiplier of LLDP frames. The device information on the neighboring devices ages out and is discarded when its corresponding TTL expires. The TTL value is to multiply the TTL multiplier by the LLDP packets transmitting interval.
Transmit Delay	This displays the delay (in seconds) between the successive LLDP PDU transmissions initiated by value or status changes in the Switch MIB.
Reinitialize Delay	This displays the number of seconds for LLDP to wait before initializing on a port.

This example shows LLDP settings on a port.

```
sysname# show lldp config interface port-channel 2
LLDP Port Configuration:
Port    AdminStatus  Notification  BasicTLV  Dot1TLV  Dot3TLV
  2        tx-rx         Disable     -----     --EFA     ----
Basic TLV Flags: (P)Port Description, (N)System Name, (D)System Description
                 (C)System Capabilities, (M)Management Address
802.1 TLV Flags: (P)Port & Protocol VLAN ID, (V)Port VLAN ID
                 (E)DCBX ETS Configuration, (F)DCBX PFC Configuration
                 (A)DCBX Application Priority Configuration
802.3 TLV Flags: (L)Link Aggregation, (M)MAC/PHY Configuration/Status
                 (F)Maximum Frame Size, (P)Power Via MDI
sysname#
```

The following table describes the labels in this screen.

Table 138 LLDP settings on a port

LABEL	DESCRIPTION
Port	This displays the port number with this LLDP configuration.
AdminStatus	This displays whether LLDP transmission and/or reception is allowed on this port.
Notification	This displays whether LLDP notification is enabled on this port.
BasicTLV	This shows which Basic TLC flags are enabled on this port. For example, 'N' is System Name.
Dot1TLV	This shows which 802.1 TLV flags are enabled on this port. For example, 'V' is Port VLAN ID.
Dot3TLV	This shows which 802.3 TLV flags are enabled on this port. For example, 'L' is Link Aggregation.
BasicTLV Flags	The Basic TLV Flags are (P) Port Description, (N) System Name, (D) System Description, (C) System Capabilities, and (M) Management Address.
802.1TLV Flags	The 802.1 TLV Flags are (P) Port & Protocol VLAN ID, (V) Port VLAN ID, (E) DCBX ETS Configuration, (F) DCBX PFC Configuration and (A) DCBX Application Priority Configuration.
802.3TLV Flags	The 802.3 TLV Flags are (L) Link Aggregation, (M) MAC/PHY Configuration/Status, (F) Maximum Frame Size, and (P) Power via MDI.

This example shows global Switch LLDP statistics.

```
sysname# show lldp statistic
LLDP Global Statistic:
Neighbor Entries List Last Update:     0:00:00
New Neighbor Entries Count: 0
Neighbor Entries Deleted Count: 0
Neighbor Entries Dropped Count: 0
Neighbor Entries Ageout Count: 0

sysname#
```

The following table describes the labels in this screen.

Table 139 Switch LLDP statistics

LABEL	DESCRIPTION
Neighbor Entries List Last Update	This displays the time the LLDP database was last updated for this and neighboring Switches.
New Neighbor Entries Count	This displays the number of new neighbors added to the LLDP database since the last update.
Neighbor Entries Deleted Count	This displays the number of neighbors deleted from the LLDP database since the last update.
Neighbor Entries Dropped Count	This displays the number of neighbors dropped from the LLDP database since the last update.
Neighbor Entries Ageout Count	This displays the number of neighbors with expired TTLs since the last update.

This example shows LLDP statistics on a port

```
sysname# show lldp statistic interface port-channel 1
LLDP Port Statistic:
        Local Port: 1
Frames Discarded: 0
 Frames Invalid: 0
Frames Received: 0
    Frames Sent: 0
TLVs Unrecognized: 0
 TLVs Discarded: 0
Neighbor Ageouts: 0

sysname#
```

The following table describes the labels in this screen.

Table 140 LLDP statistics on a port

LABEL	DESCRIPTION
Local Port	This displays the port number with these LLDP statistics.
Frames Discarded	This displays the number of discarded frames on this port.
Frames Invalid	This displays the number of invalid frames on this port.
Frames Received	This displays the number of frames received on this port.
Frames Sent	This displays the number of frames sent on this port.
TLVs Unrecognized	This displays the number of unrecognized TLVS on this port.
TLVs Discarded	This displays the number of discarded TLVs on this port.
Neighbor Ageouts	This displays the number of neighbors with expired TTLs on this port.

This example shows local Switch (the Switch you are accessing) LLDP information.

```
sysname# show lldp info local
LLDP Global Local Device Information:
Chassis ID Subtype:          mac-address
     Chassis ID:    00:19:cb:00:00:02
    System Name:               sysname
System Description: V4.00(AAEW.0)b7 | 12/11/2012
System Capabilities Supported: Bridge
System Capabilities Enabled: Bridge
Management Address :
        Management Address Subtype: ipv4 / all-802
        Interface Number Subtype:    unknown
        Interface Number: 0
        Object Identifier: 0

sysname#
```

The following table describes the labels in this screen.

Table 141 Local LLDP Information

LABEL	DESCRIPTION
LLDP Global Local Device Information	This contains the chassis ID subtype, chassis ID, and system name.
System Description	This shows the firmware version number and date released.
System Capabilities Supported	This shows what functionality the Switch supports.
System Capabilities Enabled	This shows what functionality is enabled on the Switch.
Management Address	This contains the management address subtype, interface number subtype, interface number, and object identifier.

This example shows local Switch (the Switch you are accessing) LLDP information on a port.

```
sysname# show lldp info local interface port-channel 2
LLDP Local Device Information Detail:
        Local Port:          2
Port ID Subtype: local-assigned
        Port ID:          2
Port Description:
Extended TLV Info 802.1 OUI (hex value) = 00-80-c2
-Port VLAN ID
                    -ID:     1
-DCBX Application Priority
        -    ether-type:   fcoe    Priority:     2
-DCBX ETS Configuration
           -Willing Bit: False
        -Max Traffic Classes:     3
        -Priority-Group  2:     Strict-priority, Priority-list:7
        -Priority-Group  1:     ETS Bandwidth  50%, Priority-list:3-6
        -Priority-Group  0:     ETS Bandwidth  50%, Priority-list:0-2
-DCBX PFC Configuration
           -Willing Bit:  True
        -PFC capability:     8
        -Priority enable list: 0-2
Extended TLV Info 802.3 OUI (hex value) = 00-12-0f
-MAC PHY Configuration & Status
          -AN Supported:     Y
            -AN Enabled:     Y
        -AN Advertised Capability:  1000baseTFD
         -Oper MAU type: 30
-Link Aggregation
            -Capability:     Y
                -Status:     N
               -Port ID:     2
-Max Frame Size
            -Frame Size:  1518
-------------------------------------------------

sysname#
```

The following table describes the labels in this screen.

Table 142 Local Switch LLDP information on a port

LABEL	DESCRIPTION
LLDP Local Device Information Detail	This displays the local port, port ID, and port description.
Port VLAN ID	This displays the VLAN ID for this port.
DCBX Application Priority	This displays the priority given to FCoE traffic on the Switch.
DCBX ETS Configuration	This displays the Willing Bit, Max Traffic Classes, and Traffic Class binding for each priority.
DCBX PFC Configuration	This displays the Willing Bit, PFC capability, and priority enable list.
MAC PHY Configuration & Status	This displays the AN Supported, AN Enabled, AN Advertised Capability, Open MAU type
Link Aggregation	This displays the capability, status, and port ID.
Max Frame Size	This displays the maximum frame size on this port.

This example shows remote Switch (the Switch connected to the port on the Switch you are accessing) LLDP information.

```
sysname# show lldp info remote interface port-channel 2
LLDP Remote Device Information Detail:
        Local Port:          2
Chassis ID Subtype: mac-address
     Chassis ID: 00:19:cb:00:00:02
Port ID Subtype: local-assigned
        Port ID:         47
   Time To Live:        120
Extended TLV Info 802.1 OUI (hex value) = 00-80-c2
-Port VLAN ID
                    -ID:     1
-DCBX Application Priority
             ether-type:  fcoe    Priority:     2
-DCBX ETS Configuration
           -Willing Bit: False
        -Max Traffic Classes:     3
        -Priority-Group  7:     Strict-priority, Priority-list:-
        -Priority-Group  6:     Strict-priority, Priority-list:-
        -Priority-Group  5:     Strict-priority, Priority-list:-
        -Priority-Group  4:     Strict-priority, Priority-list:-
        -Priority-Group  3:     Strict-priority, Priority-list:-
        -Priority-Group  2:     Strict-priority, Priority-list:7
        -Priority-Group  1:     ETS Bandwidth  50%, Priority-list:3-6
        -Priority-Group  0:     ETS Bandwidth  50%, Priority-list:0-2
-DCBX PFC Configuration
           -Willing Bit:  True
        -PFC capability:     8
        -Priority enable list: 0-2
Extended TLV Info 802.3 OUI (hex value) = 00-12-0f
-Max Frame Size
            -Frame Size:  1518
------------------------------------------------
sysname#
```

The following table describes the labels in this screen.

Table 143 Remote Switch LLDP information

LABEL	DESCRIPTION
LLDP Remote Device Information Detail	This contains the following information:
Local Port	This is the local port number which receives the LLDPDU from the remote Switch.
Chassis ID Subtype	This displays how the chassis of the remote Switch is identified.
Chassis ID	This displays the chassis ID of the remote Switch. The chassis ID is identified by the chassis ID subtype.
Port ID Subtype	This displays how the port is identified.
Port ID	This is the ID of the remote Switch.
Time To Live	This displays the time-to-live (TTL) multiplier of LLDP frames. The device information on the neighboring devices ages out and is discarded when its corresponding TTL expires. The TTL value is to multiply the TTL multiplier by the LLDP frames transmitting interval.
Extended TLV Info 802.1 OUI (hex value)	The 802.1 organizationally specific TLVs start with the 24-bit organizationally unique identifier (OUI) and a 1 byte organizationally specific subtype followed by data. Each organization is responsible for managing their subtypes.
Port VLAN ID	This TLV displays the VLAN ID for the remote Switch.

Table 143 Remote Switch LLDP information (continued)

LABEL	DESCRIPTION
DCBX Application Priority	This TLV displays the priority given to FCoE traffic on the remote Switch.
DCBX ETS Configuration	This TLV displays the willing bit, ETS capability and traffic class settings configured by ETS on the remote Switch.
DCBX PFC Configuration	This TLV displays the willing bit, PFC capability, and enabled priority list configured by PFC on the remote Switch.
Extended TLV Info 802.3 OUI (hex value)	The 802.3 organizationally specific TLVs start with the 24-bit organizationally unique identifier (OUI) and a 1 byte organizationally specific subtype followed by data. Each organization is responsible for managing their subtypes.
Max Frame Size	This TLV displays the maximum transmission unit (MTU) sent by the remote Switch.

CHAPTER 45
Load Sharing Commands

45.1 Load Sharing Overview

The Switch learns the next-hops using ARP and determines routing paths for a destination. The Switch supports Equal-Cost MultiPath (ECMP) to forward packets destined to the same device through different routing paths of equal path cost. This allows you to balance or share traffic loads between multiple routing paths when the Switch is connected to more than one next-hop. ECMP works with static routes or a routing protocol, such as OSPF.

With ECMP, packets are routed through the paths of equal cost according to the hash algorithm output.

The maximum number of paths for one ECMP (Equal-Cost MultiPath) route varies by Switch. A smaller number of maximum-paths means more ECMP routes are allowed and a larger number of maximum-paths means fewer ECMP routes are allowed.

The number of paths for a static route for ECMP cannot be bigger than the maximum-paths value.

Throughput may be influenced while configuring ECMP maximum-paths.

45.2 Command Summary

The following section lists the commands for this feature.

Table 144 load-sharing Command Summary

COMMAND	DESCRIPTION	M	P
`ip load-sharing`	Enables load sharing on the Switch.	C	13
`ip load-sharing <sip|sip-dip>`	Sets the criteria the Switch uses to determine the routing path for a packet. `sip`: the Switch uses a hash algorithm to convert a packet's source IP address into a hash value which acts as an index to a route path. `sip-dip`: the Switch uses a hash algorithm to convert a packet's source and destination IP addresses into a hash value which acts as an index to a route path.	C	13
`ip load-sharing aging-time <0-86400>`	Sets the time interval (from 0 to 86400 in increments of 10) in seconds at which the Switch sends an ARP request to update a resolved next-hop's MAC address.	C	13
`ip load-sharing discover-time <0-86400>`	Sets the time interval (from 0 to 86400 in increments of 10) in seconds at which the Switch sends an ARP request to update an unresolved next-hop's MAC address.	C	13

Table 144 load-sharing Command Summary (continued)

COMMAND	DESCRIPTION	M	P
ip load-sharing maximum-path	Set the maximum number of paths for one ECMP (Equal-Cost MultiPath) route.	C	13
no ip load-sharing	Disables load sharing on the Switch.	C	13

45.3 Command Examples

This example enables Equal-Cost MultiPath (ECMP) routing on the Switch and sets the Switch to use a packet's source and destination IP addresses to determine the routing path for the packet.

```
sysname# configure
sysname(config)# ip load-sharing
sysname(config)# ip load-sharing sip-dip
sysname(config)#
```

CHAPTER 46
Logging Commands

Use these commands to manage system logs.

46.1 Command Summary

The following section lists the commands for this feature.

Table 145 logging Command Summary

COMMAND	DESCRIPTION	M	P
`show logging`	Displays system logs. Press [CTRL]+C to terminate the process.	E	3
`show logging | begin <string>`	Displays system logs, which start from a line with the specified string.	E	3
`show logging | begin <string1> include <string2>`	Displays system logs, which start from a line with the first specified string and also contain the second specified string.	E	3
`show logging | include <string>`	Displays system logs, which contain the specified string.	E	3
`show logging | refresh`	Displays system logs, and updates every second until you press the [ESC] button.	E	3
`clear logging`	Clears system logs.	E	13

46.2 Command Examples

This example displays the system logs.

```
sysname# show logging
     1 2020-01-01T07:08:22Z IN authentication: SSH user admin login [IP address =
172.21.40.29]
     2 2020-01-01T05:47:42Z DE interface: Port 20 link up 1G/F
     3 2020-01-01T05:41:47Z DE interface: Port 20 link down
     4 2020-01-01T04:41:00Z IN authentication: HTTP(s) user admin login [IP address
= 172.21.40.31]
     5 2020-01-01T01:58:03Z IN authentication: HTTP(s) user admin login [IP address
= 172.21.40.31]
     6 2020-01-01T00:01:36Z ER system: Gets the time and date from a time server
failed
     7 2020-01-01T00:00:56Z WA interface: port 18 link speed and duplex mode
autonegotiation has recovered to normal state
     8 2020-01-01T00:00:56Z DE interface: Port 18 link up 100M/F
     9 2020-01-01T00:00:46Z WA interface: port 18 link speed and duplex mode
autonegotiation has failed
    10 2020-01-01T00:00:39Z DE interface: Port 20 link up 1G/F
    11 2020-01-01T00:00:32Z NO system: System cold start
```

CHAPTER 47
Login Account Commands

Use these commands to configure login accounts on the Switch.

47.1 Password Encryption

See Section 62.1 on page 248 for information on this feature.

47.2 Command Summary

The following section lists the commands for this feature.

Table 146 logins Command Summary

COMMAND	DESCRIPTION	M	P
`show logins`	Displays login account information.	E	3
`logins username <name> password [cipher] <password> [privilege <0-14>]`	Creates account with the specified user name and sets the password and privilege. The privilege level is applied the next time the user logs in. *name*: 1 – 32 alphanumeric characters. *password*: (for Switch models that do not support Password Complexity) 1 – 32 alphanumeric characters except [?], [|], ['], ["], [space], or [,]. *password*: (for Switch models that support Password Complexity) When Password Complexity is disabled: • 4 to 32 characters in length When Password Complexity is enabled: • 9 to 32 characters in length • Include at least three of these: numbers, uppercase letters, lowercase letters, and special characters (for example, 'Ea5yPas5W0rd') • Cannot match your login username • Cannot use the same character (case insensitive) or number three or more times in a row (for example, '777', 'AaA') • Cannot use four or more sequential keyboard characters (case insensitive) or numbers (for example, 'qWer', '1234'), and • Cannot use the present password again. [?], [|], ['], ["], [,], [[ ], [ ]] and space are not allowed whether Password Complexity is enabled or disabled. See Table on page 252 for more information on Password Complexity. *cipher*: inform the Switch that the string after the word "cipher" is an encrypted secret. This is used for password encryption. To encrypt the password, use the `password encryption` command.	C	14
`logins username <name> privilege <0-14> password`	password: inform the Switch to hide the password characters you entered (interactive mode).	C	14
`no logins username <name>`	Removes the specified account.	C	14
`show logins lockout`	Displays IP address login lockout configuration information.	E	3
`logins lockout`	Enables the Switch to detect and block multiple failed login attempts from the same IP address.	C	13
`no logins lockout`	Disables the Switch from detecting and blocking multiple failed login attempts from the same IP address.	C	13
`logins lockout block-period`	Set the time (from 1 to 65535 minutes) the IP address that exceeded the `logins lockout retry-count` will be stopped from trying to log in again (default is 5 minutes).	C	13

Table 146 logins Command Summary (continued)

COMMAND	DESCRIPTION	M	P
logins lockout retry-count	Set the number of login attempts (from 1 to 99) for an IP address (default is 5 attempts).	C	13
logins lockout attempt-timeout	Set the time (from 1 to 65535 minutes) if the login attempts exceed the logins lockout retry-count, to stop the IP address from trying to log in again (default is 5 minutes).	C	13

47.3 Command Examples

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

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

This example configures the IP address login lockout. For example, the Switch will block all logins from the same IP address for 30 minutes if there are 4 failed attempts within 30 minutes. The IP address cannot try to log in to the Switch until the logins lockout block period expires.

```
sysname# config
sysname(config)# logins lockout
sysname(config)# logins lockout block-period 30
sysname(config)# logins lockout retry-count 4
sysname(config)# logins lockout attempt-timeout 30
```

This example removes the IP address login lockout.

```
sysname# config
sysname(config)# no logins lockout
```

This example shows information about the IP address login lockout configuration.

```
sysname# show logins lockout
User IP Lockout Information
 Status                    :Enabled
 Block Period              :30 minutes
 Retry Count               :4
 Attempt Timeout           :30 minutes

 NO. Lockout IP
 --- ----------
```

CHAPTER 48
Loopguard Commands

48.1 Loopguard Overview

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.

48.2 Command Summary

The following section lists the commands for this feature.

Table 147 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 ports. The port list may consist of one or more ports, separated by commas with no spaces. The list may also contain ranges of ports signified by a hyphen. For example: 1,3,5–8,10.	C	13
`loopguard`	Enables the loopguard feature on the ports. 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. Note: The loop guard feature cannot be enabled on the ports that have Spanning Tree Protocol (RSTP, MRSTP or MSTP) enabled.	C	13
`no loopguard`	Disables the loopguard feature on the ports.	C	13
`clear loopguard`	Clears loopguard counters.	E	13

48.3 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 148 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.

CHAPTER 49
MAC Address Commands

49.1 MAC Address Commands Overview

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.

49.2 Command Summary

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

Table 149 Interface Command Values

COMMAND	DESCRIPTION
port-list	A list of one or more ports, separated by commas with no spaces. The list may also contain ranges of ports signified by a hyphen. For example: 1,3,5–8,10.

The following section lists the commands for this feature.

Table 150 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 <10-1000000>	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 mac <mac-addr>	Displays a specified MAC entry.	E	3
show mac address-table multicast	Displays the Multicast MAC addresses learned by the Switch. Note: The result may include the information learned from IPv4 Multicast IP (except for XGS2220, XMG1930, XS1930 and GS2220 series).	E	3
show mac address-table port <*port-list*> [<*sort*>]	Displays the MAC address table for the specified ports. Sorted by MAC, Port or VID. *sort*: MAC, VID, or PORT.	E	3

Table 150 mac, mac-aging-time, and mac-flush Command Summary (continued)

COMMAND	DESCRIPTION	M	P
show mac address-table static	Displays the static MAC address table.	E	3
show mac address-table trunk <*trunk-list*>	Displays all MAC addresses learned from the ports in the specified trunk groups.	E	3
show mac address-table vlan <*vlan-list*> [<*sort*>]	Displays the MAC address table for the specified VLANs. Optionally, sorted by MAC, Port or VID. *sort*: MAC, VID, 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
mac-transfer dynamic-to-filter mac <*mac-addr*>	Displays and changes a dynamically learned MAC address entry into a MAC filtering entry.	C	13
mac-transfer dynamic-to-filter interface port-channel <*port-list*>	Displays and changes all dynamically learned MAC address entries on the specified ports into MAC filtering entries.	C	13
mac-transfer dynamic-to-filter vlan <*vlan-list*>	Displays and changes all dynamically learned MAC address entries in the specified VLANs into MAC filtering entries.	C	13
mac-transfer dynamic-to-forward mac <*mac-addr*>	Displays and changes a dynamically learned MAC address entry into a MAC forwarding entry.	C	13
mac-transfer dynamic-to-forward interface port-channel <*port-list*>	Displays and changes all MAC addresses dynamically learned on the specified ports into static MAC addresses.	C	13
mac-transfer dynamic-to-forward vlan <*vlan-list*>	Displays and changes all dynamically learned MAC addresses in the specified VLANs into static MAC addresses.	C	13

49.3 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 151 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.

Table 151 show mac address-table (continued)

LABEL	DESCRIPTION
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 52 on page 208).

CHAPTER 50
MAC-based VLAN

50.1 MAC-based VLAN Overview

Use these commands to bind a client source MAC address to a VLAN on the Switch.

The MAC-based VLAN feature assigns incoming untagged packets to a VLAN and classifies the traffic based on the source MAC address of the packet. When untagged packets arrive at the Switch, the source MAC address of the packet is looked up in a MAC to VLAN mapping table.

If an entry is found, the corresponding VLAN ID is assigned to the packet. The assigned VLAN ID is verified against the VLAN table. If the VLAN is valid, ingress processing on the packet continues; otherwise, the packet is dropped.

This feature allows users to change ports without having to reconfigure the VLAN, which allows better mobility. You can assign priority to the MAC-based VLAN and define a MAC to VLAN mapping table by entering a specified source MAC address in the MAC-based VLAN using a command. You can also delete a MAC-based VLAN entry using a command described below.

50.2 Command Summary

The following section lists the commands for this feature.

Table 152 MAC-based VLAN Command Summary

COMMAND	DESCRIPTION	M	P
`mac-based-vlan name <name> source-mac <mac-addr> vlan <vlan-id> priority <0-7>`	Adds a binding client source MAC address to a VLAN and sets priority level. Name: 1 – 32 alphanumeric characters	C	13
`no mac-based-vlan source-mac <mac-addr>`	Removes a binding client source MAC address to a VLAN.	C	13
`show mac-based-vlan`	Show status of the MAC-based VLAN.	E	13

50.3 Command Example: add source MAC address

This example adds a binding source MAC address to a MAC-based VLAN with MAC address 00:11:22:33:44:55, VLAN ID number 3 and priority level 6.

```
sysname(config)# mac-based-vlan name test source-mac 00:11:22:33:44:55 vlan
3 priority 6
sysname(config)
sysname(config)# exit
sysname# show mac-based-vlan
Index     Name     Source MAC         VLAN   Priority
1         test     00:11:22:33:44:55     3          6
```

50.4 Command Example: remove source MAC address

This example deletes a binding source MAC address to a MAC-based VLAN with MAC address 00:11:22:33:44:55.

```
sysname(config)# no mac-based-vlan source-mac 00:11:22:33:44:55
sysname(config)# exit
```

CHAPTER 51
MAC Filter Commands

51.1 MAC Filter Overview

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

Note: Use the running configuration commands to look at the current MAC filter settings. See Chapter 78 on page 313.

Note: 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 51.3 on page 207 and Section 51.4 on page 207 for examples.

51.2 Command Summary

The following section lists the commands for this feature.

Table 153 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 <name> mac <mac-addr> vlan <vlan-id> drop <src|dst|both>`	Specifies the source and or destination filter parameters.	C	13

51.3 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
```

51.4 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
```

CHAPTER 52
MAC Forwarding Commands

52.1 MAC Forwarding Overview

Use these commands to configure static MAC address forwarding.

Note: Use the `mac` commands to look at the current `mac-forward` settings. See Chapter 49 on page 201.

52.2 Command Summary

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

Table 154 mac-forward User-input Values

COMMAND	DESCRIPTION
name	1 – 32 alphanumeric characters

The following section lists the commands for this feature.

Table 155 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

CHAPTER 53
MAC Pinning Commands

53.1 MAC Pinning Overview

Use these commands to configure MAC pinning to set a port or multiple ports to have priority over other ports in MAC address learning. That means when a MAC address (and VLAN ID) is learned on a MAC-pinning-enabled port, the MAC address will not be learned on any other port until the aging time for the dynamically learned MAC address in the table expires.

53.2 Command Summary

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

Table 156 Interface Command Values

COMMAND	DESCRIPTION
port-list	A list of one or more ports, separated by commas with no spaces. The list may also contain ranges of ports signified by a hyphen. For example: 1,3,5-8,10.

The following section lists the commands for this feature.

Table 157 mac-pinning Command Summary

COMMAND	DESCRIPTION	M	P
mac-pinning	Enables MAC pinning on the Switch.	C	13
no mac-pinning	Disables MAC pinning on the Switch.	C	13
interface port-channel <*port-list*>	Enters config-interface mode for the specified ports.	C	13
mac-pinning	Enables MAC pinning on the specified ports.	C	13
no mac-pinning	Disables MAC pinning on the specified ports.	C	13
show mac-pinning	Displays MAC pinning settings	E	3

53.3 Command Examples

This example enables MAC pinning on the Switch and port 3. It also shows the MAC pinning status.

```
sysname(config)# interface port-channel 3
sysname(config-interface)# mac-pinning
sysname(config-interface)# exit
sysname(config)# exit
sysname# show mac-pinning

  MAC Pinning Status: Enable

  Port    Active
  ----  --------
     1        No
     2        No
     3       Yes
     4        No
     5        No
     6        No
     7        No
     8        No
     9        No
    10        No
    11        No
    12        No
    13        No
    14        No
    15        No
    16        No
    17        No
    18        No
    19        No
    20        No
    21        No
    22        No
    23        No
    24        No
    25        No
    26        No
    27        No
    28        No
sysname#
```

CHAPTER 54
Mirroring Commands

54.1 Mirroring Overview

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

In local port mirroring, the mirroring ports (through which traffic you copy passes) and the monitor port are on the same device.

In remote port mirroring (RMirror), the mirroring ports and monitor port can be on different devices in a network. You can use it to monitor multiple switches across your network. The traffic from the source device's mirroring ports is sent to a reflector port for VLAN tagging and copied to the connected ports. Traffic are then carried over the specified remote port mirroring (RMirror) VLAN and sent to the destination device's monitor port through the connected ports that connect to other switches.

Single-Destination RMirror

If the mirrored traffic is forwarded to one single destination switch, you can disable the reflector port. The Switch adds RMirror VLAN tag and forwards mirrored traffic from the mirroring port to the connected port directly.

Multi-Destination RMirror

If you configure more than one connected port on the source switch to forward the mirrored traffic to multiple destination switches, you must enable a reflector port on the source switch.

Note: Use the running configuration commands to look at the current mirror settings. See Chapter 78 on page 313.

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

54.2 Command Summary

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

Table 158 Interface Command Values

COMMAND	DESCRIPTION
port-list	A list of one or more ports, separated by commas with no spaces. The list may also contain ranges of ports signified by a hyphen. For example: 1,3,5–8,10.

The following section lists the commands for this feature.

Table 159 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
no mirror-port <*port-num*>	Removes the specified monitor port. *port-num*: in a modular switch, enter the port number preceded by a slot number and backslash (/). For example, 3/11 indicates port 11 on the card in the third slot.	C	13
interface port-channel <*port-list*>	Enters config-interface mode for the specified ports. *port-list*: in a modular switch, enter the port number preceded by a slot number and backslash (/). For example, 3/11 indicates port 11 on the card in the third slot. Use a comma (,) to separate individual ports or a dash (-) to indicates a range of ports. For example, "3/11,4/5" or "3/7-3/9".	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 ports.	C	13

Table 160 mirror-filter Command Summary

COMMAND	DESCRIPTION	M	P
mirror-filter egress mac <*mac-addr*>	Copies outgoing frames with the specified source or destination MAC address from mirrored ports to the monitor port.	C	13
mirror-filter egress type <all|dest|src>	This command works with the previous command, mirror-filter egress mac. all: Specifies that the Switch should copy all outgoing traffic from mirrored ports. dest: Specifies that the Switch should copy all outgoing traffic with the specified destination MAC address from mirrored ports. src: Specifies that the Switch should copy outgoing traffic with the specified source MAC address from mirrored ports.	C	13
mirror-filter ingress mac <*mac-addr*>	Copies incoming frames matching with the specified source or destination MAC address from mirrored ports to the monitor port.	C	13

Table 160 mirror-filter Command Summary (continued)

COMMAND	DESCRIPTION	M	P
mirror-filter ingress type <all|dest|src>	This command works with the previous command, mirror-filter ingress mac. all: Specifies that the Switch should copy all outgoing traffic from mirrored ports. dest: Specifies that the Switch should copy all incoming traffic with the specified destination MAC address from mirrored ports. src: Specifies that the Switch should copy all incoming traffic with the specified source MAC address from mirrored ports.	C	13
show mirror	Displays mirror settings of the Switch.	E	3

Table 161 rmirror Command Summary

COMMAND	DESCRIPTION	M	P
rmirror vlan <*vlan-id*>	Enters config-rmirror mode to create a remote port mirroring (RMirror) VLAN through which the mirrored traffic is forwarded.	C	13
connected-port <*port-list*>	Sets the ports that helps forward mirrored traffic to other connected switches and/or receive mirrored traffic from other connected port in the same RMirror VLAN.	C	13
no connected-port <*port-list*>	Removes the specified connected ports from this RMirror VLAN.	C	13
destination monitor-port <*port-num*> <untagged|tagged>	Sets the port to which you copy the traffic in order to examine it in more detail without interfering with the traffic flow on the original ports. You can also set whether to add the RMirror VLAN tag to mirrored traffic on the monitor port.	C	13
no destination monitor-port	Removes the destination monitor port from this RMirror VLAN.	C	13
inactive	Disables the RMirror VLAN.	C	13
no inactive	Enables the RMirror VLAN.	C	13
source 8021p-priority <0 - 7>	Sets the priority of the mirrored traffic in this VLAN.	C	13
source mirror-port <*port-list*> dir <ingress|egress|both>	Sets the ports on which traffic is mirrored and the traffic flow to be copied to the monitor port when the Switch is the source device in remote port mirroring.	C	13
no source mirror-port <*port-list*>	Sets the Switch to not mirror any traffic on the specified ports.	C	13
no source mirror-port <*port-list*> dir egress	Sets the Switch to not mirror outgoing (egress) traffic on the specified ports.	C	13
no source mirror-port <*port-list*> dir ingress	Sets the Switch to not mirror incoming (ingress) traffic on the specified ports.	C	13
source reflector-port	Enables the source reflector port.	C	13
source reflector-port <*port-num*>	Sets the port that adds the RMirror VLAN tag to all mirrored traffic and forwards traffic to the connected ports in the same RMirror VLAN.	C	13
no source reflector-port	Removes the source reflector port.	C	13
no rmirror vlan <*vlan-id*>	Removes the specified RMirror VLAN.	C	13

Table 161 rmirror Command Summary (continued)

COMMAND	DESCRIPTION	M	P
show rmirror vlan	Displays all RMirror VLANs settings on the Switch.	E	3
show rmirror vlan <*vlan-id*>	Displays the specified RMirror VLAN settings.	E	3

54.3 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
```

This example displays the mirror settings of the Switch after you configured in the example above.

```
sysname# show mirror
     Mirroring:  enable
  Monitor port:  3

   Mirrored port: 1,4-6
         Ingress:
          Egress: 1,4-6
            Both:
```

This example creates an RMirror VLAN with a VLAN ID of 200 on the Switch, sets port 6 as the reflector port and sets the priority of mirrored traffic to 3 in this RMirror VLAN when the Switch is the source device.

This example also specifies the ports (4 and 5) on which traffic will be mirrored and shows the RMirror VLAN settings.

```
sysname# configure
sysname(config)# rmirror vlan 200
sysname(config-rmirror)# source reflector-port 6
sysname(config-rmirror)# source reflector-port
sysname(config-rmirror)# source 8021p-priority 3
sysname(config-rmirror)# source mirror-port 4,5
sysname(config-rmirror)# exit
sysname(config)# exit
sysname# show rmirror vlan 200
  RMirror VLAN:200      Active=Yes
  ---------------------------------------
  Source
        802.1p priority         :3
        Mirror-port             :
                Ingress         :
                Egress          :
                Both            :4-5
        Reflector-port
                Active          :Yes
                Port            :6
  Destination
        Monitor-port            :
  Connected-port                :

sysname#
```

CHAPTER 55
MRSTP Commands

55.1 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 83 on page 333 for information on RSTP commands and Chapter 56 on page 219 for information on MSTP commands.

55.2 Command Summary

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

Table 162 Interface Command Values

COMMAND	DESCRIPTION
port-list	A list of one or more ports, separated by commas with no spaces. The list may also contain ranges of ports signified by a hyphen. For example: 1,3,5–8,10.

The following section lists the commands for this feature.

Table 163 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 MRSTP 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 MRSTP configuration.	C	13
mrstp <*tree-index*> priority <0-61440>	Sets the bridge priority of the Switch for the specified MRSTP configuration.	C	13

Table 163 Command Summary: mrstp (continued)

COMMAND	DESCRIPTION	M	P
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 MRSTP configuration.	C	13
mrstp interface <*port-list*>	Activates MRSTP on the specified ports.	C	13
mrstp interface <*port-list*> edge-port	Sets the specified ports as edge ports. This allows the port to transition to a forwarding state immediately without having to go through the listening and learning states. Note: An edge port becomes a non-edge port as soon as it receives a Bridge Protocol Data Units (BPDU).	C	13
no mrstp interface <*port-list*> edge-port	Sets the listed ports as non-edge ports.	C	13
mrstp interface <*port-list*> path-cost <0-200000000>	Sets a path cost to the specified ports. It is recommended you assign it according to the speed of the link. Note: If you set the value to '0', the Switch will use the auto path cost you set using the auto-path-cost command. See Section 83.1 on page 333 for more information.	C	13
mrstp interface <*port-list*> priority <0-255>	Sets the priority value to the specified ports for MRSTP.	C	13
mrstp interface <*port-list*> rootguard	Enables root guard on the specified port in order to prevent the switches attached to the port from becoming the root bridge.	C	13
no mrstp interface <*port-list*> rootguard	Disables root guard on a port.	C	13
mrstp interface <*port-list*> tree-index <*tree-index*>	Assigns the specified port list to a specific MRSTP configuration.	C	13
no mrstp <*tree-index*>	Disables the specified MRSTP configuration.	C	13
no mrstp interface <*port-list*>	Disables the MRSTP assignment from the specified ports.	C	13

55.3 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
```

In this example, we enable MRSTP on ports 21–24. Port 24 is connected to the host while ports 21–23 are connected to another switch.

```
sysname(config)# configure
sysname(config)# spanning-tree mode MRSTP
sysname(config)# mrstp 1
sysname(config)# mrstp interface 21-24
sysname(config)# no mrstp interface 21-23 edge-port
```

CHAPTER 56
MSTP Commands

56.1 MSTP Overview

Multiple Spanning Tree Protocol (IEEE 802.1s) is backward compatible with STP/RSTP and addresses the limitations of existing spanning tree protocols (STP and RSTP) in networks to include the following features:

- One Common and Internal Spanning Tree (CIST) that represents the entire network's connectivity.
- Grouping of multiple bridges (or switching devices) into regions that appear as one single bridge on the network.
- A VLAN can be mapped to a specific Multiple Spanning Tree Instance (MSTI). MSTI allows multiple VLANs to use the same spanning tree.
- Load-balancing is possible as traffic from different VLANs can use distinct paths in a region.

56.2 Command Summary

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

Table 164 Interface Command Values

COMMAND	DESCRIPTION
port-list	A list of one or more ports, separated by commas with no spaces. The list may also contain ranges of ports signified by a hyphen. For example: 1,3,5–8,10.

The following section lists the commands for this feature.

Table 165 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

Table 165 mstp Command Summary (continued)

COMMAND	DESCRIPTION	M	P
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
mstp interface port-channel <*port-list*> edge-port	Sets the specified ports as edge ports. This allows the port to transition to a forwarding state immediately without having to go through the listening and learning states. Note: An edge port becomes a non-edge port as soon as it receives a Bridge Protocol Data Units (BPDU).	C	13
no mstp interface port-channel <*port-list*> edge-port	Sets the listed ports as non-edge ports.	C	13
mstp interface port-channel <*port-list*> rootguard	Enables root guard on the specified port in order to prevent the switches attached to the port from becoming the root bridge.	C	13
no mstp interface port-channel <*port-list*> rootguard	Disables root guard on a port.	C	13

Table 166 mstp instance Command Summary

COMMAND	DESCRIPTION	M	P
show mstp instance <*number*>	Displays the specified MSTP instance configuration.	E	3
no mstp instance <*number*>	Disables the specified MSTP instance on the Switch.	C	13
mstp instance <*number*> priority <0-61440>	Specifies the bridge priority of the instance. priority: Must be a multiple of 4096.	C	13
mstp instance <*number*> vlan <*vlan-list*>	Specifies the VLANs that belongs to the instance.	C	13
no mstp instance <*number*> vlan <1-4094>	Disables the assignment of specific VLANs from an MST instance.	C	13
mstp instance <*number*> interface port-channel <*port-list*>	Specifies the ports you want to participate in this MST instance.	C	13
no mstp instance <*number*> interface port-channel <*port-list*>	Disables the assignment of specific ports from an MST instance.	C	13

Table 166 mstp instance Command Summary (continued)

COMMAND	DESCRIPTION	M	P
mstp instance <*number*> interface port-channel <*port-list*> path-cost <0-200000000>	Sets a path cost to the specified ports. It is recommended you assign it according to the speed of the link. Note: If you set the value to '0', the Switch will use the auto path cost you set using the auto-path-cost command. See Section 83.1 on page 333 for more information.	C	13
mstp instance <*number*> interface port-channel <*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

56.3 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
  (e)TransmissionLimit:         3
  (f)ForceVersion:              3
  (g)MST Configuration ID
     Format Selector:           0
     Configuration Name:        001349aefb7a
     Revision Number:           0
     Configuration Digest:      0xAC36177F50283CD4B83821D8AB26DE62
     msti       vlans mapped
     ----------------------------
      0         1-4094
     ----------------------------
```

The following table describes the labels in this screen.

Table 167 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.
TransmissionLimit	This field displays the maximum number of BPDUs that can be transmitted in the interval specified by **BridgeHelloTime**.

Table 167 show mstp (continued)

LABEL	DESCRIPTION
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 168 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.
TopoChange	This field indicates whether or not the current topology is stable. **0**: The current topology is stable. **1**: The current topology is changing.

Table 168 show mstp instance (continued)

LABEL	DESCRIPTION
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
```

CHAPTER 57
Multiple Login Commands

57.1 Command Summary

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

The following section lists the commands for this feature.

Table 169 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

57.2 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 170 show multi-login

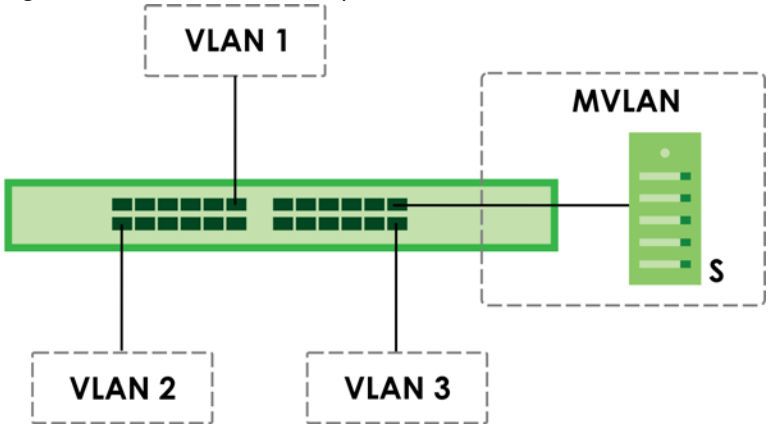
LABEL	DESCRIPTION
index	This field displays a sequential number for this entry. If there is an asterisk (*) next to the index number, this entry is your session.
session	This field displays the service the administrator used to log in.
remote ip	This field displays the IP address of the administrator's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

CHAPTER 58
MVR Commands

58.1 MVR Overview

Multicast VLAN Registration (MVR) is designed for applications (such as Media-on-Demand (MoD)) that use Multicast traffic across an Ethernet ring-based service provider network. MVR allows one single Multicast VLAN to be shared among different subscriber VLANs on the network. While isolated in different subscriber VLANs, connected devices can subscribe to and unsubscribe from the Multicast stream in the Multicast VLAN. This improves bandwidth utilization with reduced Multicast traffic in the subscriber VLANs and simplifies Multicast group management.MVR only responds to IGMP join and leave control messages from Multicast groups that are configured under MVR. Join and leave reports from other Multicast groups are managed by IGMP snooping.The following figure shows a network example. The subscriber VLAN (**1**, **2** and **3**) information is hidden from the streaming media server, **S**. In addition, the Multicast VLAN information is only visible to the Switch and **S**.

Figure 7 MVR Network Example



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

58.2 Command Summary

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

Table 171 Interface Command Values

COMMAND	DESCRIPTION
port-list	A list of one or more ports, separated by commas with no spaces. The list may also contain ranges of ports signified by a hyphen. For example: 1,3,5–8,10.

The following section lists the commands for this feature.

Table 172 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 ports.An MVR receiver port can only receive Multicast traffic in a Multicast VLAN.	C	13
no receiver-port <*port-list*>	Disables the receiver ports.An MVR receiver port can only receive Multicast traffic in a Multicast VLAN.	C	13
source-port <*port-list*>	Sets the source ports.An MVR source port can send and receive Multicast traffic in a Multicast VLAN.	C	13
no source-port <*port-list*>	Disables the source ports.An MVR source port can send and receive Multicast traffic in a Multicast VLAN.	C	13
tagged <*port-list*>	Sets the ports to tag VLAN tags.	C	13
no tagged <*port-list*>	Sets the ports 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

58.3 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
```

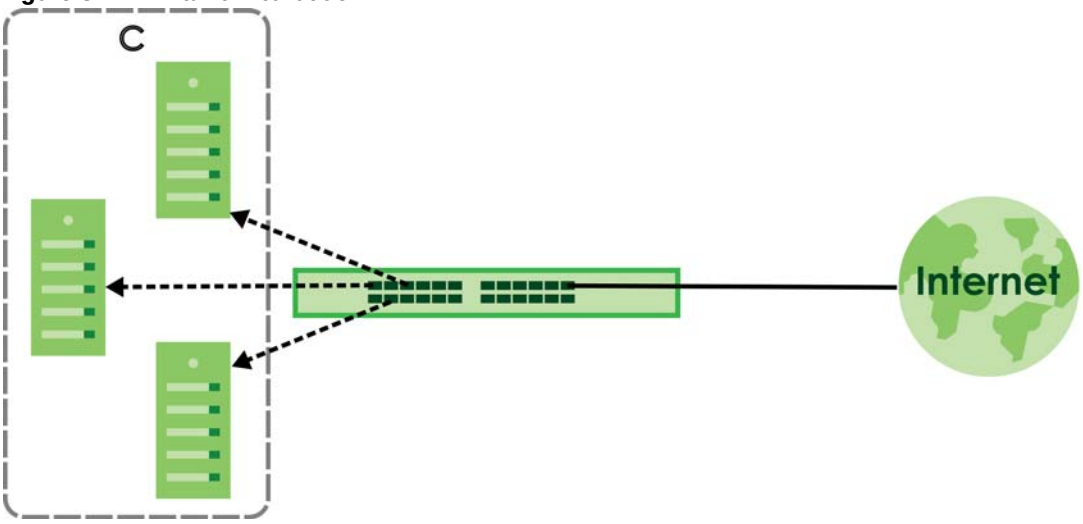
PART IV
Reference N-S

CHAPTER 59
NLB Commands

59.1 NLB Overview

The Switch supports NLB (Network Load Balancing) traffic distribution. The Switch will copy and forward the incoming traffic to a cluster (**C**). Each server in a cluster (**C**) tackles a separate copy of traffic.

Figure 8 NLB Traffic Distribution



The Switch only supports up to two clusters for NLB traffic distribution.

Note: NLB settings are configured on the servers.

NLB

Network Load Balancing (NLB) is a feature developed by Microsoft. NLB enhances the performance reliability for critical applications by sharing traffic with multiple servers in a cluster using TCP/IP protocol. Each server of a cluster tackles a copy of a traffic. You can create a cluster by grouping up to 32 servers together.

If a server in a cluster fails, traffic will be redistributed to the other operating servers. When the server is back in service, it will join the cluster automatically and share the traffic.

Unicast Mode

NLB replaces the real MAC addresses of the servers in a cluster with a unicast MAC address. Each server uses the same unicast MAC address, and a switch cannot map the unicast MAC address to a port. This forces a switch to flood traffic meant for the cluster to all ports of the switch to make sure the traffic is forwarded to the right destination.

The servers in a cluster cannot communicate with each other, because they use the same unicast MAC address.

Multicast Mode

NLB assigns a Multicast MAC address to the servers in a cluster. Therefore, each server has two MAC addresses, the real MAC address and the Multicast MAC address.

Create static ARP entries on a switch for the servers, so the switch will only forward traffic to the servers of the cluster.

The servers in a cluster can communicate with each other, because they keep their real MAC address and already have their own IP addresses.

59.2 Command Summary

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

Table 173 Interface Command Values

COMMAND	DESCRIPTION
port-list	A list of one or more ports, separated by commas with no spaces. The list may also contain ranges of ports signified by a hyphen. For example: 1,3,5–8,10.

The following section lists the commands for this feature.

Table 174 NLB Command Summary

COMMAND	DESCRIPTION	M	P
`nlb mac-forward name <name> mac <mac> vlan <vlan-id> interface port-channel <port-list>`	Configures to which MAC addresses and ports the Switch should forward the incoming NLB traffic. <*name*>: Enters a descriptive name for identification purposes for this rule. <*mac*>: Enters a Multicast or unicast MAC address of a cluster. The last binary bit of the first octet pair in a Multicast MAC address must be 1. For example, the first octet pair 00000001 is 01 and 00000011 is 03 in hexadecimal, so 01:00:5e:00:00:0A and 03:00:5e:00:00:27 are valid Multicast MAC addresses. The last binary bit of the first octet pair in a unicast MAC address must be 0. For example, the first octet pair 00000000 is 00 and 00000010 is 02 in hexadecimal, so 00:00:5e:00:00:0A and 02:00:5e:00:00:27 are valid unicast MAC addresses. <*vlan-id*>: Enters the VLAN identification number. If you don't have a specific target VLAN, enter 1. The Switch will forward traffic to ports in this VLAN group. <*port-list*>: Enters the ports to which you want the Switch to forward the incoming NLB traffic. You can enter multiple ports separated by (no space) comma (,) or hyphen (-). For example, enter "3-5" for ports 3, 4, and 5. Enter "3,5,7" for ports 3, 5, and 7.	C	13
`no nlb mac-forward mac <mac> vlan <vlan-id>`	Removes the specified MAC forwarding rule. <*mac*>: Enters a Multicast or unicast MAC address of a cluster. <*vlan-id*>: Enters the VLAN identification number.	C	13
`nlb arp name <name> ip <ip> mac <mac>`	Maps the IP address to the MAC address of a cluster for layer-3 forwarding. <*name*>: Enters a descriptive name for identification purposes for this rule. <*ip*>: Enters an IPv4 address for a cluster. <*mac*>: Enters a Multicast or unicast MAC address added via the `nlb mac-forward name <name> mac <mac> vlan <vlan-id> interface port-channel <port-list>` command. The last binary bit of the first octet pair in a Multicast MAC address must be 1. For example, the first octet pair 00000001 is 01 and 00000011 is 03 in hexadecimal, so 01:00:5e:00:00:0A and 03:00:5e:00:00:27 are valid Multicast MAC addresses. The last binary bit of the first octet pair in a unicast MAC address must be 0. For example, the first octet pair 00000000 is 00 and 00000010 is 02 in hexadecimal, so 00:00:5e:00:00:0A and 02:00:5e:00:00:27 are valid unicast MAC addresses.	C	13

Table 174 NLB Command Summary (continued)

COMMAND	DESCRIPTION	M	P
`no nlb arp ip <ip>`	Removes the specified IPv4-to-MAC mapping. <*ip*>: Enters an IPv4 address for a cluster.	C	13
`nlb ipv6 neighbor name <name> ip <ip> mac <mac>`	Maps the IP address to the MAC address of a cluster for layer-3 forwarding. <*name*>: Enters a descriptive name for identification purposes for this rule. <*ip*>: Enters an IPv6 address for a cluster. <*mac*>: Enters a Multicast or unicast MAC address added via the `nlb mac-forward name <name> mac <mac> vlan <vlan-id> interface port-channel <port-list>` command. The last binary bit of the first octet pair in a Multicast MAC address must be 1. For example, the first octet pair 00000001 is 01 and 00000011 is 03 in hexadecimal, so 01:00:5e:00:00:0A and 03:00:5e:00:00:27 are valid Multicast MAC addresses. The last binary bit of the first octet pair in a unicast MAC address must be 0. For example, the first octet pair 00000000 is 00 and 00000010 is 02 in hexadecimal, so 00:00:5e:00:00:0A and 02:00:5e:00:00:27 are valid unicast MAC addresses.	C	13
`no nlb ipv6 neighbor ip <ip>`	Removes the specified IPv6-to-MAC mapping. <*ip*>: Enters an IPv6 address for a cluster.	C	13

CHAPTER 60
ONVIF Commands

60.1 Overview

IP-based security products use a specific protocol for communication. One of the most common protocols is ONVIF (Open Network Video Interface Forum). ONVIF is a standard interface for interoperability of IP-based security products.

When ONVIF is enabled and configured, the Switch can obtain information from connected ONVIF compatible devices, such as a device's system name and IP address. This lets you know what types of ONVIF compatible devices, such as IP cameras and NVRs (network video recorders), are connected to the Switch.

60.2 Command Summary

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

Table 175 ONVIF Command Values

COMMAND	DESCRIPTION
port-list	A list of one or more ports, separated by commas with no spaces. The list may also contain ranges of ports signified by a hyphen. For example: 1,3,5–8,10.

The following section lists the commands for this feature.

Table 176 ONVIF Command Summary

COMMAND	DESCRIPTION	M	P
onvif	Enables the ONVIF feature on the Switch.	C	13
no onvif	Disables the ONVIF feature on the Switch.	C	13
onvif vlan <*vlanid*> interface port-channel <*port-list*>	Enables ONVIF on the specified VLAN and ports. The Switch snoops WS-Discovery messages on the specified VLAN and ports, in order to obtain informations about security devices.	C	13
no onvif vlan <*vlanid*>	Disables ONVIF on the specified VLAN.	C	13
show onvif info	Displays how many security devices are connected to each port on the Switch	E	3
show onvif info interface port-channel <*port-list*>	Displays detailed information about security devices connected to the specified port.	E	3
clear onvif info interface port-channel <*port-list*>	Clears information about security devices connected to the specified port.	C	13

60.3 Command Examples

This example enables ONVIF, and then configures the Switch to snoop for information about security devices which are using VLAN 1 and connected to ports 1 to 3.

```
sysname# config
sysname(config)# onvif
sysname(config)# onvif vlan 1 interface port-channel 1-3
```

This example disables ONVIF, and removes the ONVIF configuration for VLAN 1.

```
sysname# config
sysname(config)# no onvif
sysname(config)# no onvif vlan 1
```

This example shows how many security devices have been detected on each port of the Switch.

```
sysname# show onvif info
Port     Discovered Devices
------   --------------------------
    1                            2
    2                            0
    3                            1
    4                            0
   ...
   28                            0
```

This example shows detailed information about the security devices detected on ports 1 to 3.

```
sysname# show onvif info interface port-channel 1-3
Port 1
  Discovered Devices         :2

  Device Name                :Bosch
  Device Type                :IP Camera
  Model                      :DINION_IP_5000_HD
  IP Address                 :192.168.1.10
  Location                   :country china, city beijing, building
                             headquarter, building headquarter, floor R5

  Device Name                :
  Device Type                :NVR
  Model                      :
  IP Address                 :192.168.1.20
  Location                   :

Port 2
  Discovered Devices         :0

Port 3
  Discovered Devices         :1

  Device Name                :WBox
  Device Type                :IP Camera
  Model                      :0E-13BF36
  IP Address                 :00:07:5f:9f:11:22
  Location                   :city Hsinchu
```

CHAPTER 61
OSPF Commands

61.1 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.

The Switch uses OSPFv2 for IPv4, and also supports OSPFv3 to work with IPv6. OSPFv2 and OSPFv3 are quite similar. The OSPF mechanisms and algorithms are not changed but there are two new Link State Advertisements (LSA) types in OSPFv3. OSPFv2 uses plain text or MD5 authentication, while no authentication is required for OSPFv3 on the Switch. Their packet format is different, too.

Note: You must purchase the Advance Routing service license and go to myZyxel to activate it for your Switch in order to use advanced L3 routing features, such as RIPng and OSPFv3 for IPv6. See Section 79.1 on page 316 for more information.

61.1.1 OSPF Autonomous Systems and Areas

An OSPF autonomous system (AS) can be divided into logical areas. Each area represents a group of adjacent networks. All areas are connected to a backbone (also known as area 0). The backbone is the transit area to route packets between two areas. A stub area, at the edge of an AS is not a transit area since there is only one connection to the stub area.

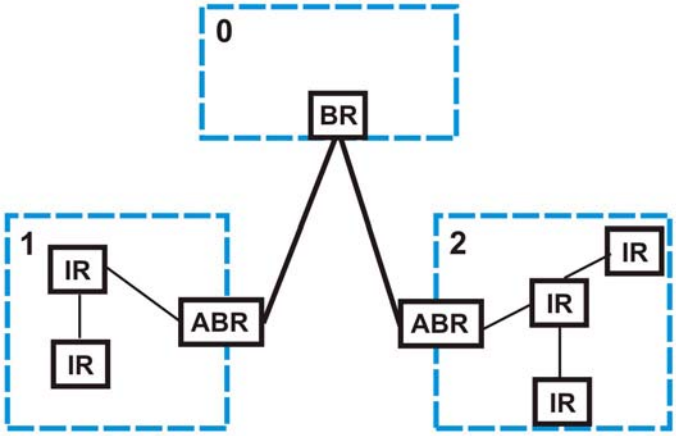
The following table describes the four classes of OSPF routers.

Table 177 OSPF: Router Types

TYPE	DESCRIPTION
Internal Router (IR)	An Internal or intra-area router is a router in an area.
Area Border Router (ABR)	An Area Border Router connects two or more areas.
Backbone Router (BR)	A backbone router has an interface to the backbone.
AS Boundary Router	An AS boundary router exchanges routing information with routers in other ASs.

The following figure depicts an OSPF network example. The backbone is area 0 with a backbone router. The internal routers are in area 1 and 2. The area border routers connect area 1 and 2 to the backbone.

Figure 9 OSPF Network Example



61.2 Command Summary

The following section lists the commands for this feature.

Table 178 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 ipv6 ospf database	Displays IPv6 OSPF link state database information.	E	3
show ipv6 ospf interface	Displays IPv6 OSPF interface settings.	E	3
show ipv6 ospf neighbor	Displays IPv6 OSPF neighbor information.	E	3
show ipv6 ospf redistribute	Displays IPv6 OSPF redistribution settings.	E	3
show ipv6 ospf route	Displays IPv6 OSPF route entries.	E	3
show ip protocols	Displays the routing protocol the Switch is using and its administrative distance value.	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

Table 178 OSPF Command Summary (continued)

COMMAND	DESCRIPTION	M	P
ip ospf authentication-same-aa	Sets the same OSPF authentication settings in the routing domain as the associated area.	C	13
ip ospf authentication-same-as-area	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
no ip ospf authentication-same-as-area	Sets the routing domain not to use the same OSPF authentication settings as the area.	C	13
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 retransmit-interval <1-65535>	Sets the OSPF retransmission interval in this routing domain.	C	13
ip ospf transmit-delay <1-65535>	Sets the OSPF transmission delay in this routing domain.	C	13
ip ospf dead-interval <1-65535>	Sets the OSPF dead interval in this routing domain.	C	13
ip ospf hello-interval <1-65535>	Sets the OSPF hello interval in this routing domain.	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 network-type <broadcast|point-to-point>	Sets the OSPF network type in this routing domain. You should set the network type according to your network topology in this routing domain. If you set the network type to broadcast, the Switch will elect a DR/BDR for this routing domain. If you set the network type to point-to-point, the Switch will not elect a DR/BDR for the routing domain. Note that the OSPF interface might not be able to correctly exchange routing information if you set the wrong network type. Note: A loopback interface has its own network type other than broadcast or point-to-point network. You are not allowed to set the network type for the OSPF interface if it is a loopback interface.	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
interface vlan <*vlan-id*>	Enters the configuration mode for this VLAN interface.	C	13

Table 178 OSPF Command Summary (continued)

COMMAND	DESCRIPTION	M	P
ipv6 ospf cost <1-65535>	Sets the IPv6 OSPF cost in this VLAN interface.	C	13
ipv6 ospf dead-interval <1-65535>	Sets the IPv6 OSPF dead interval in this VLAN interface.	C	13
ipv6 ospf hello-interval <1-65535>	Sets the IPv6 OSPF hello interval in this VLAN interface.	C	13
ipv6 ospf instance-id <0-255>	OSPFv3 can support multiple instances per link. Sets the IPv6 OSPF Instance ID to which the VLAN is assigned. The interface will drop the packets that contain a different instance ID number.	C	13
ipv6 ospf passive-interface	Sets the VLAN interface to be passive. A passive interface does not send or receive IPv6 OSPF traffic.	C	13
no ipv6 ospf passive-interface	Sets the VLAN interface to not be passive.	C	13
ipv6 ospf priority <0-255>	Sets the IPv6 OSPF priority for the VLAN interface. Setting this value to 0 means that this router will not participate in router elections.	C	13
ipv6 ospf retransmit-interval <1-65535>	Sets the IPv6 OSPF retransmission interval in this VLAN interface.	C	13
ipv6 ospf transmit-delay <1-65535>	Sets the IPv6 OSPF transmission delay in this IPv6 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 <0-16777215>	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 stub area to send LSAs (Link State Advertisements).	C	13
area <*area-id*> nssa	Enables and sets the area as a not-so-stubby area.	C	13
no area <*area-id*> nssa	Disables not-so-stubby network settings in the area.	C	13

Table 178 OSPF Command Summary (continued)

COMMAND	DESCRIPTION	M	P
area <*area-id*> nssa no-summary	Sets the not-so-stubby area not to send any LSA (Link State Advertisement).	C	13
no area <*area-id*> nssa no-summary	Sets the not-so-stubby 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
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
area <*area-id*> virtual-link <*router-id*> retransmit-interval <1-65535>	Sets the retransmission interval for the virtual link in the area.	C	13
area <*area-id*> virtual-link <*router-id*> transmit-delay <1-65535>	Sets the transmission delay for the virtual link in the area.	C	13
area <*area-id*> virtual-link <*router-id*> dead-interval <1-65535>	Sets the dead interval for the virtual link in the area.	C	13
area <*area-id*> virtual-link <*router-id*> hello-interval <1-65535>	Sets the hello interval for the virtual link in the area.	C	13

Table 178 OSPF Command Summary (continued)

COMMAND	DESCRIPTION	M	P
distance <10-255>	When two different routing protocols, such as RIP and OSPF provide multiple routes to the same destination, the Switch can use the administrative distance of the route source to determine which routing protocol to use and add the route to the routing table. Sets the administrative distance (from 10 to 255) that is assigned to the routes learned by OSPF. The lower the administrative distance value is, the more preferable the routing protocol is. If two routes have the same administrative distance value, the Switch uses the route that has the lowest metric value. Note: You cannot set two routing protocols to have the same administrative distance.	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 <0-16777215>	Sets the Switch to learn RIP routing information which will use the specified metric information. metric-type: sets RIP routes to use metric type1 or type 2. Type 1 is for routing protocols (such as RIP) whose external metrics are directly comparable to the internal OSPF cost. When selecting a path, the internal OSPF cost is added to the ABR (Area Border Router) to the external metrics. Type 2 is for routing protocols whose external metrics are not comparable to the OSPF cost. In this case, only the external cost (metric) of the ABR is used in path decision to a destination. metric: sets the external metric of RIP routes.	C	13
redistribute rip	Sets the Switch to redistribute RIP routing information. Route redistribution allows your Switch to import and translate external routes learned through other routing protocols (RIP/Static/Connected) into the OSPF network transparently.	C	13
no redistribute rip	Sets the Switch not to learn RIP routing information.	C	13

Table 178 OSPF Command Summary (continued)

COMMAND	DESCRIPTION	M	P
`redistribute static metric-type <1|2> metric <0-16777215>`	Sets the Switch to learn static routing information which will use the specified metric information. `metric-type`: sets static routes to use metric type1 or type 2. Type 1 is for routing protocols (such as RIP) whose external metrics are directly comparable to the internal OSPF cost. When selecting a path, the internal OSPF cost is added to the ABR (Area Border Router) to the external metrics. Type 2 is for routing protocols whose external metrics are not comparable to the OSPF cost. In this case, only the external cost (metric) of the ABR is used in path decision to a destination. `metric`: sets the external metric of static routes.	C	13
`redistribute static`	Sets the switch to redistribute static routing information. Route redistribution allows your Switch to import and translate external routes learned through other routing protocols (RIP/Static/Connected) into the OSPF network transparently.	C	13
`no redistribute static`	Sets the Switch not to learn static routing information.	C	13
`redistribute connected metric-type <1|2> metric <0-16777215>`	Sets the Switch to learn connected routes information which will use the specified metric information. `metric-type`: sets connected routes to use metric type1 or type 2. Type 1 is for routing protocols (such as RIP) whose external metrics are directly comparable to the internal OSPF cost. When selecting a path, the internal OSPF cost is added to the ABR (Area Border Router) to the external metrics. Type 2 is for routing protocols whose external metrics are not comparable to the OSPF cost. In this case, only the external cost (metric) of the ABR is used in path decision to a destination. `metric`: sets the external metric of connected routes.	C	13

Table 178 OSPF Command Summary (continued)

COMMAND	DESCRIPTION	M	P
redistribute connected	Sets the switch to redistribute connected routes information. Connected routes are routes to the networks that are directly connected to the Switch interfaces. These interfaces must have an IP address, such as a loopback interface, DHCP interface, or VLAN interface. Route redistribution allows your Switch to import and translate external routes learned through other routing protocols (RIP/Static/Connected) into the OSPF network transparently.	C	13
no redistribute connected	Sets the Switch not to learn connected 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 passive-iface <*ip-addr/bits*>	Sets the interface to not be passive.	C	13
summary-address <*ip-address*> <*mask*>	Sets a summary address which is a network IP address used to cover more than one network routing entry in order to reduce the routing table size.	C	13
no summary-address <*ip-address*> <*mask*>	Removes a summary address.	C	13
show router ospf summary-address	Displays all summary addresses on the Switch.	E	3
ipv6 router ospf <*router-id*>	Enables and enters the IPv6 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*> default-cost <0-16777215>	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*> nssa	Enables and sets the area as a not-so-stubby area.	C	13
no area <*area-id*> nssa	Disables not-so-stubby network settings in the area.	C	13
area <*area-id*> nssa no-summary	Sets the not-so-stubby area not to send any LSA (Link State Advertisement).	C	13
no area <*area-id*> nssa no-summary	Sets the not-so-stubby area to send LSAs (Link State Advertisements).	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 stub 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

Table 178 OSPF Command Summary (continued)

COMMAND	DESCRIPTION	M	P
no area <*area-id*> virtual-link <*router-id*>	Deletes the virtual link from the area.	C	13
area <*area-id*> virtual-link <*router-id*> dead-interval <1-65535>	Sets the dead interval for the virtual link in the area.	C	13
area <*area-id*> virtual-link <*router-id*> hello-interval <1-65535>	Sets the hello interval for the virtual link in the area.	C	13
area <*area-id*> virtual-link <*router-id*> retransmit-interval <1-65535>	Sets the retransmission interval for the virtual link in the area.	C	13
area <*area-id*> virtual-link <*router-id*> transmit-delay <1-65535>	Sets the transmission delay for the virtual link in the area.	C	13
distance <10-255>	When two different routing protocols, such as RIP and OSPF provide multiple routes to the same destination, the Switch can use the administrative distance of the route source to determine which routing protocol to use and add the route to the routing table. Sets the administrative distance (from 10 to 255) that is assigned to the routes learned by OSPF. The lower the administrative distance value is, the more preferable the routing protocol is. If two routes have the same administrative distance value, the Switch uses the route that has the lowest metric value. Note: You cannot set two routing protocols to have the same administrative distance.	C	13
interface <*interface-type*> <*interface-number*> area <*area-id*>	Sets the area ID of an area to associate a specific VLAN interface with that area.	C	13
no interface <*interface-type*> <*interface-number*>	Removes the specified IPv6 VLAN interface.	C	13
redistribute rip	Sets the Switch to redistribute RIP routing information. Route redistribution allows your Switch to import and translate external routes learned through other routing protocols (RIP and Static) into the OSPF network transparently.	C	13
no redistribute rip	Sets the Switch not to learn RIP routing information.	C	13
redistribute rip metric-type <1|2> metric <0-16777215>	Sets the Switch to learn RIP routing information which will use the specified metric information.	C	13
redistribute static	Sets the switch to redistribute static routing information. Route redistribution allows your Switch to import and translate external routes learned through other routing protocols (RIP and Static) into the OSPF network transparently.	C	13

Table 178 OSPF Command Summary (continued)

COMMAND	DESCRIPTION	M	P
no redistribute static	Sets the Switch not to learn static routing information.	C	13
redistribute static metric-type <1|2> metric <0-16777215>	Sets the Switch to learn static routing information which will use the specified metric information.	C	13
no router ospf	Disables OSPF on the Switch.	C	13
no ipv6 router ospf	Disables OSPFv3 for IPv6 on the Switch.	C	13

61.3 Command Examples

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.

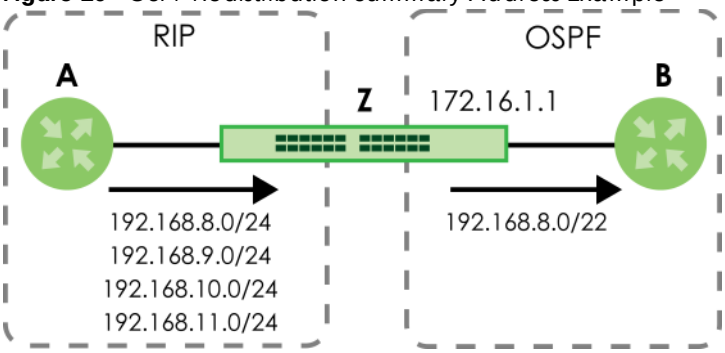
```
sysname(config)# router ospf 172.16.1.1
sysname(config-ospf)# area 0.0.0.0
sysname(config-ospf)# area 0.0.0.0 authentication
sysname(config-ospf)# area 0.0.0.0 name backbone
sysname(config-ospf)# network 172.16.1.1/24 area 0.0.0.0
sysname# show router ospf area
  index:1       active:Y        name:backbone
  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 network type of this interface is set to **broadcast**; 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 network-type broadcast
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
```

In this example, the Switch (**Z**) is a redistributor between a RIP network and an OSPF network. It summarizes 4 routing entries 192.168.8.0/24 – 192.168.11.0/24 (learned from RIP router **A**) into 192.168.8.0/22 and then sends it to OSPF router **B**.

Figure 10 OSPF Redistribution Summary Address Example



This example shows you how to enable the redistribution for RIP protocol and then show all redistribution entries.

```
sysname# config
sysname(config)# router ospf 172.16.1.1
sysname(config-ospf)# redistribute rip metric-type 1 metric 123
sysname(config-ospf)# exit
sysname(config)# exit
sysname# show ip ospf database

       OSPF Router with ID (172.16.1.1)

(Omit not external part °K)

                AS External Link States

Link ID         ADV Router      Age  Seq#       CkSum  Route
192.168.8.0     192.168.2.2      618 0x80000001 0x02f6 E1 192.168.8.0/24
192.168.9.0     192.168.2.2      618 0x80000001 0xf601 E1 192.168.9.0/24
192.168.10.0    192.168.2.2     618 0x80000001 0xeb0b E1 192.168.10.0/24
192.168.11.0    192.168.2.2     618 0x80000001 0xe015 E1 192.168.11.0/24
```

From the example above, the third octet of all the four network IP addresses is 00001000, 00001001, 00001010, 000001011 respectively. The first 4 digits (000010) are the common part among these IP addresses. So 192.168.8.0/22 can be used to represent all of the four networks. The following example shows you how to configure the OSPF summary address and then show all redistribution entries.

```
sysname# config
sysname(config)# router ospf 172.16.1.1
sysname(config-ospf)# summary-address 192.168.8.0 255.255.252.0
sysname(config-ospf)# exit
sysname(config)# exit
sysname# show ip ospf database

OSPF Router with ID (172.16.1.1)

(Omit not external part °K)

                AS External Link States

Link ID         ADV Router      Age  Seq#       CkSum  Route
192.168.8.0     192.168.2.2        6 0x80000001 0xf209 E1 192.168.8.0/22
```

CHAPTER 62
Password Commands

62.1 Password Commands Overview

Password Encryption

Password encryption provides service providers a means to securely enter administrator and login passwords. By default, passwords are sent in plain text. Plain text passwords are also stored temporarily in the Switch's spt and temp buffers. By enabling password encryption, you can hide these plain text passwords in transit as well as in the device buffers.

62.2 Command Summary

The following section lists the commands for this feature.

Table 179 password Command Summary

COMMAND	DESCRIPTION	M	P
admin-password <*pw-string*> <*confirm-string*>	Changes the administrator password. *pw-string*: When Password Complexity is disabled or for Switch models without Password Complexity: • 4 to 32 characters in length When Password Complexity is enabled on supported Switch models: • 9 to 32 characters in length • Include at least three of these: numbers, uppercase letters, lowercase letters, and special characters (for example, 'Ea5yPas5W0rd') • Cannot match your login username • Cannot use the same character (case insensitive) or number three or more times in a row (for example, '777', 'AaA') • Cannot use four or more sequential keyboard characters (case insensitive) or numbers (for example, 'qWer', '1234'), and • Cannot use the present password again. Note: Not all Switch models support password complexity. Note: [?], [|], ['], ["], [,], [[ ], [ ]] and space are not allowed whether Password Complexity is enabled or disabled. *confirm-string*: Enter the pw-string again.	C	14

Table 179 password Command Summary (continued)

COMMAND	DESCRIPTION	M	P
admin-password [[cipher] <*pw-string*>]	Changes the administrator password. If you only enter the 'admin-password', you will enter the interactive password input mode. At this time, the password you enter will not display on the screen. cipher: inform the Switch that the string after the word "cipher" is an encrypted secret. This is used in password encryption. To encrypt the password, use the password encryption command. *pw-string*: (for Switch models that do not support Password Complexity) 1 – 32 alphanumeric characters except [?], [|], ['], ["], [space], or [,]. *pw-string*: (for Switch models that support Password Complexity) When Password Complexity is disabled: • 4 to 32 characters in length When Password Complexity is enabled: • 9 to 32 characters in length • Include at least three of these: numbers, uppercase letters, lowercase letters, and special characters (for example, 'Ea5yPas5W0rd') • Cannot match your login username • Cannot use the same character (case insensitive) or number three or more times in a row (for example, '777', 'AaA') • Cannot use four or more sequential keyboard characters (case insensitive) or numbers (for example, 'qWer', '1234'), and • Cannot use the present password again. Note: Not all Switch models support password complexity. Note: [?], [|], ['], ["], [,], [[ ], [ ]] and space are not allowed whether Password Complexity is enabled or disabled.	C	14

Table 179 password Command Summary (continued)

COMMAND	DESCRIPTION	M	P
password [cipher] <*pw-string*> [privilege <*0-14*>]	Changes the password for the highest privilege level or, optionally, the specified privilege. cipher: inform the Switch that the string after the word "cipher" is an encrypted secret. This is used in password encryption. To encrypt the password, use the password encryption command. *pw-string*: (for Switch models that do not support Password Complexity) 1 – 32 alphanumeric characters except [?], [|], ['], ["], [space], or [,]. *pw-string*: (for Switch models that support Password Complexity) When Password Complexity is disabled: • 4 to 32 characters in length When Password Complexity is enabled: • 9 to 32 characters in length • Include at least three of these: numbers, uppercase letters, lowercase letters, and special characters (for example, 'Ea5yPas5W0rd') • Cannot match your login username • Cannot use the same character (case insensitive) or number three or more times in a row (for example, '777', 'AaA') • Cannot use four or more sequential keyboard characters (case insensitive) or numbers (for example, 'qWer', '1234'), and • Cannot use the present password again. Note: Not all Switch models support password complexity. Note: [?], [|], ['], ["], [,], [[ ], [ ]] and space are not allowed whether Password Complexity is enabled or disabled.	C	14
password privilege <*0-14*> password	password: inform the Switch to hide the password characters you entered (interactive mode).	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
password encryption	Encrypts all passwords configured on the Switch. The encrypted secret will be preceded by the word "cipher" in the configuration file (called running-config)."	C	14
no password encryption	Disables password encryption. The encrypted password will not be changed back to plain text. Note: Be careful who can access configuration files with plain text passwords!	C	14

Table 179 password Command Summary (continued)

COMMAND	DESCRIPTION	M	P
password complexity	Enforce using a strong login/enable/SNMP user password on the Switch. The rules for a strong login/enable/SNMP user password are: • 9 to 32 characters in length • [?], [|], ['], ["], [,], [[ ], [ ]] and space are not allowed • Include at least three of these: numbers, uppercase letters, lowercase letters, and special characters (for example, 'Ea5yPas5W0rd') • Cannot match your login/SNMP user username • Cannot use the same character (case-insensitive) or number three or more times in a row (for example, '777', 'AaA') • Cannot use four or more sequential keyboard characters (case-insensitive) or numbers (for example, 'qWer', '1234'), and • Cannot use the present password again.	C	14
no password complexity	Disables enforcing the use of a strong login/enable/SNMP user password on the Switch. The rules for a simple login/enable/SNMP user password are: • 4 to 32 characters in length, and • [?], [|], ['], ["], [,], [[ ], [ ]] and space are not allowed.	C	14

Note: For examples of these commands, see Section 3.2.3.2 on page 20.

CHAPTER 63
PoE Commands

63.1 Command Summary

Use these commands to configure Power over Ethernet (PoE).

Note: These are applicable for PoE models only.

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

Table 180 Interface Command Values

COMMAND	DESCRIPTION
port-list	A list of one or more ports, separated by commas with no spaces. The list may also contain ranges of ports signified by a hyphen. For example: 1,3,5–8,10.

The following section lists the commands for this feature.

Table 181 pwr Command Summary

COMMAND	DESCRIPTION	M	P
`interface port-channel <port-list>`	Enters config-interface mode for the specified ports.	C	13
`extend-range`	Sets the ports to extend the PoE range up to 250 meters. After you enable this feature, the port will transfer data at a rate up to10 Mbps in full duplex mode. If a PD is connected to the port, the Switch follows the IEEE 802.3at PoE+ standard to supply power to the connected PD during power-up. Note: Maximum PoE power that can be supplied to a PD at 250 m is 15 W. Note: If you enable extended range on a port after the connected PD starts up completely, you must disable PoE and enable it again or disconnect and reconnect the cable to the port for extended mode to take effect. Note: The port speed and duplex mode you previously configured will be applied automatically when the extend range feature is disabled.	C	13
`no extend-range`	Sets the ports to not extend the PoE range.	C	13
`pwr auto-pd-recovery`	Turns on auto PD recovery on the Switch.	C	13

Table 181 pwr Command Summary (continued)

COMMAND	DESCRIPTION	M	P
no pwr auto-pd-recovery	Turns off auto PD recovery on the Switch.	C	13
pwr continuous-poe	Enables this function to guarantee continuous power supply to the connected PDs when you restart the Switch (warm reboot) without physically turning the power off. The Switch will NOT perform a power cycle on the connected PDs. If you do a cold reboot, the Switch also restarts the connected PDs.	C	13
no pwr continuous-poe	Disables continuous PoE on the Switch.	C	13
pwr interface *<port-list>*	Enables PoE (Power over Ethernet) on the specified ports.	C	13
no pwr interface *<port-list>*	Disables PoE (Power over Ethernet) on the specified ports.	C	13
pwr interface *<port-list>* auto-pd-recovery	Turns on auto PD recovery on the specified ports.	C	13
no pwr interface *<port-list>* auto-pd-recovery	Turns off auto PD recovery on the specified ports.	C	13
pwr interface *<port-list>* auto-pd-recovery action <reboot-alarm|alarm>	Set the action to take when the connected PD has stopped responding. reboot-alarm: to have the Switch turn OFF the power of the connected PD and turn it back ON again to restart the PD after sending an SNMP trap and generating a log message. alarm: to have the Switch send an SNMP trap and generate a log message.	C	13
pwr interface *<port-list>* auto-pd-recovery mode <lldp|onvif|ping *<ip>* [polling-interval <10-300>] [polling-count <2-5>]>	Sets whether the Switch uses LLDP, ONVIF or ping to check current status of a connected PD. lldp: to have the Switch passively monitor current status of the connected PD by reading LLDP packets from the PD on the specified ports. onvif: to have the Switch send ONVIF packets to scan the current status of the connected ONVIF-compatible PD. Note: Make sure to enable the ONVIF feature on the Switch. See ONVIF Commands for more information. ping: to have the Switch ping the IP address of the connected PD to test whether the PD is reachable or not.	C	13
pwr interface *<port-list>* auto-pd-recovery pd-reboot-count <1-5>	Sets how many times the Switch attempts to restart the PD on the specified ports.	C	13
pwr interface *<port-list>* auto-pd-recovery resume-polling-interval <60-800>	Sets the number of seconds the Switch waits before monitoring the PD status again after it restarts the PD on the specified ports.	C	13
pwr interface *<port-list>* auto-pd-recovery resume-power-interval <5-120>	Sets the number of seconds the Switch waits before supplying power to the connected PD again after it restarts the PD on the specified ports.	C	13

Table 181 pwr Command Summary (continued)

COMMAND	DESCRIPTION	M	P
pwr interface <*port-list*> max-power <1000-33000>	Sets the maximum amount of power the PD could use from the Switch on the specified ports. Note: The user-configured maximum power setting will not take effect when the power-up mode is set to 802.3bt.	C	13
no pwr interface <*port-list*> max-power	Removes the maximum power settings for the specified ports. The PDs that is connected to the ports then can use power up to the Switch's total power budget.	C	13
pwr interface <*port-list*> power-up <802.3af|legacy|pre-802.3at|802.3at|802.3bt|force-802.3at>	Sets how the Switch provides power to a connected PD at power-up. 802.3af: the Switch follows the IEEE 802.3af Power over Ethernet standard to supply power to the connected PDs during power-up. legacy: the Switch can provide power to the connected PDs that require high inrush currents at power-up. Inrush current is the maximum, instantaneous input current drawn by the PD when first turned on. pre-802.3at: the Switch initially offers power on the port according to the IEEE 802.3af standard, and then switches to support the IEEE 802.3at standard within 75 milliseconds after a PD is connected to the port. Select this option if the Switch is performing 2-event Layer-1 classification (PoE+ hardware classification) or the connected PD is NOT performing Layer 2 power classification using Link Layer Discovery Protocol (LLDP). 802.3at: the Switch supports the IEEE 802.3at High Power over Ethernet standard and can supply power of up to 30W per Ethernet port. IEEE 802.3at is also known as PoE+ or PoE Plus. An IEEE 802.3at compatible device is referred to as Type 2. Power Class 4 (High Power) can only be used by Type 2 devices. If the connected PD requires a Class 4 current when it is turned on, it will be powered up in this mode. force-802.3at: the Switch offers power of up to 33W on the port without performing PoE hardware classification. Select this option if the connected PD does not comply with any PoE standard and requests power higher than a standard power limit. 802.3bt: the Switch supports the IEEE 802.3bt standard and can supply power of up to 60W per Ethernet port to the connected PDs at power-up.	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

Table 181 pwr Command Summary (continued)

COMMAND	DESCRIPTION	M	P
pwr interface <*port-list*> time-range <*name*>	Specifies a pre-defined schedule to control when the Switch enables PoE to provide power on the specified ports.	C	13
no pwr interface <*port-list*> time-range	Removes all the applied schedules from the specified ports.	C	13
no pwr interface <*port-list*> time-range <*name*>	Removes a specific schedule from the specified ports.	C	13
pwr interface <*port-list*> wide-range	Enables this function to let the Switch have a wider detection range for the PDs on the specified ports. The Switch detects whether a connected device is a powered device or not before supplying power to the port. For the PD detection, the Switch applies a fixed voltage to the device and then receives returned current. If the returned current is within the IEEE 802.3af/at standard range, the device will be considered as a valid PD by the Switch. However, in real cases, environmental interferences might easily cause the returned current to be out of the standard range.	C	13
no pwr interface <*port-list*> wide-range	Disables wide range detection on the specified ports.	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 mode <classification|consumption>	Sets the power management mode. • Classification – Reserve the maximum power to each PD according to the PD's power class and priority level. • Consumption – Supply the actual power that the PD needs. The Switch also allocates power based on a port's maximum power and the PD's power class and priority level.	C	13
pwr usagethreshold <1-99>	Sets the percentage of power usage which initiates MIB traps.	C	13
show pwr	Displays information about port power consumption and Power over Ethernet (PoE). Only available on models with the PoE feature.	E	3
show pwr time-range	Displays the name of the applied schedule and whether or not the ports currently receives power from the Switch according to its schedule. • It shows "In" if PoE is currently enabled on the port. • It shows "Out" if PoE is currently disabled on the port. • It shows "–" if no schedule is applied to the port. PoE is enabled by default.	E	3
show pwr time-range interface <*port-list*>	Displays the name of the schedule applied to the specified ports and the current PoE state.	E	3

63.2 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 sets the maximum amount of power allowed for port 2 to 7500 mW.

```
sysname# configure
sysname(config)# pwr interface 2 max-power 7500
sysname(config)# exit
```

This example creates a schedule (named **Work**), applies the pre-defined schedule to port 1 and displays the port's current PoE state.

```
sysname# configure
sysname(config)# time-range Work periodic weekdays 08:00 to 20:00
sysname(config)# pwr interface 1 time-range Work
sysname(config)# exit
sysname# show pwr time-range interface
sysname# show pwr time-range interface 1
  Port  TimeRange  State
  ----  ---------  -----
     1       Work    Out
sysname# exit
```

This example enables auto PD discovery on the Switch and ports 1 to 3.

```
sysname# configure
sysname(config)# pwr auto-pd-recovery
sysname(config)# pwr interface 1-3 auto-pd-recovery
sysname# exit
```

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

```
sysname# sh pwr

  PoE Mode : Classification mode
  Continuous PoE : enable
  Total Power:60.0(W)
  Usage:10(%)
  Consuming Power:6.9(W)
  Allocated Power:30.0 (W)
  Remaining Power:30.0(W)

  Averaged Junction Temperature: 42 (c), 107 (f).

  Port   State   PD  Class  Priority  Power-Up  Wide Range  Consumption (mW)  Ma
xPower(mW)
  ----  ------  ---  -----  --------  --------  ----------  ----------------  --
----------
     1  Enable   On      4       Low   802.3bt      Enable              6900
     30000
     2  Enable  Off      0       Low   802.3bt      Enable                 0
         0
     3  Enable  Off      0       Low   802.3at      Enable                 0
         0
     4  Enable  Off      0       Low   802.3at      Enable                 0
         0
     5  Enable  Off      0       Low   802.3at      Enable                 0
         0
```

The following table describes the labels in this screen.

Table 182 show pwr

LABEL	DESCRIPTION
PoE Mode	This field displays the power management mode used by the Switch, whether it is in **Classification** or **Consumption** mode.
Continuous PoE	This field displays whether continuous PoE is enabled on the Switch.
Total Power	This field displays the total power the Switch can provide to PoE-enabled devices.
Usage	This field displays the percentage of PoE Power consumption.
Consuming Power	This field displays the amount of power the Switch is currently supplying to the PoE-enabled devices.
Allocated Power	This field displays the total amount of power the Switch has reserved for PoE after negotiating with the PoE devices. Note: If the management mode is set to **Consumption**, this field shows **NA**.
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.
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.

Table 182 show pwr (continued)

LABEL	DESCRIPTION
Class	This field displays the power classification of the PD. Each PD has a specified maximum power that fall under one of the classes. The Class is a number from 0 to 6, where each value represents the range of power that the Switch provides to the PD. The power ranges in PoE standards are as follows. • Class **0** – default: 0.44 W to 15.4 W. • Class **1** – default: 0.44 W to 4 W. • Class **2** – default: 0.44 W to 7 W. • Class **3** – default: 0.44 W to 15.4 W. • Class **4** – default: 0.44 W to 30 W. • Class **5** – default: 0.44 W to 45 W. • Class **6** – default: 0.44 W to 60 W. Note: You can extend or set a limit on the maximum power the connected PD can use on a port using the `pwr interface <port-list> max-power <1000-33000>` command. The user-configured maximum power setting will not take effect when the power-up mode is set to **802.3bt**. When the power-up mode is NOT **802.3bt** and the Switch is in consumption mode, the default maximum power that can be delivered to the PD is 33 W (IEEE 802.3at Class 4) or 22 W (IEEE 802.3af Classes 0 to 3).
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.
Power-Up	This field displays the PoE standard the Switch uses to provide power on this port.
Wide Range	This field displays whether wide range detection is enabled on the Switch.
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.

CHAPTER 64
Policy Commands

64.1 Policy Commands Overview

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.

Note: Configure classifiers before you configure policies. See Chapter 15 on page 58 for more information on classifiers.

64.2 Command Summary

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

Table 183 Interface Command Values

COMMAND	DESCRIPTION
port-list	A list of one or more ports, separated by commas with no spaces. The list may also contain ranges of ports signified by a hyphen. For example: 1,3,5–8,10.

The following section lists the commands for this feature.

Table 184 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 184 policy Command Summary (continued)

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*>][egress-port <*port-list*>][outgoing-packet-format <tagged|untagged>][out-of-profile-dscp <0-63>][forward-action <drop|forward|egressmask>] [priority-action <[prio-set|set-prio-as-inner-prio |prio-replace-tos] [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 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: • priority-action: tells the Switch to: – replace the packet's IEEE 802.1p priority field with the priority you specified in the priority parameter (prio-set) – replace the packet's IEEE 802.1p priority field with the existing customer priority level carried in the frames (set-prio-as-inner-prio) – replace the IEEE 802.1p priority field with the tos parameter value (prio-replace-tos). • queue-action: tells the Switch to: – set the IEEE 802.1p priority you specified in the priority parameter (prio-set) – sends the packet to priority queue (prio-queue) – replace the IEEE 802.1p priority field with the tos parameter value (prio-replace-tos). • diffserv-action – chooses whether you want to set the ToS field with the value you specified for the tos parameter (diff-set-tos), replaces the IP ToS with IEEE 802.1p priority value (diff-replace-priority) or sets the DSCP field with the dscp parameter value (diff-set-dscp) • outgoing-mirror – sends the packet to the mirror port. • outgoing-eport – sends the packet to the egress port. • outgoing-non-unicast-eport – sends 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). – discards 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.	C	13

Table 184 policy Command Summary (continued)

COMMAND	DESCRIPTION	M	P
policy <*name*> classifier <*classifier-list*> <[vlan <*vlan-id*>] [egress-port <*port-num*>] [priority <0-7>] [bandwidth <*bandwidth*>] [forward-action <drop>] [queue-action <prio-set>] [outgoing-eport] [outgoing-set-vlan] [rate-limit] [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: vlan: a VLAN ID number egress-port: an outbound port number priority: IEEE 802.1p priority field bandwidth: bandwidth limit in Kbps, packets which exceed the bandwidth limit are dropped.		
	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) • outgoing-eport – sends the packet to the egress port. • outgoing-set-vlan – replaces the VLAN ID of the packets with the one you configured. • rate-limit – enables bandwidth limitations on the traffic flows. inactive – disables the policy rule.		
no policy <*name*>	Deletes the policy.	C	13
no policy <*name*> inactive	Enables a policy.	C	13

64.3 Command Examples

This example creates a policy (**highPriority**) for the traffic flow identified through classifier **VLAN3** (see the classifier example in Chapter 15 on page 58). 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;
```

This example creates a policy (**Policy1**) for the traffic flow identified through classifier **Class1** (see the classifier example in Chapter 15 on page 58). This policy forwards **Class1** packets to port 8.

```
sysname(config)# policy Policy1 classifier Class1 egress-port 8 outgoing-
eport
sysname(config)# exit
sysname# show policy Policy1
Policy Policy1:
  Classifiers:
    Class1;
  Parameters:
    VLAN = 1; Priority = 0;
    Egress Port = 8;
    Bandwidth = 64;
  Action:
    Send the packet to the egress port;
sysname#
```

CHAPTER 65
Policy Route Commands

65.1 Policy Route Overview

Use these commands to configure policy route to override the default routing behavior and alter the packet forwarding. Policy-based routing is based on the classification of traffic flows and applied to incoming packets prior to the normal routing. A classifier distinguishes traffic into flows based on the configured criteria.

Note: Configure layer-3 classifiers before you configure policy routing. See Chapter 15 on page 58 for more information on classifiers.

65.2 Command Summary

The following section lists the commands for this feature.

Table 185 policy-route Command Summary

COMMAND	DESCRIPTION	M	P
`show ip policy-route`	Displays all policy routing profile settings.	E	3
`show ip policy-route <name>`	Displays the specified policy routing profile settings. *name*: 32 alphanumeric characters	E	3
`show ip policy-route <name> sequence <number>`	Displays settings for the specified policy routing rule in a profile. sequence: sets the rule number from 1 to 64. The ordering of policy routing rules is important as rules are applied in turn.	E	3
`ip policy-route <name>`	Sets a a policy routing profile with the specified name. You must configure a profile before you can configure a rule.	C	13
`ip policy-route <name> inactive`	Disables a policy routing profile.	C	13
`ip policy-route <name> sequence <number> <permit|deny> classifier <classifier> next-hop <ip-addr>`	Configures a policy routing rule in the specified profile. `permit|deny`: turns on or off this policy routing rule. `classifier`: sets the name of active layer 3 classifier to which this rule applies. `next-hop`: sets the IP address of the gateway to which the Switch forwards the matched traffic.	C	13
`no ip policy-route <name>`	Deletes the specified policy routing profile.	C	13

Table 185 policy-route Command Summary (continued)

COMMAND	DESCRIPTION	M	P
no ip policy-route <*name*> inactive	Enables a policy routing profile.	C	13
no ip policy-route <*name*> sequence <*number*>	Deletes a rule from the specified policy routing profile.	C	13

65.3 Command Examples

By default, the Switch forwards all packets to the default gateway. This example configures a layer 3 classifier (Class-1) to group traffic with source IP address 192.168.2.13. This example also creates a policy routing rule in profile Profile-1 to set the Switch to forward packets that match the layer 3 classifier to the gateway with IP address 10.1.1.99. It then shows the policy routing information.

```
sysname# configure
sysname(config)# classifier Class-1 source-ip 192.168.2.13 mask-bits 24
sysname(config)# ip policy-route Profile-1 sequence 5 permit classifier
Class-1 next-hop 10.1.1.99
sysname(config)# exit
sysname# show ip policy-route
ActiveProfile Name                    Sequence  State   Classifier

-----------------------------------------------------------------
Yes   Profile-1                       5         permit  Class-1

sysname# show ip policy-route Profile-1 sequence 5
Policy route profile: Profile-1 Yes
Information: permit 5
Classifier: Class-1
Action:
 Next hop: 10.1.1.99
Matched policy route: 19074 packets
sysname#
```

CHAPTER 66 Port Authentication Commands

66.1 Port Authentication Overview

This chapter describes the IEEE 802.1x, MAC, and Guest VLAN authentication methods.

Port authentication is a way to validate client access to ports on the Switch using an external authentication server. The Switch supports the following methods for port authentication:

- **IEEE 802.1x Authentication**: An authentication server validates access to the port based on a user name and password provided by the user.
- **MAC Authentication**: An authentication server validates access to the port based on the MAC address and password of the user.
- **Guest VLAN** – In either mode, if authentication fails the Switch can still allow the user to access the network on a **Guest VLAN**.
- **Compound Authentication**: An authentication server validates access to a port based on combination of IEEE 802.1x and MAC authentication. There are two modes:
  - **Loose**: Select **Loose** to allow network access to clients when clients pass IEEE 802.1x authentication OR MAC authentication.
  - **Strict**: Select **Strict** to allow network access to clients only when clients pass IEEE 802.1x authentication and MAC authentication.

Note: All types of authentication use the RADIUS (Remote Authentication Dial In User Service, RFC 2138, 2139) protocol to validate users. You must configure a RADIUS server before enabling port authentication. For details, see Chapter 74 on page 296.

Note: IEEE 802.1x is not supported by all client operating systems. For details on compatibility, see your operating system documentation. If your operating system does not support 802.1x, you must install 802.1x client software.

66.2 IEEE 802.1x and Compound Authentication Commands

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

Table 186 IEEE 802.1x and compound authentication values

COMMAND	DESCRIPTION
<port-list>	A list of one or more ports, separated by commas with no spaces. The list may also contain ranges of ports signified by a hyphen. For example: 1,3,5–8,10.

The following table lists the commands for IEEE 802.1x and Compound Authentication.

Table 187 IEEE 802.1x and compound authentication Command Summary

COMMAND	DESCRIPTION	M	P
`no port-access-authenticator`	Disables IEEE 802.1x port authentication on the Switch.	C	13
`no port-access-authenticator eapol-flood`	Disables EAPoL flood.	C	13
`no port-access-authenticator <port-list>`	Disables IEEE 802.1x authentication on the listed ports.	C	13
`no port-access-authenticator <port-list> reauthenticate`	Disables the IEEE 802.1x re-authentication mechanism on the listed ports.	C	13
`no port-access-authenticator <port-list> guest-vlan`	Disables the guest VLAN feature on the listed ports.	C	13
`no port-access-authenticator <port-list> guest-vlan Host-mode`	Resets the guest VLAN host-mode to its default settings (`Multi-host`).	C	13
`port-access-authenticator`	Enables IEEE 802.1x authentication on the Switch.	C	13
`port-access-authenticator eapol-flood`	Floods EAPoL (EAP over LAN) packets to all ports in the same VLAN. EAPoL is a port authentication protocol used in IEEE 802.1x. It is used to encapsulate and transmit EAP packets between the supplicant (a client device that requests access to the network resources or services) and authenticator (the Switch) directly over the LAN. EAPoL flood will not take effect when you enable 802.1x authentication in the Web Configurator or CLI using `port-access-authenticator`.	C	13
`port-access-authenticator <port-list>`	Enables IEEE 802.1x authentication on the specified ports.	C	13
`port-access-authenticator <port-list> compauth-mode <strict|loose>`	Enables compound authentication on the specified ports. Compound authentication uses a combination of IEEE 802.1x and MAC authentication, and has two modes: • **Strict:** Clients authenticate using both IEEE 802.1x and MAC authentication. • **Loose:** Clients authenticate using either IEEE 802.1x or MAC authentication.	C	13
`port-access-authenticator <port-list> guest-vlan`	Enables the guest VLAN feature on the specified ports.	C	13
`port-access-authenticator <port-list> guest-vlan <vlan-id>`	Sets the guest VLAN ID number on the specified ports.	C	13

Table 187 IEEE 802.1x and compound authentication Command Summary (continued)

COMMAND	DESCRIPTION	M	P
port-access-authenticator <*port-list*> guest-vlan Host-mode Multi-host	Sets the Switch to authenticate only the first client that connects to the listed ports. If the first user enters the correct credential, any other users are allowed to access the ports without authentication. Otherwise, they are all put in the guest VLAN. Once the first user who did authentication logs out or disconnects from the port, rest of the users are blocked until a user does the authentication process again.	C	13
port-access-authenticator <*port-list*> guest-vlan Host-mode Multi-secure [<1-5>]	Sets the Switch to authenticate each client that connects to the listed ports. Optionally, sets the maximum number of the clients that the Switch authenticates on the ports. The maximum number supported varies by Switch (5 in this example).	C	13
port-access-authenticator <*port-list*> max-req <1-10>	Sets the number of times the Switch tries to authenticate a client before sending the client to the guest VLAN.	C	13
port-access-authenticator <*port-list*> quiet-period <0-65535>	Sets the number of seconds the ports remains in the HELD state and rejects further authentication requests from the client after a failed authentication exchange.	C	13
port-access-authenticator <*port-list*> supp-timeout <30-65535>	Sets the number of seconds the Switch waits for client's response to the authentication request before sending a request again.	C	13
port-access-authenticator <*port-list*> tx-period <1-65535>	Sets the number of seconds the Switch waits before re-sending an authentication request to clients on the specified ports.	C	13
port-access-authenticator <*port-list*> reauthenticate	Sets the Switch to periodically send a new authentication request to clients connected to the specified ports. The clients must reauthenticate to stay connected.	C	13
port-access-authenticator <*port-list*> reauth-period <1-65535>	Specifies how often (in seconds) a client has to reauthenticate using IEEE 802.1x in order to stay connected to the specified ports.	C	13
show port-access-authenticator	Displays all IEEE 802.1x port authentication settings.	E	3
show port-access-authenticator <*port-list*>	Displays IEEE 802.1x port authentication settings for the specified ports.	E	3

66.2.1 IEEE 802.1x Authentication Example

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 IEEE 802.1x port authentication on the Switch.
4. Enables IEEE 802.1x port authentication on ports 4 – 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. Enables the guest VLAN feature on port 8.
2. Puts port 8 in guest VLAN 200.
3. Sets host mode to multi-secure to have the Switch authenticate each client that connects to port 8.

```
sysname(config)# port-access-authenticator 8 guest-vlan
sysname(config)# port-access-authenticator 8 guest-vlan 200
sysname(config)# port-access-authenticator 8 guest-vlan Host-mode Multi-
secure
```

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
```

66.2.2 Compound Authentication Example

In this example, we enable loose compound authentication on port 1.

```
sysname# config
sysname(config)# port-access-authenticator 1 compauth-mode loose
sysname(config)# exit
sysname# show port-access-authenticator
802.1x-Active : No
EAPOL flooding : No

port 1
Active :  No
Authorized :  No
Reauthenticate : Yes
Reauth-Period : 3600
Tx-period : 30
Quiet-period :  60
supp-timeout :  30
Max-req :  2
Guest-Vlan Acitve :  No
Guest-Vlan :  1
Host-Mode :  Multi-host
Compound Authentication Mode: Loose
```

66.3 MAC Authentication Commands

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

Table 188 MAC-authentication values

COMMAND	DESCRIPTION
<port-list>	A list of one or more ports, separated by commas with no spaces. The list may also contain ranges of ports signified by a hyphen. For example: 1,3,5–8,10.

The following table lists the commands for MAC address-based port authentication.

Table 189 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 case <upper|lower>`	Sets the case (upper or lower) the external server requires for using MAC addresses as the account username and password. For example, use `mac-authentication case upper` and `mac-authentication delimiter dash` if you need to use a MAC address formatted like 00-11-AC-01-A0-11 as the user name and password.	C	13

Table 189 Mac-authentication Command Summary (continued)

COMMAND	DESCRIPTION	M	P
mac-authentication delimiter <dash|colon|none>	Specifies the separator the external server uses for the two-character pairs within MAC addresses used as the account username and password. For example, use mac-authentication case upper and mac-authentication delimiter dash if you need to use a MAC address formatted like 00-11-AC-01-A0-11 as the username and password.	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 except [?], [|], ['], ["], [space], or [,].	C	13
mac-authentication password-type <static|mac-address>	Sets the password type (static or mac-address) for the MAC authentication password. <static>: Have the Switch send the password you specify using the mac-authentication password <*name-string*> command. <mac-address>: Have the Switch use the client MAC address as the password.	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 setting is superseded by the mac-aging-time command.	C	13
no mac-authentication	Disables MAC authentication on the Switch.	C	13
no mac-authentication timeout	Sets the MAC address entries learned through 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 through a RADIUS server on the ports.	C	13
no mac-authentication	Disables MAC authentication through a RADIUS server on the ports.	C	13
mac-authentication trusted-vlan <*vlan-list*>	Sets the clients in the specified VLANs to access the ports and the connected networks without MAC authentication.	C	13
no mac-authentication trusted-vlan <*vlan-list*>	Removes the trusted VLAN settings.	C	13

66.3.1 MAC Authentication Command Examples

This example enables MAC port authentication on the Switch, and then sets the name prefix to **clientName** and the MAC authentication password to **Lech89**. Next, MAC authentication is activated on ports 1 – 5 and the 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
```

CHAPTER 67
Port Security Commands

67.1 Port Security Overview

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 addresses for a port.

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

67.2 Command Summary

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

Table 190 Interface Command Values

COMMAND	DESCRIPTION
port-list	A list of one or more ports, separated by commas with no spaces. The list may also contain ranges of ports signified by a hyphen. For example: 1,3,5–8,10.

The following section lists the commands for this feature.

Table 191 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 ports.	E	3
port-security	Enables port security on the Switch.	C	13
no port-security	Disables port security on the Switch.	C	13
port-security <*port-list*>	Enables port security on the specified ports.	C	13
no port-security <*port-list*>	Disables port security on the specified ports.	C	13
port-security <*port-list*> learn inactive	Disables MAC address learning on the specified ports.	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 ports.	C	13

Table 191 port-security Command Summary (continued)

COMMAND	DESCRIPTION	M	P
port-security <*port-list*> MAC-freeze	Stops MAC address learning and enables port security on the ports. Note: All previously-learned dynamic MAC addresses are saved to the static MAC address table.	C	13
port-security <*port-list*> vlan <*vlan-id*> address-limit <*number*>	Limits the number of (dynamic) MAC addresses that may be learned on the specified ports in a specified VLAN.	C	13
no port-security <*port-list*> vlan <*vlan-id*> address-limit	Removes the specified VLAN MAC address limit.	C	13
port-security <*port-list*> vlan <*vlan-id*> address-limit <*number*> inactive	Disables the specified VLAN MAC address limit.	C	13
no port-security <*port-list*> vlan <*vlan-id*> address-limit inactive	Enables the specified VLAN MAC address limit.	C	13

67.3 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
```

CHAPTER 68 Port-based VLAN Commands

68.1 Port-based VLAN Overview

Use these commands to configure port-based VLAN.

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

68.2 Command Summary

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

Table 192 Interface Command Values

COMMAND	DESCRIPTION
port-list	A list of one or more ports, separated by commas with no spaces. The list may also contain ranges of ports signified by a hyphen. For example: 1,3,5–8,10.

The following section lists the commands for this feature.

Table 193 egress Command Summary

COMMAND	DESCRIPTION	M	P
show interfaces config <*port-list*> egress	Displays outgoing port information for the specified ports.	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 ports.	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

68.3 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
```

CHAPTER 69
PPPoE IA Commands

69.1 PPPoE Intermediate Agent Overview

A PPPoE Intermediate Agent (PPPoE IA) is deployed between a PPPoE server and PPPoE clients. It helps the PPPoE server identify and authenticate clients by adding subscriber line specific information to PPPoE discovery packets from clients on a per-port or per-port-per-VLAN basis before forwarding them to the PPPoE server.

Use these commands if you want the Switch to add a vendor-specific tag to PADI (PPPoE Active Discovery Initiation) and PADR (PPPoE Active Discovery Request) packets from PPPoE clients. This tag gives a PPPoE termination server additional information (such as the port number, VLAN ID, and MAC address) that the server can use to identify and authenticate a PPPoE client.

69.1.1 Port State

Every port is either a trusted port or an untrusted port for the PPPoE intermediate agent. This setting is independent of the trusted/untrusted setting for DHCP snooping or ARP inspection. You can also specify the agent sub-options (circuit ID and remote ID) that the Switch adds to PADI and PADR packets from PPPoE clients.

Trusted ports are connected to PPPoE servers.

- If a PADO (PPPoE Active Discovery Offer), PADS (PPPoE Active Discovery Session-confirmation), or PADT (PPPoE Active Discovery Terminate) packet is sent from a PPPoE server and received on a trusted port, the Switch forwards it to all other ports.
- If a PADI or PADR packet is sent from a PPPoE client but received on a trusted port, the Switch forwards it to other trusted ports.

Note: The Switch will drop all PPPoE discovery packets if you enable the PPPoE intermediate agent and there are no trusted ports.

Untrusted ports are connected to subscribers.

- If a PADI, PADR, or PADT packet is sent from a PPPoE client and received on an untrusted port, the Switch adds a vendor-specific tag to the packet and then forwards it to the trusted ports.
- The Switch discards PADO and PADS packets which are sent from a PPPoE server but received on an untrusted port.

69.2 Command Summary

The following section lists the commands for this feature.

Table 194 PPPoE Intermediate Agent Command Summary

COMMAND	DESCRIPTION	M	P
clear pppoe intermediate-agent statistics	Removes all statistics records of PPPoE packets on the Switch.	E	13
clear pppoe intermediate-agent statistics vlan <*vlan-list*>	Removes statistics records of PPPoE packets for the specified VLANs.	E	13
interface port-channel <*port-list*>	Enters config-interface mode for the specified ports. The port list must consist of one or more ports, separated by commas with no spaces. The list may also contain ranges of ports signified by a hyphen. For example: 1,3,5-8,10.	C	13
pppoe intermediate-agent trust	Sets the specified ports as PPPoE IA trusted ports.	C	13
pppoe intermediate-agent format-type circuit-id string <*string*>	Specifies a string the Switch adds into the Agent Circuit ID sub-option for PPPoE discovery packets received on this port. Spaces are allowed. *string*: up to 63 ASCII characters	C	13
pppoe intermediate-agent format-type remote-id string <*string*>	Specifies a string the Switch adds into the Agent Remote ID sub-option for PPPoE discovery packets received on this port. Spaces are allowed. *string*: up to 63 ASCII characters	C	13
pppoe intermediate-agent vlan <*vlan-id*> format-type circuit-id string <*string*>	Specifies a string the Switch adds into the Agent Circuit ID sub-option for PPPoE discovery packets received on this VLAN on the specified port. Spaces are allowed. The Circuit ID you configure for a specific VLAN on a port has the highest priority.	C	13
pppoe intermediate-agent vlan <*vlan-id*> format-type remote-id string <*string*>	Specifies a string the Switch adds into the Agent Remote ID sub-option for PPPoE discovery packets received on this VLAN on the specified port. Spaces are allowed. The Remote ID you configure for a specific VLAN on a port has the highest priority.	C	13
no pppoe intermediate-agent trust	Sets the specified ports PPPoE IA untrusted ports.	C	13
no pppoe intermediate-agent format-type circuit-id	Disables the PPPoE IA Circuit ID settings for the specified ports.	C	13
no pppoe intermediate-agent format-type remote-id	Disables the PPPoE IA Remote ID settings for the specified ports.	C	13
no pppoe intermediate-agent vlan <*vlan-id*> format-type circuit-id	Disables the PPPoE IA Circuit ID settings for the specified ports on the specified VLANs.	C	13
no pppoe intermediate-agent vlan <*vlan-id*> format-type remote-id	Disables the PPPoE IA Remote ID settings for the specified ports on the specified VLANs.	C	13
no pppoe intermediate-agent	Disables PPPoE IA globally.	C	13
no pppoe intermediate-agent vlan <*vlan-list*> remote-id	Disables the PPPoE IA Remote ID settings for the specified VLANs.	C	13

Table 194 PPPoE Intermediate Agent Command Summary (continued)

COMMAND	DESCRIPTION	M	P
no pppoe intermediate-agent format-type access-node-identifier	Removes the access-node-identifier you have set.	C	13
no pppoe intermediate-agent format-type identifier-string	Removes the identifier-string you have set.	C	13
no pppoe intermediate-agent format-type identifier-string hostname	Sets the Switch to not add the Switch's host name to the identifier-string.	C	13
no pppoe intermediate-agent vlan <*vlan-list*>	Disables PPPoE IA for the specified VLANs.	C	13
no pppoe intermediate-agent vlan <*vlan-list*> circuit-id	Disables the PPPoE IA Circuit ID settings for the specified VLANs.	C	13
pppoe intermediate-agent	Enables PPPoE Intermediate Agent (PPPoE IA) globally.	C	13
pppoe intermediate-agent format-type identifier-string hostname	Sets the Switch to add the Switch's host name to the identifier-string.	C	13
pppoe intermediate-agent format-type access-node-identifier string <*string*>	Sets the access-node-identifier string. *string*: Enter up to 20 alphanumeric characters to identify the PPPoE intermediate agent. Hyphens (-) and spaces are also allowed. The default is the Switch's host name.	C	13
pppoe intermediate-agent format-type identifier-string string <*string*> option <s|p|v|sp|sv|pv|spv> delimiter <#|.|,|;|/| |>	This command sets the following: • a string that the Switch adds in the Agent Circuit ID sub-option • the variables to generate and add in the Agent Circuit ID sub-option, • a delimiter to separate the identifier-string, slot ID, port number and/or VLAN ID from each other. *string*: You can up to 63 printable characters. Spaces are allowed. option <s|p|v|sp|sv|pv|spv>: s, p and v indicate slot, port, vlan, and sp, sv, pv and spv indicate combinations of slot-port, slot-VLAN, port-VLAN and slot-port-VLAN respectively. The Switch enters a zero into the PADI and PADR packets for the slot value. delimiter <#|.|,|;|/| |>: You can use a pound key (#), semi-colon (**;**), period (**.**), comma (**,**), forward slash (***/***) or a space.	C	13
pppoe intermediate-agent vlan <*vlan-list*>	Enables PPPoE IA for the specified VLANs.	C	13
pppoe intermediate-agent vlan <*vlan-list*> circuit-id	Enables the PPPoE IA Circuit ID settings for the specified VLANs.	C	13
pppoe intermediate-agent vlan <*vlan-list*> remote-id	Enables the PPPoE IA Remote ID settings for the specified VLANs.	C	13
show pppoe intermediate-agent	Shows the PPPoE IA settings.	E	13
show pppoe intermediate-agent statistic	Shows the statistics of PPPoE packets handled (received, forwarded and dropped) by PPPoE IA on the Switch.	E	13
show pppoe intermediate-agent statistic vlan <*vlan-list*>	Shows the statistics of PPPoE packets for the specified VLANs.	E	13

69.3 Command Examples

This is an example of how to enable and disable PPPoE IA on the Switch.

```
sysname# configure
sysname(config)# pppoe intermediate-agent
sysname(config)# no pppoe intermediate-agent
```

This is an example of how to enable and configure PPPoE IA for VLANs.

```
sysname# configure
sysname(config)# pppoe intermediate-agent vlan 2
sysname(config)# pppoe intermediate-agent vlan 5,9,11
sysname(config)# pppoe intermediate-agent vlan 1 circuit-id
sysname(config)# pppoe intermediate-agent vlan 3,6 remote-id
sysname(config)# no pppoe intermediate-agent vlan 2-10
sysname(config)# no pppoe intermediate-agent vlan 1 circuit-id
sysname(config)# no pppoe intermediate-agent vlan 3,6 remote-id
```

This is an example of how to set a PPPoE IA trust port.

```
sysname# configure
sysname(config)# interface port-channel 3
sysname(config-interface)# pppoe intermediate-agent trust
sysname(config-interface)# no pppoe intermediate-agent trust
```

This example is more advanced. It assumes a PPPoE IA client is connected to port 2 and a PPPoE IA server is connected to port 5. If we want PPPoE IA to work, port 2 and port 5 must be belong to the some VLAN and the PPPoE IA must be enabled globally and in this corresponding VLAN. We also need to set port 5 as trust port. Then the last thing we need to do is to decide which sub-options the received PADI, PADR, or PADT packet needs to carry. Here, assume both circuit-id and remote-id should be carried.

```
sysname# configure
sysname(config)# vlan 2
sysname(config-vlan)# fixed 2,5
sysname(config-vlan)# untagged 2,5
sysname(config-vlan)# exit
sysname(config)# pppoe intermediate-agent
sysname(config)# pppoe intermediate-agent vlan 2
sysname(config)# interface port-channel 2
sysname(config-interface)# pvid 2
sysname(config-interface)# exit
sysname(config)# interface port-channel 5
sysname(config-interface)# pvid 2
sysname(config-interface)# pppoe intermediate-agent trust
sysname(config-interface)# exit
sysname(config)# pppoe intermediate-agent vlan 2 circuit-id
sysname(config)# pppoe intermediate-agent vlan 2 remote-id
```

69.3.1 Vendor-Specific Tag Examples

The following examples show you how to configure the vendor-specific tag for PPPoE IA. They assume there is a PPPoE IA client connected to port 2 and PPPoE IA server (or up-link port) connected to port 5.

```
sysname# configure
sysname(config)# pppoe intermediate-agent
sysname(config)# pppoe intermediate-agent format-type access-node-
identifier string test
sysname(config)# pppoe intermediate-agent vlan 1
sysname(config)# pppoe intermediate-agent vlan 1 circuit-id
sysname(config)# pppoe intermediate-agent vlan 1 remote-id
sysname(config)# interface port-channel 5
sysname(config-interface)# pppoe intermediate-agent trust
sysname(config-interface)#exit
```

This is a variation of the previous one and uses the same initial setup (client on port 2, server on port 5).

```
sysname# configure
sysname(config)# pppoe intermediate-agent
sysname(config)# pppoe intermediate-agent format-type identifier-string
string PrivateTest option spv delimiter /
sysname(config)# pppoe intermediate-agent vlan 1
sysname(config)# pppoe intermediate-agent vlan 1 circuit-id
sysname(config)# pppoe intermediate-agent vlan 1 remote-id
sysname(config)# interface port-channel 5
sysname(config-interface)# pppoe intermediate-agent trust
sysname(config-interface)#exit
```

Because we did not assign the appended string for remote-id in examples 1 and 2, the Switch appends a string to carry the client's MAC address as default. If we want the remote-id to carry the "ForPortVlanRemoteIdTest" information for a specific VLAN on a port, we can add the following configuration:

```
sysname# configure
sysname(config)# interface port-channel 2
sysname(config-interface)# pppoe intermediate-agent vlan 1 format-type
remote-id string ForPortVlanRemoteIdTest
sysname(config-interface)# exit
```

Similarly, we can let the circuit-id carry the information which we configure:

```
sysname# configure
sysname(config)# interface port-channel 2
sysname(config-interface)# pppoe intermediate-agent vlan 1 format-type
circuit-id string ForPortVlanCircuitIdTest
sysname(config-interface)# exit
```

Additionally, we can let the circuit-id or remote-id carry the user-configured information from a specific port whose priority is less than the specific VLAN on a port setting:

```
sysname# configure
sysname(config)# interface port-channel 2
sysname(config-interface)# pppoe intermediate-agent format-type circuit-
id string ForPortCircuitIdTest
sysname(config-interface)# pppoe intermediate-agent format-type remote-
id string ForPortRemoteIdTest
sysname(config-interface)# exit
```

Since we did not assign the appended string for remote-id in example 1 and 2, it will carry the client's MAC address as default.

CHAPTER 70
Private VLAN Commands

70.1 Private VLAN Overview

Use Private VLANs if you want you to block communication between ports in the same VLAN. **Community** and **Isolated** VLANs are secondary private VLANs that must be associated with a **Primary** private VLAN.

- **Primary**: Ports in a **Primary** VLAN are promiscuous and they can communicate with all promiscuous ports in the same primary VLAN, and all ports in associated community and isolated VLANs. They cannot communicate with ports in different primary VLANs.
- **Community**: Ports in a **Community** VLAN can communicate with promiscuous ports in an associated **Primary** VLAN and other community ports in the same **Community** VLAN. They cannot communicate with ports in **Isolated** VLANs, non-associated **Primary** VLAN promiscuous ports nor community ports in different **Community** VLANs.
- **Isolated**: Ports in an **Isolated** VLAN can communicate with promiscuous ports in an associated **Primary** VLAN only. They cannot communicate with other isolated ports in the same **Isolated** VLAN, non-associated **Primary** VLAN promiscuous ports nor any community ports.

Note: You can also prevent ports from communicating with each other in the same VLAN using VLAN Isolation. For details, see Chapter 98 on page 379. If Private VLAN and VLAN Isolation are both enabled, then the VLAN Isolation rules take priority.

70.1.1 Private VLAN Example 1

Figure 11 PVLAN Example 1

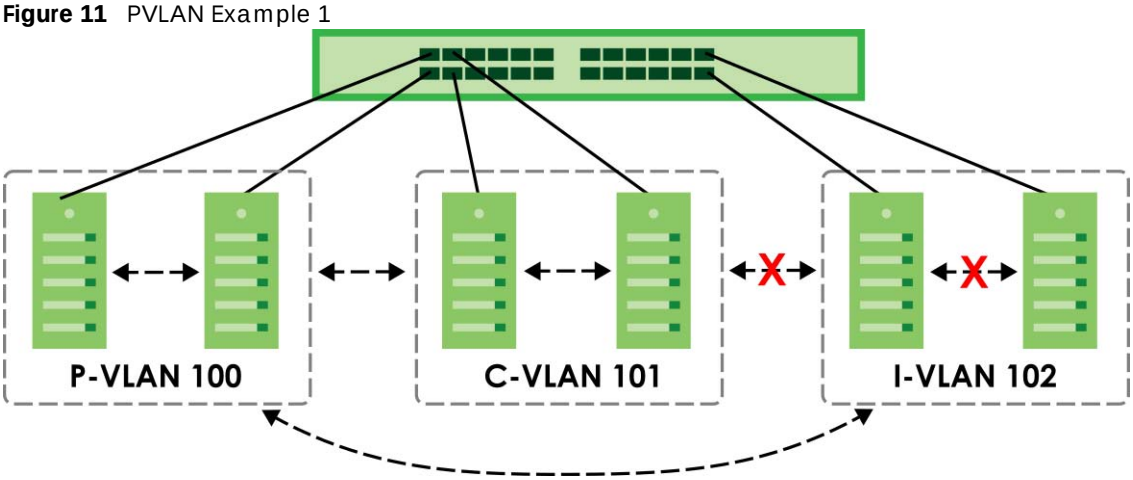


Table 195 PVLAN Example 1 Key

LABEL	DESCRIPTION
P-VLAN 100	Primary private VLAN

Table 195 PVLAN Example 1 Key (continued)

LABEL	DESCRIPTION
C-VLAN 101	Community private VLAN
I-VLAN 102	Isolated private VLAN

70.1.2 Private VLAN Example 2

To apply tagged Private VLANs across switches, you must enable VLAN Trunking on the trunking ports of each switch.

Figure 12 PVLAN Example 2

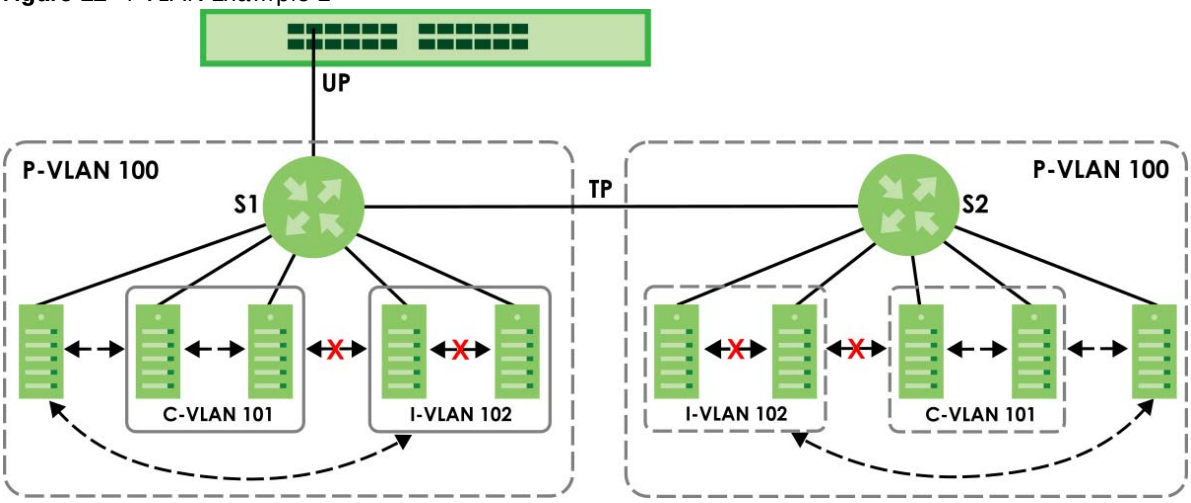


Table 196 Spanning PVLAN Graphic Key

LABEL	DESCRIPTION
UP	Uplink promiscuous port
TP	VLAN-trunking ports
S1, S2	Switch 1, Switch 2
P-VLAN 100	Primary private VLAN with VLAN ID 100
C-VLAN 101	Community private VLAN with VLAN ID 101
I-VLAN 102	Isolated private VLAN with VLAN ID 102

This is the communication process if primary VLAN **P-VLAN 100** is associated with community VLAN **C-VLAN 101** and isolated VLAN **I-VLAN 102**.

- Promiscuous ports in **P-VLAN 100** can communicate with all ports in **P-VLAN 100** including community ports in **C-VLAN 101** and isolated ports in **I-VLAN 102**.
- Community ports in **C-VLAN 101** can communicate with promiscuous ports in **P-VLAN 100** and other community ports in **C-VLAN 101**. They cannot communicate with isolated ports in **I-VLAN 102**.
- Isolated ports can communicate with promiscuous ports in **P-VLAN 100**. They cannot communicate with other isolated ports in **I-VLAN 102** nor community ports in **C-VLAN 101**.

70.1.3 Command Summary

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

Table 197 private-vlan Command Values

COMMAND	DESCRIPTION
port-list	A list of one or more ports, separated by commas with no spaces. The list may also contain ranges of ports signified by a hyphen. For example: 1,3,5–8,10.

The following section lists the commands for this feature.

Table 198 private-vlan Command Summary

COMMAND	DESCRIPTION	M	P
vlan <*vlan-id*>	Enters config-vlan mode for the specified VLAN. The Switch creates the VLAN if it does not already exist. The valid range is 1 – 4094. You cannot select a VLAN that is configured as a voice VLAN.	C	13
private-vlan <primary | isolated | community>	Tags the specified VLAN as a Primary VLAN, Isolated VLAN or a Community VLAN.	C	13
private-vlan association <*secondary-vlan-list*>	Primary private VLANs can associate with several (secondary) Community private VLANs and up to one (secondary) Isolated private VLAN. Specify a primary private VLAN, then associate it with one or more secondary VLANs using this command. The VLAN list may consist of one or more VLAN IDs separated by a comma with no spaces. The list may also contain ranges of VLANs signified by a hyphen. For example: 10,20–30,50.	C	13
no private-vlan <primary | isolated | community>	Untags the VLAN as a Primary, Isolated or Community VLAN.	C	13
no private-vlan association	Removes all association between the primary VLAN and secondary VLANs.	C	13
no private-vlan association <*secondary-vlan-list*>	Removes association between the primary VLAN and the specified secondary VLANs. The VLAN list may consist of one or more VLAN IDs separated by a comma with no spaces. The list may also contain ranges of VLANs signified by a hyphen. For example: 10,20–30,50.	C	13
interface port-channel <*port-list*>	Enters config-interface mode for the specified ports.	C	13
private-vlan mode <promiscuous | isolated | community> association <vlan-id> dot1q <tagged | untagged>	Configures PVLAN on a port. Set the associated PVLAN ID, type of private VLAN and specify whether outgoing frames from this port are tagged or not.	C	13
no private-vlan mode	Removes PVLAN mode configuration.	C	13
show vlan private-vlan	Displays the settings and status of all private VLAN rules on the Switch.	E	3
show vlan private-vlan <*vlan-id*>	Displays the settings and status of the specified private VLAN rule on the Switch.	E	3

70.1.4 Command Example

This example sets private VLAN 100 as a primary private VLAN, private VLAN 101 as a community private VLAN and private VLAN 102 as an isolated private VLAN. VLANs 101 and 102 are secondary private VLANs that are associated primary private VLAN 101. Primary PVLAN 100 is then mapped to port 2 on the Switch and outgoing frames from port 2 will be tagged.

```
sysname# configure
sysname(config)# vlan 100
sysname(config-vlan)# private-vlan primary
sysname(config-vlan)# exit
sysname(config)# vlan 101
sysname(config-vlan)# private-vlan community
sysname(config-vlan)# exit
sysname(config)# vlan 102
sysname(config-vlan)# private-vlan isolated
sysname(config-vlan)# exit
sysname(config)# vlan 100
sysname(config-vlan)# private-vlan association 101,102
sysname(config-vlan)# exit
sysname(config)# exit
sysname# show vlan private-vlan
  Private Vlan:
  Primary  Secondary        Type                 Ports
  -------  ---------  ----------  --------------------
      100               Primary
      100        102    Isolated
      100        101   Community
sysname#
sysname# configure
sysname(config)# interface port-channel 2
sysname(config-interface)# private-vlan mode promiscuous association 100-->
dot1q tagged
sysname(config-interface)# exit
sysname(config)#
```

CHAPTER 71 Protocol-based VLAN Commands

71.1 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 87 on page 349 for subnet-based VLAN commands and Chapter 96 on page 371 for VLAN commands.

71.2 Command Summary

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

Table 199 Interface Command Values

COMMAND	DESCRIPTION
port-list	A list of one or more ports, separated by commas with no spaces. The list may also contain ranges of ports signified by a hyphen. For example: 1,3,5–8,10.

The following section lists the commands for this feature.

Table 200 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 ports.	E	3
`interface port-channel <port-list>`	Enters subcommand mode for configuring the specified ports.	C	13

Table 200 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 do not select a predefined Ethernet protocol (ip, ipx, arp, rarp, appletalk or decnet), type the protocol number in hexadecimal notation with a prefix, "0x". For example, type 0x0800 for the IP protocol and type 0x8137 for the Novell IPX protocol. 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

71.3 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#
```

CHAPTER 72
Proxy Server and NCC Discovery Commands

72.1 Nebula Control Center Overview

If your Switch can be managed through the Zyxel Nebula Control Center (NCC) and is behind a proxy server, you will need to enable NCC discovery and configure the proxy server settings so that the Switch can access the NCC through the proxy server. The Switch will go to Cloud mode (cloud management mode) when it is:

- connected to the Internet
- connected to NCC
- registered on NCC.

72.2 Command Summary

The following table describes the commands available for NCC discovery.

Table 201 NCC Discovery Command Summary

COMMAND	DESCRIPTION	M	P
[no] cloud center discovery	Turns on NCC discovery on the Switch. The Switch will try to discover the NCC and go into Cloud mode when it is connected to the Internet and NCC, and has been registered on NCC. The no command turns off NCC discovery. If NCC discovery is disabled, the Switch will not discover the NCC and remain in Standalone mode.	C	14
show cloud	Displays whether NCC discovery is enabled/disabled on the Switch, and whether the Switch is in Standalone/Cloud mode. If the NCC discovery is enabled, Nebula connection status log will display. Use the status log for troubleshooting if the Switch cannot go into Cloud mode.	E	3

The proxy server of an organization may prohibit communication between the Switch and NCC (Nebula Control Center). Use these commands to enable communication between the Switch and NCC through an proxy server.

Table 202 Proxy Server Command Summary

COMMAND	DESCRIPTION	M	P
`[no] client proxy-server http`	Enables or disables communication between the Switch and NCC through an HTTP proxy server.	C	14
`[no] client proxy-server http authentication`	Enables or disables HTTP proxy server authentication using a username and password.	C	14
`client proxy-server http username <name> password <pwd>`	Sets a username and password to use for proxy server authentication. *name*: 1 – 32 characters consisting of letters, numbers, and any special characters in the square brackets: [~!@#$%^&*()_+{}|:"<>?–=[]\;',./‘]. *pwd*: 1 – 32 characters consisting of letters, numbers, and any special characters except [?], [|], ['], ["], [space], or [,].	C	14
`client proxy-server http username <name> password encrypt <pwd>`	Sets a username and an encrypted password to use for proxy server authentication. *name*: 1 – 32 alphanumeric characters are allowed including special characters in the square brackets: [~!@#$%^&*()_+{}|:"<>?–=[]\;',./‘]. *pwd* : A pre-encrypted 32-character password string.	C	14
`client proxy-server http server <ip|hostname> port <socket-number>`	Sets the address and port number of the proxy server. <*ip*|*hostname*>: Enter the IP address (dotted decimal notation) or host name of the proxy server. When entering the host name, up to 128 alphanumeric characters are allowed including special characters inside the square quotes [~!@#$%^&*()_+{}|:"<>?–=[]\;',./‘] <socket-number>: Enter the port number of the proxy server (1 – 65535).	C	14
`show client proxy-server http`	Displays the current client HTTP proxy server settings.	E	3

72.3 Command Examples

The following example shows you how to enable NCC discovery and check the Nebula connection status on the Switch.

```
sysname# config
sysname(config)# cloud center discovery
sysname(config)# exit
sysname# show cloud
  Hybrid Mode: Standalone
  Nebula Discovery: Enable
  Cloud Center:
        Address d.nebula.zyxel.com
        port            4335, 6667
        IP address      0.0.0.0
  Nebula Connection Status:
        [Internet]
           Status: Fail
           Message: Gateway is unreachable, please check the connection.
           Log Time: 2022-04-29 02:29:20 (UTC+00:00)
        [Nebula]
           Status: Fail
           Message: Contact Nebula or ISP support to verify if your DNS can resolve
                    NCC.
           Log Time: 2022-04-29 02:29:15 (UTC+00:00)
        [Registration]
           Status: Ignore
           Message: Device is not registered yet, please register it with NCC.
           Log Time: 2022-04-25 09:45:11 (UTC+00:00)
sysname#
```

This example allows NCC traffic through an HTTP proxy server that has authentication enabled.

```
sysname# configure
sysname(config)# client proxy-server http
sysname(config)# client proxy-server http authentication
sysname(config)# client proxy-server http username ZyxelUser password
1234
sysname(config)# client proxy-server http server www.zyxel.com.tw port
3100
sysname(config)# exit
sysname# show client proxy-server http
  HTTP Proxy Information:
    Proxy State: Enable
      Server: www.zyxel.com.tw
      Port: 3100
    Proxy Authentication State: Enable
      Username: ZyxelUser
```

CHAPTER 73
Queuing Commands

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

Note: 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.

73.1 Queuing Overview

The following queuing algorithms are supported by Zyxel Switches:

Note: 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.

Note: Switch models which have only four 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.

73.2 Command Summary: Port by Port Configuration

The following section lists the commands for this feature.

Table 203 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 four queues.	C	13
interface port-channel <*port-list*>	Enters subcommand mode for configuring the specified ports. The port list must consist of one or more ports, separated by commas with no spaces. The list may also contain ranges of ports signified by a hyphen. For example: 1,3,5–8,10.	C	13
spq	Sets the switch to use Strictly Priority Queuing (SPQ) on the specified ports.	C	13
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
no hybrid-spq	Disables 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
wrr <*wt1*> <*wt2*> ... <*wt8*>	Assigns a weight value to each physical queue on the Switch.	C	13

73.3 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
```

73.4 Command Summary: System-Wide Configuration

The following section lists the commands for this feature.

Table 204 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 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 four 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
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

73.5 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 queuing 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
```

CHAPTER 74
RADIUS Commands

74.1 Command Summary

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

The following section lists the commands for this feature.

Table 205 radius-server Command Summary

COMMAND	DESCRIPTION	M	P
show radius-server	Displays RADIUS server settings and attributes.	E	3
radius-server host <*index*> <*ip* | *ipv6*> [auth-port <*socket-number*>] [key <*key-string*> | key-cipher <encrypted-*key-string*>]	Specifies the IP/IPv6 address of the RADIUS authentication server. The UDP port number and shared secret are optional. *index*: 1 or 2. cipher: inform the Switch that the string after the word "cipher" is an encrypted secret. This is only used when the Switch is restoring the encrypted key from a configuration file. To encrypt the key, use the aaa server key encryption command. *key-string*: 1 – 32 alphanumeric characters except [?], [|], ['], ["], [space], or [,].	C	14
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	14
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. 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	14
no radius-server <*index*>	Resets the specified RADIUS server to its default values.	C	14

Table 205 radius-server Command Summary (continued)

COMMAND	DESCRIPTION	M	P
radius-server attribute nas-ip-address <*ip-address*>	Sets the NAS IP Address attribute of the RADIUS server to the specified address. Note: This attribute is used if you have multiple NAS devices in a cluster, and you want the RADIUS server to treat all clustered NAS devices as a single device for accounting. In this situation, put all clustered NAS devices behind a NAT router, then assign the public IP address of the NAT router as the nas-ip-address.	C	14
no radius-server attribute nas-ip-address	Clears the NAS IP Address attribute of the RADIUS server.	C	14

Table 206 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
radius-accounting host <*index*> <*ip* | *ipv6*> [acct-port <*socket-number*>] [key <*key-string*> | key-cipher <encrypted-*key-string*>]	Specifies the IP/IPv6 address of the RADIUS accounting server. The port number and key of the external RADIUS accounting server are optional. *index*: 1 or 2. cipher: inform the Switch that the string after the word "cipher" is an encrypted secret. This is only used when the Switch is restoring the encrypted key from a configuration file. To encrypt the key, use the aaa server key encryption command. *key-string*: 1 – 32 alphanumeric characters except [?], [|], ['], ["], [space], or [,].	C	13
no radius-accounting <*index*>	Resets the specified RADIUS accounting server to its default values.	C	13

74.2 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
```

This example sets the NAS IP Address attribute of the RADIUS server to 192.168.33.11.

```
sysname# configure
sysname(config)# radius-server attribute nas-ip-address 192.168.33.11
sysname(config)# exit
sysname# show radius-server
RADIUS Server Information
        Timeout: 30
        Mode: index-priority

        RADIUS server 1:
                host-ip:        172.16.10.11
                auth-port:      1812
        RADIUS server 2:
                host-ip:        172.16.10.11
                auth-port:      1812
        Attribute
                NAS-IP-Address: 192.168.33.11
```

CHAPTER 75
Remote Management Commands

75.1 Remote Management Overview

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.

75.2 Command Summary

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

Table 207 remote-management User-input Values

COMMAND	DESCRIPTION
index	1 – 16

The following section lists the commands for this feature.

Table 208 remote-management Command Summary

COMMAND	DESCRIPTION	M	P
`show remote-management [index]`	Displays all trusted client information with an IPv4 address or, optionally, a specific group of trusted clients with an IPv4 address.	E	3
`show remote-management6 [index]`	Displays all trusted client information with an IPv6 address or, optionally, a specific group of trusted clients with an IPv6 address. Note: See Table 8 on page 13 for the product that supports this command.	E	3
`remote-management <index>`	Enables the specified group of trusted clients with an IPv4 address.	C	13
`remote-management6 <index>`	Enables the specified group of trusted clients with an IPv6 address.	C	13
`no remote-management <index>`	Disables the specified group of trusted clients with an IPv4 address.	C	13
`no remote-management6 <index>`	Disables the specified group of trusted clients with an IPv6 address.	C	13

Table 208 remote-management Command Summary (continued)

COMMAND	DESCRIPTION	M	P
`remote-management <index> start-addr <ip> end-addr <ip> service <[telnet] [ftp] [http] [icmp] [snmp] [ssh] [https]>`	Specifies a group of trusted clients with an IPv4 address from which an administrator may use the specified services to manage the Switch. Group `0.0.0.0 - 0.0.0.0` refers to every clients with an IPv4 address.	C	13
`no remote-management <index> service <[telnet] [ftp] [http] [icmp] [snmp] [ssh] [https]>`	Disables the specified services for the specified group of trusted clients with an IPv4 address.	C	13
`remote-management6 <index> start-addr <ipv6> end-addr <ipv6> service <[telnet] [ftp] [http] [icmp] [snmp] [ssh] [https]>`	Specifies a group of trusted clients with an IPv6 address from which an administrator may use the specified services to manage the Switch. Group 0000:0000:0000::0000 – 0000:0000:0000::0000 refers to every clients with an IPv6 address. Note: See Table 8 on page 13 for the product that supports this command.	C	13
`no remote-management6 <index> service <[telnet] [ftp] [http] [icmp] [snmp] [ssh] [https]>`	Disables the specified services for the specified group of trusted clients with an IPv6 address.	C	13

Table 209 service-control Command Summary

COMMAND	DESCRIPTION	M	P
`show service-control`	Displays service control settings.	E	3
`service-control console <timeout>`	Defines the timeout period (in minutes) for a management session through the console port.	C	13
`service-control ftp`	Allows FTP access to the Switch.	C	13
`service-control ftp <socket-number> <timeout>`	Specifies the service port for the FTP service and defines the timeout period (in minutes).	C	13
`no service-control ftp`	Disables FTP access to the Switch.	C	13
`service-control http`	Allows HTTP access to the Switch.	C	13
`service-control http <socket-number> <timeout>`	Specifies the service port for the HTTP service and defines the timeout period (in minutes). *timeout*: 1 – 255 Note: The HTTP and HTTPS sessions will be set to use the same timeout value.	C	13
`no service-control http`	Disables HTTP access to the Switch.	C	13
`service-control http redirect-to-https`	Allows your web browser to automatically redirect to a secure HTTPS login page, from HTTP. Note: See Table 8 on page 13 for the product that supports this command.	C	13
`no service-control http redirect-to-https`	Disables your web browser from being automatically redirected to a secure HTTPS login page, from HTTP.	C	13
`service-control https`	Allows HTTPS access to the Switch.	C	13
`service-control https <socket-number>`	Specifies the service port for the HTTPS service.	C	13
`no service-control https`	Disables HTTPS access to the Switch.	C	13
`service-control icmp`	Allows ICMP management packets.	C	13

Table 209 service-control Command Summary (continued)

COMMAND	DESCRIPTION	M	P
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	Allows SSH access to the Switch.	C	13
service-control ssh <*socket-number*>	Specifies the service port for the SSH service.	C	13
no service-control ssh	Disables SSH access to the Switch.	C	13
service-control telnet	Allows Telnet access to the Switch.	C	13
service-control telnet <*socket-number*> <*timeout*>	Specifies the service port for the Telnet service and defines the timeout period (in minutes). Note: The timeout period you specified for Telnet sessions also applies to SSH sessions.	C	13
service-control telnet login-timeout <*timeout*>	Defines how many seconds (from 30 to 300) the Switch waits before stopping a computer's failed attempt to log in and access the Switch. Note: The login timeout period you specified for Telnet sessions also applies to SSH sessions.	C	13
no service-control telnet	Disables Telnet access to the Switch.	C	13

75.3 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 allows computers only in the 2001::1 to 2001::5 IPv6 address range to access the Switch through any telnet, FTP or HTTP services only. This prevents other computers from accessing the Switch at all.

```
sysname# configure
sysname(config)# remote-management6 1 start-addr 2001::1 end-addr
--> 2001::5 service telnet ftp http
sysname(config)# remote-management6 1
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
```

CHAPTER 76
RIP Commands

76.1 RIP Overview

Routing Information Protocol (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.

Apart from RIPv1 and RIPv2 for IPv4, the Switch also supports RIPng (RIP next generation) for IPv6. RIPv2 uses UDP port 520 and the Multicast address 224.0.0.9, while RIPng uses UDP port 521 and the Multicast address FF02::9.

Note: You must purchase the Advance Routing service license and go to myZyxel to activate it for your Switch in order to use advanced L3 routing features, such as RIPng and OSPFv3 for IPv6. See Chapter 79 on page 316 for more information.

76.2 Command Summary

The following section lists the commands for this feature.

Table 210 rip Command Summary

COMMAND	DESCRIPTION	M	P
`show router rip`	Displays global RIP settings.	E	3
`show ip protocols`	Displays the routing protocol the Switch is using and its administrative distance value.	E	3
`router rip`	Enables and enters the RIP configuration mode on the Switch.	C	13

Table 210 rip Command Summary (continued)

COMMAND	DESCRIPTION	M	P
distance <10-255>	When two different routing protocols, such as RIP and OSPF provide multiple routes to the same destination, the Switch can use the administrative distance of the route source to determine which routing protocol to use and add the route to the routing table. Sets the administrative distance (from 10 to 255) that is assigned to the routes learned by RIP. The lower the administrative distance value is, the more preferable the routing protocol is. If two routes have the same administrative distance value, the Switch uses the route that has the lowest metric value. Note: You cannot set two routing protocols to have the same administrative distance.	C	13
exit	Leaves the RIP configuration mode.	C	13
ipv6 router rip	Enables and enters the IPv6 RIP configuration mode on the Switch.	C	13
distance <10-255>	When two different routing protocols, such as RIP and OSPF provide multiple routes to the same destination, the Switch can use the administrative distance of the route source to determine which routing protocol to use and add the route to the routing table. Sets the administrative distance (from 10 to 255) that is assigned to the routes learned by RIP. The lower the administrative distance value is, the more preferable the routing protocol is. If two routes have the same administrative distance value, the Switch uses the route that has the lowest metric value. Note: You cannot set two routing protocols to have the same administrative distance.	C	13
exit	Leaves the RIP configuration mode.	C	13
timer garbage-collection <1-65535>	Sets how long (in seconds) the Switch waits before removing the invalid route from the routing table.	C	13
timer timeout <1-65535>	Sets how long (in seconds) the Switch waits for route updates before a route is declared no longer valid. The metric of route will then be set to 16, which means the route is considered unreachable. Timeout Timer should be greater than Update Timer.	C	13
timer update <1-65535>	Sets the duration of the Update Timer (in seconds) to specify how often the Switch broadcasts its routing table and incorporates routing table information sent from other routers.	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

Table 210 rip Command Summary (continued)

COMMAND	DESCRIPTION	M	P
ip rip direction <Outgoing|Incoming|Both|None> version <v1|v2b|v2m>	Sets the RIP direction and version in this routing domain.	C	13
interface vlan <*vlan-id*>	Enters the configuration mode for this VLAN interface.	C	13
ipv6 rip	Enables IPv6 RIP on the VLAN interface.	C	13
no ipv6 rip	Disables IPv6 RIP on the VLAN interface.	C	13
ipv6 rip method <no-horizon|split-horizon|poison-reverse>	Specifies the mechanism used by the interface to prevent routing loops. no-horizon: to not use any mechanism on this interface to prevent routing loops. split-horizon; to prevent the interface from sending back the routing information received and learned from a neighbor. This also helps save bandwidth. poison-reverse: to have the interface set the metric of routes learned from a neighbor to 16 and send the routing information back. The neighbor will then delete the routes from its routing table.	c	13
ipv6 rip metric <*metric*>	Enters a number that approximates the cost for this link. The number need not be precise, but it must be between 1 and 15. In practice, 2 or 3 is usually a good number. *metric*: 1 – 15	c	13
show ip rip database	Displays the RIP configuration settings on the Switch.	E	3
show ipv6 rip	Shows whether IPv6 RIP is enabled on the Switch.	E	3
show ipv6 rip database	Displays the IPv6 RIP configuration settings on the Switch.	E	3

76.3 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
```

CHAPTER 77
RMON

77.1 RMON Overview

Similar to SNMP, RMON (Remote Network Monitor) allows you to gather and monitor network traffic.

Both SNMP and RMON use an agent, known as a probe, which are software processes running on network devices to collect information about network traffic and store it in a local MIB (Management Information Base). With SNMP, a network manager has to constantly poll the agent to obtain MIB information. The probe on the Switch communicates with the network manager through SNMP.

RMON groups contain detailed information about specific activities. The following table describes the four RMON groups that your Switch supports.

Table 211 Supported RMON Groups

GROUP	DESCRIPTION
Statistics	Records current network traffic information on a specified Ethernet port.
History	Records historical network traffic information on a specified Ethernet port for a certain time period.
Alarm	Provides alerts when configured alarm conditions are met.
Event	Defines event generation and resulting actions to be taken based on an alarm.

77.2 User Input Values

This section lists the common term definition appears in this chapter.

Table 212 rmon command user input values

USER INPUT	DESCRIPTION
event-index	This is an event's index number in the event table, between 1 and 65535.
alarm-index	This is an alarm's index number in the alarm table, between 1 and 65535.
etherstats-index	This is an entry's index number in the Ethernet statistics table, between 1 and 65535.
historycontrol-index	This is an entry's index number in the history control table, between 1 and 65535.
owner	This is a person's name who will handle the event, alarm, history control, or Ethernet statistics entry.
interface-id	This is a port that the Switch will poll for data.

77.3 Command Summary

The following section lists the commands for this feature.

Table 213 rmon Command Summary

COMMAND	DESCRIPTION	M	P
rmon alarm alarmtable <*alarm-index*> variable <*variable*> interval <*interval-integer*> sample-type <absolute|delta> startup-alarm <*startup-alarm*> rising-threshold <*rising-integer*> <*event-index*> falling-threshold <*falling-integer*> <*event-index*> [owner <*owner*>]	Sets an alarm that occurs when the sampled data exceeds the specified threshold. See Section 77.3.2 on page 308 for more information.	C	13
rmon event eventtable <*event-index*> [log] [trap <*community*>] [owner <*owner*>] [description <*description*>]	Sets the actions that the Switch takes when an associated alarm is generated by the Switch. log: set this to have the Switch record the logs for the alarm trap <*community*>: set this to have the Switch send a trap with the specified community. *description*: the description of the event.	C	13
rmon history historycontrol <*historycontrol-index*> buckets <1-65535> interval <1-3600> port-channel <*interface-id*> [owner <*owner*>]	Sets RMON history configuration settings. buckets <1-65535>: the number of data samplings the network manager requests the Switch to store. At the time of writing, the Switch can only store up to 200 data samplings although you can configure a bucket number higher than 200. interval <1-3600>: the time in seconds between data samplings.	C	13
rmon statistics etherstats <*etherstats-index*> port-channel <*interface-id*> [owner <*owner*>]	Sets to collect network traffic on the specified Ethernet port since the last time the Switch was reset.	C	13
no rmon alarm alarmtable <*alarm-index*>	Removes the specified alarm's settings.	C	13
no rmon event eventtable <*event-index*>	Removes the action's settings of the specified event.	C	13
no rmon history historycontrol <*historycontrol-index*>	Removes the RMON history configuration settings for the specified event.	C	13
no rmon statistics etherstats <*etherstats-index*>	Stops collecting network traffic for the specified event.	C	13
show rmon alarm alarmtable [*alarm-index*]	Displays all or the specified alarm settings.	E	3
show rmon event eventtable [*event-index*]	Displays all or the specified event settings.	E	3
show rmon history historycontrol [index <*historycontrol-index*>]	Displays all historical network traffic statistics or only the specified entry's.	E	3
show rmon history historycontrol port-channel <*interface-id*>	Displays historical network traffic statistics for the specified port.	E	3
show rmon statistics etherstats [index <*etherstats-index*>]	Displays all current network traffic statistics or only the specified entry's.	E	3
show rmon statistics etherstats port-channel <*interface-id*>	Displays current network traffic statistics for the specified port.	E	3

77.3.1 RMON Event Command Example

This example shows how to configure the Switch's action when an RMON event using the following settings:

- event index number: 2
- enable event logging and SNMP traps: Yes
- the trap's community: public
- who will handle this alarm: operator
- additional description for this event entry: test

This example also shows how to display the setting results.

```
ras# config
ras(config)# rmon event eventtable 2 log trap public owner operator description test
ras(config)# exit
ras# show rmon event eventtable 2
  Event 2 owned by operator is valid
    eventType: logandtrap
    eventCommunity: public
    eventDescription: test
```

77.3.2 RMON Alarm Command Example

Syntax:

rmon alarm alarmtable <*alarm-index*> variable <*variable*> interval <*interval-integer*> sample-type <absolute|delta> startup-alarm <*startup-alarm*> rising-threshold <*rising-integer*> <*event-index*> falling-threshold <*falling-integer*> <*event-index*> [owner <*owner*>]

where

1-65535	This is an alarm's index number in the alarm table.
variable	This is the variables whose data is sampled. The allowed options are: • [ifType.<port>] • [ifMtu.<port>] • [ifSpeed.<port>] • [ifAdminStatus.<port>] • [ifOperStatus.<port>] • [ifLastChange.<port>] • [ifInOctets.<port>] • [ifInUcastPkts.<port>] • [ifInNUcastPkts.<port>] • [ifInDiscards.<port>] • [ifInErrors.<port>] • [ifInUnknownProtos.<port>] • [ifOutOctets.<port>] • [ifOutUcastPkts.<port>] • [ifOutNUcastPkts.<port>] • [ifOutDiscards.<port>] • [ifOutErrors.<port>] • [ifOutQLen.<port>] • [sysMgmtCPUUsage.<index>] • [sysMemoryPoolUtil.<index>] • [<OID>]
interval-integer	This is the time interval (in seconds) between data samplings.
absolute|delta	This is the method of obtaining the sample value and calculating the value to be compared against the thresholds. • absolute – the sampling value of the selected variable will be compared directly with the thresholds. • delta – the last sampling value of the selected variable will be subtracted from the current sampling value first. Then use the difference to compare with the thresholds.
startup-alarm	Specify when the Switch should generate an alarm regarding to the rising and/or falling thresholds. • risingAlarm – the Switch generates an alarm if the sampling value (or calculated value) is greater than or equal to the rising threshold. • fallingAlarm – the Switch generates an alarm if the sampling value (or calculated value) is less than or equal to the falling threshold. • risingOrFallingAlarm – the Switch generates an alarm either when the sampling value (or calculated value) is greater than or equal to the rising threshold or when the sampling value (or calculated value) is less than or equal to the falling threshold.
rising-integer	Specify an integer for the rising threshold. When the value is greater or equal to this threshold, the Switch generates an alarm.
rising-event-index	Specify an event's index number (between 0 and 65535). The Switch will take the corresponding action of the selected event for the rising alarm. Set this to 0 if you do not want to take any action for the alarm.
falling-integer	Specify an integer for the falling threshold. When the value is smaller or equal to this threshold, the Switch generates an alarm.
falling-event-index	Specify an event's index number (between 0 and 65535). The Switch will take the corresponding action of the selected event for the falling alarm. Set this to 0 if you do not want to take any action for the alarm.
owner	Specify who should handle this alarm.

This example shows you how to configure an alarm using the following settings:

- alarm index number: 2
- variable: getting the number of error packets received on port 1
- how often to get a data sample: every 60 seconds
- sampling method: delta
- when to send an alarm: when the value is higher than the rising threshold
- the rising threshold: 50
- which event's action should be taken for the rising alarm: 2 (see Section 77.3.1 on page 308)
- the falling threshold: 0
- which event's action should be taken for the falling alarm: 0 (see Section 77.3.1 on page 308)
- who will handle this alarm: operator

This example also shows how to display the setting results.

```
ras# config
ras(config)# rmon alarm alarmtable 2 variable ifInErrors.1 interval 60 sample-type
delta startup-alarm rising rising-threshold 50 2 falling-threshold 0 2 owner operator
ras(config)# exit
ras# show rmon alarm alarmtable
  Alarm 2 owned by operator is valid
    alarmVariable: ifInErrors.1
    alarmInterval: 60
    alarmSampleType: delta
    alarmStartupAlarm: rising
    alarmRisingThreshold: 50
    alarmRisingEventIndex: 2
    alarmFallingThreshold: 0
    alarmFallingEventIndex: 0
    Last value monitored: 0
ras#
```

77.3.3 RMON Statistics Command Example

This example shows how to configure the settings to display current network traffic statistics using the following settings:

- the Ethernet statistics table entry's index number: 1
- collecting data samples from which port: 12

This example also shows how to display the data collection results.

```
ras# config
ras(config)# rmon statistics etherstats 1 port-channel 12
ras(config)# exit
ras# show rmon statistics etherstats index 1
  Statistics 1 owned by  is valid
    Monitor on interface port-channel 12
    etherStatsDropEvents: 0
    etherStatsOctets: 1576159
    etherStatsPkts: 19861
    etherStatsBroadcastPkts: 16721
    etherStatsMulticastPkts: 1453
    etherStatsCRCAlignErrors: 2
    etherStatsUndersizePkts: 0
    etherStatsOversizePkts: 0
    etherStatsFragments: 0
    etherStatsJabbers: 0
    etherStatsCollisions: 0
    Packet length distribution:
      64: 17952
      65-127: 666
      128-255: 671
      256-511: 509
      512-1023: 26
      1024-1518: 37
ras#
```

77.3.4 RMON History Command Example

This example shows how to configure the settings to display historical network traffic statistics using the following settings:

- the history control table entry's index number: 1
- how many data sampling data you want to store: 10
- time interval between data samplings: 10 seconds
- collecting data samples from which port: 12

This example also shows how to display the data collection results.

```
ras# config
ras(config)# rmon history historycontrol 1 buckets 10 interval 10 port-channel 12
ras(config)# exit
ras# show rmon history historycontrol index 1
  History control 1 owned by  is valid
    Monitors interface port-channel 12 every 10 sec.
    historyControlBucketsRequested: 10
    historyControlBucketsGranted: 10
    Monitored history 1:
      Monitored at 0 days 00h:08m:59s
      etherHistoryIntervalStart: 539
      etherHistoryDropEvents: 0
      etherHistoryOctets: 667217
      etherHistoryPkts: 7697
      etherHistoryBroadcastPkts: 5952
      etherHistoryMulticastPkts: 505
      etherHistoryCRCAlignErrors: 2
      etherHistoryUndersizePkts: 0
      etherHistoryOversizePkts: 0
      etherHistoryFragments: 0
      etherHistoryJabbers: 0
      etherHistoryCollisions: 0
      etherHistoryUtilization: 72
    Monitored history 2:
      Monitored at 0 days 00h:09m:08s
      etherHistoryIntervalStart: 548
      etherHistoryDropEvents: 0
      etherHistoryOctets: 673408
      etherHistoryPkts: 7759
      etherHistoryBroadcastPkts: 5978
      etherHistoryMulticastPkts: 519
      etherHistoryCRCAlignErrors: 2
      etherHistoryUndersizePkts: 0
      etherHistoryOversizePkts: 0
      etherHistoryFragments: 0
      etherHistoryJabbers: 0
      etherHistoryCollisions: 0
      etherHistoryUtilization: 0
ras#
```

CHAPTER 78
Running Configuration Commands

78.1 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.

Note: The Switch rejects configuration files with invalid or incomplete commands.

78.2 Command Summary

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

Table 214 running-config User-input Values

COMMAND	DESCRIPTION
attribute	Possible values: `active`, `name`, `speed-duplex`, `bpdu-control`, `flow-control`, `vlan1q`, `vlan1q-member`, `bandwidth-limit`, `vlan-stacking`, `port-security`, `broadcast-storm-control`, `mirroring`, `port-access-authenticator`, `queuing-method`, `spanning-tree`, `mrstp`, `protocol-based-vlan`, `port-based-vlan`, `mac-authentication`, `ethernet-oam`, `loopguard`, `arp-inspection`, `dhcp-snooping`.
port-list	A list of one or more ports, separated by commas with no spaces. The list may also contain ranges of ports signified by a hyphen. For example: 1,3,5–8,10.

The following section lists the commands for this feature.

Table 215 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 interface port-channel <*port-list*> | begin <*string*>	Displays the current configuration for the Switch or the specified ports, which start from a line with the specified string.	E	3
show running-config [interface port-channel <*port-list*>] | begin <*string1*> include <*string2*>	Displays the current configuration for the Switch or the specified ports, which start from a line with the first specified string and also contain the second specified string.	E	3
show running-config [interface port-channel <*port-list*>] | include <*string*>	Displays the current configuration for the Switch or the specified ports, which contain the specified string.	E	3
show running-config [interface port-channel <*port-list*>] | refresh	Displays the current configuration for the Switch or the specified ports, and updates every second until you press the [ESC] button.	E	3
show running-config help	Provides more information about the specified command.	E	3
show running-config page	Displays the current configuration file page by page.	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.	C	13
copy running-config custom-default	Saves the current configuration settings permanently to a customized default file on the Switch.	E	14
copy running-config help	Provides more information about the specified command.	C	13
copy running-config slot <*slot*> <*slot-list*>	Clones (copies) the attributes from the specified slot to other slots.	C	13
copy running-config slot <*slot*> <*slot-list*> [bandwidth-limit ...]	Copies the specified attributes from one slot to other slots.	C	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

Table 215 running-config Command Summary (continued)

COMMAND	DESCRIPTION	M	P
reload custom-default	Reboots the system and loads a saved customized default file on the Switch. Note: This will save the customized default configuration settings to both Configuration 1 and Configuration 2. Note: If you did not save a customized default file in the web configurator or CLI using copy running-config custom-default, then the factory default file is restored. You will then have to make all your configurations again on the Switch.	E	14
reload factory-default	Resets the Switch to the factory default settings, including default user name and password.	E	14
sync running-config	Uses the current configuration on the active management card to update the current configuration on the standby management card.	E	13

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

CHAPTER 79
Service Register

79.1 Service Register Overview

Some Switch models require a license to use certain services. The service register commands allow you to view which licenses are currently active on the Switch, and update license information from myZyxel. You can register your Switch and manage Switch licenses at www.myzyxel.com.

- To register your Switch, go to **www.myzyxel.com** > **Device Registration**. Enter your Switch's **MAC Address** and **Serial Number**.
- To register your license, go to **www.myzyxel.com** > **Service Registration**. Enter your License Key.

Note: Make sure you have Internet connectivity when registering your Switch and service license. Then use the `service-register update` command to activate the service license and update the license status (see Table 216 on page 317 for a complete description of the `service-register update` command). After activating the license, Internet connectivity is not required to use the license services.

Note: Licensed features are only available after you activate your license on the Switch. For Switches that support CLI configuration as additional license options, use the Web Configurator to activate the license. See the Switch User's Guide for how to activate your license through the Web Configurator.

79.2 Command Summary

The following section lists the commands for this feature.

Table 216 service-register Command Summary

COMMAND	DESCRIPTION	M	P
service-register update	Updates the licensing information for the Switch from myZyxel. If you have registered your Switch and license on myZyxel, the Switch will automatically activate the license after you use this command. Reboot your Switch to see the services. Note: To run this command, the Switch must be registered on myZyxel and connected to the Internet.	E	13
show service-register	Displays whether the Switch is registered at myZyxel, and the status of each available license. Licenses statuses: • **Not Licensed**: The license is not activated on the Switch. • **Licensed (activated after reboot):** The service license is registered to your Switch but you need to reboot your Switch to see the license services. • **Licensed**: The license is activated on the Switch.	E	3

79.3 Command Example

This example shows you how to activate licensed services on the Switch.

1 Register your Switch and license on *www.myZyxel.com*.

2 Update the Switch's licensing information from myZyxel. Use the show service-register command to check the updated license status.

```
sysname# service-register update
sysname# show service-register
  Device Registration Status : Registered
  License Token : ******3fff3

  Service Register Module Table :
          Service                              Status      Type   Expiration
  --------------  ---------------------------------  --------   ----------
  Advance Routing  Licensed (activated after reboot)  Standard          N/A
```

3 Reboot the Switch. Check your license status again. You should now be able to use the licensed services on your Switch.

```
sysname# show service-register
  Device Registration Status : Registered
  License Token : ******3fff3

  Service Register Module Table :
          Service    Status      Type  Expiration
  ---------------  --------  --------  ----------
  Advance Routing  Licensed  Standard         N/A
```

The following table describes the labels in this screen.

Table 217 show service-register

LABEL	DESCRIPTION
Device Registration Status	This displays whether the Switch is registered at myZyxel.
License Token	A license token is a unique electronic key that the Switch uses to get licenses. The token is created when the Switch is registered at myZyxel.
Service	This displays the name of a service that is available on the Switch.
Status	This field displays the service license status. **See Section Table 216 on page 317 for the status list.**
Type	**Trial** indicates a 30-day trial service license is currently registered on the Switch. **Standard** indicates a service license is registered at *www.myzyxel.com*. **N/A** is displayed if the service license is not registered.
Expiration	This field displays the amount of time remaining before your trial license expires. This displays **N/A** (no expiry) if a standard license is enabled. Note: The Switch will automatically reboot and reset to the factory-default settings after the trial license expires. You should activate a standard license on the Switch before the trial license expires to avoid erasing the current Switch configurations.

CHAPTER 80
sFlow

80.1 sFlow Overview

This chapter shows you how to configure sFlow to have the Switch monitor traffic in a network and send information to an sFlow collector for analysis.

sFlow (RFC 3176) is a standard technology for monitoring switched networks. An sFlow agent embedded on a switch or router gets sample data and packet statistics from traffic forwarded through its ports. The sFlow agent then creates sFlow data and sends it to an sFlow collector. The sFlow collector is a server that collects and analyzes sFlow datagram. An sFlow datagram includes packet header, input and output interface, sampling process parameters and forwarding information.

sFlow minimizes impact on CPU load of the Switch as it analyzes sample data only. sFlow can continuously monitor network traffic and create reports for network performance analysis and troubleshooting. For example, you can use it to know which IP address or which type of traffic caused network congestion.

80.2 Command Summary

The following section lists the commands for this feature.

Table 218 sflow Command Summary

COMMAND	DESCRIPTION	M	P
`interface port-channel <port-list>`	Enters config-interface mode for the specified ports.	C	13
`no sflow`	Disables sFlow on this port.	C	13
`no sflow collector <ip-address>`	Removes the specified collector IP address from the port.	C	13
`sflow`	Enables sFlow on this port. The Switch will monitor traffic on this port and generate and send sFlow datagram to the specified collector.	C	13
`sflow collector <ip-address> [poll-interval <20-120>] [sample-rate <256-65535>]`	Specifies a collector for this port. You can set a time interval (from 20 to 120 in seconds) the Switch waits before sending the sFlow datagram and packet counters for this port to the collector. You can also set a sample rate (N) from 256 to 65535. The Switch captures every one out of N packets for this port to create sFlow datagram.	C	13
`no sflow`	Disables the sFlow agent on the Switch.	C	13
`no sflow collector <ip-address>`	Removes an sFlow collector entry.	C	13
`sflow`	Enables the sFlow agent on the Switch.	C	13

Table 218 sflow Command Summary (continued)

COMMAND	DESCRIPTION	M	P
sflow collector <*ip-address*> [udp-port <*udp-port*>]	Configures an sFlow collector and the UDP port the Switch uses to send sFlow datagram to the collector. The default UDP port is 6343.	C	13
show sflow	Displays sFlow settings on the Switch.	E	3

80.3 Command Examples

This example enables the sFlow agent on the Switch and configures an sFlow collector with the IP address 10.1.1.58 and UDP port 6343. This example also enables sFlow on ports 1, 2, 3 and 4 and configures the same collector, sample rate and poll interval for these ports.

```
sysname(config)# sflow
sysname(config)# sflow collector 10.1.1.58 udp-port 6343
sysname(config)# interface port-channel 1,2,3,4
sysname(config-interface)# sflow
sysname(config-interface)# sflow collector 10.1.1.58 poll-interval 120
sample-rate 2500
sysname(config-interface)# exit
sysname(config)# exit
sysname# show sflow
  sFlow version: 5
  sFlow Global Information:
    sFlow Status: Active
    index  Collector Address  UDP port
    -----  -----------------  --------
      1         10.1.1.58     6343

  sFlow Port Information:
    Port  Active  Sample-rate  Poll-interval  Collector Address
    ----  ------  -----------  -------------  -----------------
     1     Yes         2500            120          10.1.1.58
     2     Yes         2500            120          10.1.1.58
     3     Yes         2500            120          10.1.1.58
     4     Yes         2500            120          10.1.1.58
     5      No         32768           120            0.0.0.0
     6      No         32768           120            0.0.0.0
     7      No         32768           120            0.0.0.0
....
```

CHAPTER 81
SNMP Server Commands

81.1 Command Summary

Use these commands to configure SNMP on the Switch.

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

Table 219 snmp-server User-input Values

COMMAND	DESCRIPTION
property	1 – 32 alphanumeric characters
options	aaa: authentication, authorization, accounting. interface: linkup, linkdown, autonegotiation, lldp, transceiver-ddm. ip: ping, traceroute. switch: stp, mactable, rmon. system: coldstart, warmstart, fanspeed, temperature, voltage, reset, timesync, loopguard, errdisable, poe.
port-list	A list of one or more ports, separated by commas with no spaces. The list may also contain ranges of ports signified by a hyphen. For example: 1,3,5–8,10.

The following section lists the commands for this feature.

Table 220 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 – 128 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 [cipher] <*property*>	Sets the get community. Only for SNMPv2c or lower. cipher: inform the Switch that the string after the word "cipher" is an encrypted secret. This is used in password encryption. To encrypt the password, use the password encryption command.	C	13

Table 220 snmp-server Command Summary (continued)

COMMAND	DESCRIPTION	M	P
snmp-server set-community [cipher] <*property*>	Sets the set community. Only for SNMPv2c or lower. cipher: inform the Switch that the string after the word "cipher" is an encrypted secret. This is used in password encryption. To encrypt the password, use the password encryption command.	C	13
snmp-server trap-community [cipher] <*property*>	Sets the trap community. Only for SNMPv2c or lower. cipher: inform the Switch that the string after the word "cipher" is an encrypted secret. This is used in password encryption. To encrypt the password, use the password encryption command.	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
snmp-server trap-destination <*ip*> enable traps <aaa|help|interface|ip|switch|system> [*options*]	Sets the types of SNMP traps that should be sent to the specified SNMP manager. *options*: enter the trap type you want to configure here, such as timesync, loopguard, errdisable, poe, loginrecord, linkup, linkdown, autonegotiation, lldp, transceiver-ddm, storm-control, zuld, authentication, authorization, accounting, ping, traceroute, stp, mactable, rmon, or classifier.	C	13
no snmp-server trap-destination <*ip*>	Deletes the specified SNMP manager.	C	13
interface port-channel <*port-list*>	Enters config-interface mode for the specified ports.	C	13
snmp trap [*options*]	Enables sending of SNMP traps on this port. The Switch sends the related traps received on this port to the SNMP manager. *options*: enter the trap type you want to configure here, such as loopguard, errdisable, poe, linkup, linkdown, autonegotiation, lldp, transceiver-ddm, storm-control, or zuld.	C	13
no snmp trap [*options*]	Disables sending of SNMP traps on this port. The Switch sends the related traps received on this port to the SNMP manager. *options*: enter the trap type you want to configure here, such as loopguard, errdisable, poe, linkup, linkdown, autonegotiation, lldp, transceiver-ddm, storm-control, or zuld.	C	13

Table 220 snmp-server Command Summary (continued)

COMMAND	DESCRIPTION	M	P
snmp-server username <*name*> sec-level <noauth|auth|priv> [auth <md5|sha> auth-password [cipher] <*password*>] | [priv <des|aes> priv-password [cipher] <*password*>] group <*group-name*>	Sets the authentication level for SNMP v3 user authentication. Optionally, specifies the authentication and encryption methods for communication with the SNMP manager. *name*: Enter the SNMP user name. noauth: Use the user name 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 privacy settings and encryption for SNMP messages sent by this user. This is the highest security level. auth-password: Set the authentication password for SNMP messages sent by this user. priv-password: Set the privacy settings password for SNMP messages sent by this user. The following are the password rules for auth-password and priv-password: (for Switch models that do not support Password Complexity) 1 – 32 alphanumeric characters except [?], [|], ['], ["] or [,]. (for Switch models that support Password Complexity) When Password Complexity is disabled: • 4 to 32 characters in length When Password Complexity is enabled: • 9 to 32 characters in length • Include at least three of these: numbers, uppercase letters, lowercase letters, and special characters (for example, 'Ea5yPas5W0rd') • Cannot match your login username • Cannot use the same character (case insensitive) or number three or more times in a row (for example, '777', 'AaA') • Cannot use four or more sequential keyboard characters (case insensitive) or numbers (for example, 'qWer', '1234'), and • Cannot use the present password again. Note: Not all Switch models support password complexity. Note: [?], [|], ['], ["], [,], [[ ], [ ]] and space are not allowed whether Password Complexity is enabled or disabled. See Table 179 on page 249 for more information on Password Complexity.	C	14

Table 220 snmp-server Command Summary (continued)

COMMAND	DESCRIPTION	M	P
(continued)	group-name: Set the View-based Access Control Model (VACM) group. Available group names are: *admin*: The user belongs to the admin group and has maximum access rights to the Switch. *readwrite*: The user can read and configure the Switch except for confidential options (such as user account and AAA configuration options.) *readonly*: The user can read but cannot make any configuration changes. cipher: inform the Switch that the string after the word "cipher" is an encrypted secret. This is used in password encryption. To encrypt the password, use the password encryption command. 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	14
no snmp-server username <*name*>	Removes the specified SNMP user's information.	C	14
show snmp-server [user]	Displays the SNMP information on the Switch. The **user** flag displays SNMP user information.	E	3

Table 221 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
snmp-server trap-destination <*ip*> enable traps ip <*options*>	Sends the specified IP traps to the specified manager.	C	13

Table 221 snmp-server trap-destination enable traps Command Summary (continued)

COMMAND	DESCRIPTION	M	P
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
snmp-server trap-destination <*ip*> enable traps system system-log	Sends the specified system trap to the specified manager when the number of log entries recorded in the system log table reaches 90%.	C	13

81.2 Command Examples

This example sets the Switch to not send the linkup and linkdown traps received on port 3 to the SNMP manager.

```
sysname# configure
sysname(config)# interface port-channel 3
sysname(config-interface)# no snmp trap linkup linkdown
```

This example shows you how to display the SNMP information on the Switch.

```
sysname# show snmp-server

[General Setting]
SNMP Version    : v2c
Get  Community  : public
Set  Community  : public
Trap Community  : public

[ Trap Destination ]
Index     Version    IP            Port  Username
-----      -------   ------------  ----  --------
    1      v2c       0.0.0.0       162
    2      v2c       0.0.0.0       162
    3      v2c       0.0.0.0       162
    4      v2c       0.0.0.0       162
```

This example shows you how to display all SNMP user information on the Switch.

```
sysname# show snmp-server user

[ User Information ]
Index   Name    SecurityLevel     GroupName
-----   ------  -------------     --------------
    1   admin   noauth            admin
```

This example shows you how to set up the SNMP user information on the Switch.

```
sysname# configure
sysname(config)# snmp-server username 1 sec-level auth auth md5 auth-
password 1234 priv des priv-password 2345 group admin
sysname(config)#
```

This example shows you how to display the snmp-server and snmp-server user information on the Switch.

```
sysname# show snmp-server user

  [ User Information ]
  Index  Name  SecurityLevel  Group
  -----  ----  -------------  -----
      1     1           auth  admin
```

This example shows you how to enable the system log trap on the Switch.

```
sysname# configure
sysname(config)# snmp-server trap-destination 192.168.1.1
sysname(config)# snmp-server trap-destination 192.168.1.1 enable traps
system system-log
sysname(config)#
```

CHAPTER 82
Stacking Commands

82.1 Stacking Overview

Stacking is directly connecting Switches to form a larger system that behaves as a single Switch or a virtual chassis with increased port density.

The ports of your Switch which are dedicated for Switch stacking vary depending on your Switch model. Please check the User's Guide for your Switch.

You can manage each Switch in the stack from a master Switch using its Web Configurator or console. Each Switch supports up to two stacking channels. Use the master Switch to assign a 'slot ID' for each 'linecard' non-master Switch. 'Slot' refers to a Switch in the 'virtual chassis' stack.

You can build a Switch stack using a ring or chain topology. In a ring topology, the last Switch is connected to the first.

Note: When you change modes, all configurations except user accounts, but including running configuration, config01 and config02 will be erased and the Switch will reboot with a new config01. Therefore, you should back up previous configurations if you want to reload them later.

Stacking will automatically choose a master Switch in a stack but you can overwrite that by actively forcing a Switch to become a master Switch using the `Stacking force-master` command. This master Switch will have the highest priority over all other stacked Switches even when they have same priority value.

If two or more Switches have `Stacking force-master` enabled, then the Switch will use `Stacking priority` to determine which is master. If they have the same `Stacking priority`, then the Switch with the longest up-time is selected. Uptime is measured in increments of 10 minutes. The Switch with the higher number of increments is selected. If they have the same uptime, then the Switch with the lowest MAC address will be the master.

This is the master election priority in a stack system:

1. `Stacking force-master`
2. Highest `Stacking priority`
3. Longest System Up Time
4. Lowest MAC Address

Note: Master election occurs when stacking / standalone mode changes or when a stacking port is temporarily disconnected in stacking mode.

Note: The stacking and no stacking commands are not supported in Cloud mode. To use these commands, go to the NCC (Nebula Cloud Center). See the NCC User's Guide for more information.

82.2 Command Summary

The following section lists the commands for this feature.

Table 222 stacking Command Summary

COMMAND	DESCRIPTION	M	P
show stacking	Shows all the Switch'es slot stacking status. This includes the **Slot Id**, **Type**, **Status**, **MAC address**, **Role**, **Stacking up time**, **Stacking Topology**, **Stacking Channel**, **Neighbor** (slot ID) and **Speed**.	E	3
show running-config	Shows current Switch configuration including stacking slot summary. Press [CTRL]+C to terminate the process.	E	3
show stacking slot	Shows stacking details for all stacking slots.	E	3
show stacking slot <*number*>	Shows stacking details for the specified slot.	E	3
show system-information	Shows Switch stacking mode.	E	3
stacking	Enables stacking when the Switch is in standalone mode. The Switch will automatically reboot with a new config01.	C	13
no stacking	Enables standalone when the Switch is in stacking mode. The Switch will automatically reboot with a new config01.	C	13
stacking priority <*1-63*>	Sets Switch stacking priority.	C	13
no stacking priority	Sets Switch stacking priority to default (32).	C	13
stacking force-master	Enables force master mode which makes this Switch the master in the stack.	C	13
no stacking force-master	Disables force master mode.	C	13
stacking slot-id <*current slot-id*> renumber auto	Sets selected slot to auto mode.	C	13
stacking slot-id <*current slot-id*> renumber <*new slot-id*>	Sets selected slot to new slot ID.	C	13
stacking slot-id freeze	Sets selected slot to have the Switch retain its slot ID after reboot.	C	13
reload stacking-default	Resets all configurations done since the change to stacking mode except user name and password back to the original settings.	E	13

Table 222 stacking Command Summary (continued)

COMMAND	DESCRIPTION	M	P
`stacking port <port-list> media-type <SFP+|DAC10G>`	Sets the media type of the SFP+ module that is attached to the stacking port. On the Switch that has a 10 Gigabit interface for stacking, such as the SFP+ slot, you can insert either an SFP+ transceiver or an SFP+ Direct Attach Copper (DAC). An SFP+ Direct Attach Copper (DAC) is an SFP+ housing that has no optical module but uses a fixed-length passive copper cable assembly, which reduces cost and power significantly.	C	13
`stacking port-mode <2-ports|4-ports>`	Select the number of stacking ports on the Switch that has 4 SFP+ ports for Switch stacking. Select **2-ports** mode to use the last 2 SFP+ ports for Switch stacking. This allows you to use the SFP+ slots 27 and 28 (XGS2220-30/-30HP/-30F) and SFP+ slots 51 and 52 (XGS2220-54/-54HP/-54FP) as uplink fiber optic ports. You can transmit data over long distances (over 100 kilometers) using fiber optic cables compared to copper cables (up to 100 meters only). Select **4-ports** mode to use the last 4 SFP+ ports for Switch stacking. Note: See Table 8 on page 13 for the product that supports this command.	C	13

82.3 Command Examples

Use `show system-information` to show current Switch stacking mode.

```
sysname# show system-information

Product Model           : XGS2220-30HP
System Name             : XGS2220-30HP
System Mode             : Standalone
System Contact          :
System Location         :
System up Time          :     0:58:37 (2cd30 ticks)
Ethernet Address        : 00:19:cb:00:00:02
Bootbase Version        : V1.00 | 06/13/2022
ZyNOS F/W Version       : V4.80(ABXO.3)b2 | 01/23/2024
Hardware Version        : V1.0
Config Boot Image       : 1
Current Boot Image      : 1
Current Configuration   : 1
RomRasSize              : 6550116
Serial Number           : S20230807xxxx
Register MAC Address    : 19:22:07:06:xx:xx
sysname#
```

Use the following procedure to create a stack:

1. Select a Switch to be the master. Change its mode to stacking mode. You will see a message asking you to confirm the change. Press [Y] to confirm and the Switch will reboot automatically using a new config01.

2. After reboot completes, the master LED will turn on.

3. Force the Switch to be master, configure stacking priority to a high value, such as 63 and set its slot ID to 1.

```
sysname# configure
sysname(config)# stacking
System will erase all configuration and reboot. Continue? [y/N]y
< reboot…….>

sysname(config)# stacking force-master
sysname(config)# stacking priority 63
sysname(config)# stacking slot-id 1 renumber 1
```

4. Change a second Switch to stacking mode and wait for it to finish rebooting automatically. This master LED will also turn on.

```
sysname# configure
sysname(config)# stacking
System will erase all configuration and reboot. Continue? [y/N]y
< reboot…….>
```

5. Connect the two Switches using the stacking ports for the Switch defined.

6. The second Switch master LED will then turn off, and its **Sys** LED will blink while it's initializing. Please wait until it stops blinking, indicating that it has joined the stack.

7. Repeat steps 4 to 6 to connect other Switches to the stack.

Use these commands to then see the stacking status of the stack, see details of the slots in the stack and see details of an individual slot.

```
sysname# show stacking
Slot Id          Type  Status        MAC address     Role Stacking up time
-------  ------------  ------  -----------------   ------ ---------------
     *1  XGS2220-30HP  active  00:19:cb:00:00:02   master          0:03:32
      2  XGS2220-54HP  active  00:19:cb:00:00:03   backup          0:02:22
      3    XGS2220-54  active  00:19:cb:00:00:04 linecard          0:02:22
      4

Stacking Topology:Chain
Slot Id    Stacking Channel 1  Stacking Channel 2
-------   ------------------- -------------------
    No.    Neighbor    Speed   Neighbor    Speed
-------   ---------  ------- ----------  -------
     *1       slot 2      10G          -        -
      2       slot 1      10G     slot 3      10G
      3            -        -     slot 2      10G
      4            -        -          -        -

sysname#
sysname# show stacking slot status
Slot          Name    Status      Up Time  Version(Running/Flash1/Flash2)
----  ------------  --------  -----------  ------------------------------
  *1  XGS2220-30HP    active      0:03:30  V4.80(ABXO.3)b2 | 01/23/2024
                                           V4.80(ABXO.3)b2 | 01/23/2024
                                           V4.80(ABXO.3)b2 | 01/23/2024
   2  XGS2220-54HP    active      0:03:30  V4.80(ABXQ.3)b2 | 01/23/2024
                                           V4.80(ABXQ.3)b2 | 01/23/2024
                                           V4.80(ABXQ.3)b2 | 01/23/2024
   3    XGS2220-54    active      0:03:29  V4.80(ABXP.3)b2 | 01/23/2024
                                           V4.80(ABXP.3)b2 | 01/23/2024
                                           V4.80(ABXP.3)b2 | 01/23/2024
   4               inactive

sysname#
sysname# show stacking slot 1
  Stacking Slot 1 Information
         Stacking                      : active
         Role                          : master
         Force Master Mode             : active
         Priority                      : 32
         Slot ID after reboot          : 1
         Stacking Status               : active
         Master Capable                : auto
         Stacking MAC Address          : 00:19:cb:00:00:02
         Stacking port mode            : 4-ports
         Stacking-channel 1            : up
         Stacking-channel 2            : down
         System Up Time                :     0:20:30
         Stacking Up Time              :     0:19:41
         ZyNOS Version
                Running                : V4.80(ABXO.3)b2 | 01/23/2024
                Flash 1                : V4.80(ABXO.3)b2 | 01/23/2024
                Flash 2                : V4.80(ABXO.3)b2 | 01/23/2024
sysname#
```

Use these commands to see the stacking mode on a Switch.

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

  Current configuration:

; Product Name = XGS2220-30HP
; Firmware Version = V4.80(ABXO.3)b2 | 01/23/2024
; Stacking Port Mode = 4-ports
;; slot 1 type XGS2220-30HP
;; slot 2 type XGS2220-54HP
;; slot 3 type XGS2220-54
no service-control snmp
stacking force-master
vlan 1
  name 1
  fixed 1/1-1/26, 2/1-2/50, 3/1-3/50
  forbidden ""
  untagged 1/1-1/26, 2/1-2/50, 3/1-3/50
  ip address 192.168.1.1 255.255.255.0
exit
interface route-domain 192.168.1.1/24
exit
interface vlan 1
  ipv6
  ipv6 address dhcp client ia-na
exit
timesync server 1.pool.ntp.org
timesync ntp
pwr mode consumption

sysname# show system-information

Product Model           : XGS2220-30HP
System Name             : XGS2220
System Mode             : Stacking
System Contact          :
System Location         :
System up Time          :     0:03:38 (35677 ticks)
Ethernet Address        : 00:19:cb:00:00:02
Bootbase Version        : V1.00 | 06/13/2022
ZyNOS F/W Version       : V4.80(ABXO.3)b2 | 01/23/2024
Hardware Version        : V1.17
Config Boot Image       : 1
Current Boot Image      : 1
Current Configuration   : 1
RomRasSize              : 6550116
Serial Number           : S182L4808xxxx
Register MAC Address    : bc:99:11:cb:a2:xx

sysname#
```

CHAPTER 83
STP and RSTP Commands

83.1 STP and RSTP Overview

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 55 on page 216 and Chapter 56 on page 219 for more information on MRSTP and MSTP commands respectively. See also Chapter 48 on page 199 for information on loopguard commands.

Auto Path Cost

The Auto Path Cost feature allows you to have the Switch automatically set the path cost for each port according to their link speeds. The Switch uses the path costs to determine the best path to the root bridge in a spanning tree. There are three auto path-cost modes that support different path cost lengths:

- Short (16-bit)
- Long (32-bit)
- User-defined (32-bit).

Choose the auto path-cost mode (see Table 227 on page 335) according to the device average link speeds in the STP network.

If most of your devices support high link speed, you should select Long or User-defined mode. The path cost of link speed slower than 10 Mbps can be set to 2000000 (long) / 200000000 (user-defined), and the path cost of link speed faster than 10 Gbps can be set to 200. This way, the path costs can better reflect actual link speeds with a wider range (32 bits) of path cost values. If the link speeds within the system are averagely smaller than 1 Gbps, you should select Short mode since Short mode have path cost values more detailed defined for link speeds under 1 Gbps.

The auto path cost values are described in the following tables.

The Switch defines the following Short mode path costs.

Table 223 Auto Path Cost Mode: Short

LINK SPEED	AUTO PATH COST VALUE
Up to 4 Mbps	250
Up to 10 Mbps	100

Table 223 Auto Path Cost Mode: Short (continued)

LINK SPEED	AUTO PATH COST VALUE
Up to 16 Mbps	62
Up to 100 Mbps	19
Up to 1 Gbps	4
Up to 10 Gbps	2
More than 10 Gbps	1

The Switch defines the following Long mode path costs.

Table 224 Auto Path Cost Mode: Long

LINK SPEED	AUTO PATH COST VALUE
Up to 10 Mbps	2000000
Up to 100 Mbps	200000
Up to 1 Gbps	20000
Up to 2.5 Gbps	8000
Up to 5 Gbps	4000
Up to 10 Gbps	2000
Up to 25 Gbps	800
Up to 100 Gbps	200

If you do not configure the auto path cost values for User-defined mode, the Switch will use the following default values.

Table 225 Auto Path Cost Mode: User-defined

LINK SPEED	AUTO PATH COST VALUE
Up to 10 Mbps	2000000
Up to 100 Mbps	200000
Up to 1 Gbps	20000
Up to 2.5 Gbps	8000
Up to 5 Gbps	4000
Up to 10 Gbps	2000
Up to 25 Gbps	800
Up to 100 Gbps	200

83.2 Command Summary

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

Table 226 Interface Command Values

COMMAND	DESCRIPTION
port-list	A list of one or more ports, separated by commas with no spaces. The list may also contain ranges of ports signified by a hyphen. For example: 1,3,5–8,10.

The following section lists the commands for this feature.

Table 227 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 auto-path-cost mode <short|long|user-defined>`	Sets the auto path cost mode. You can set the path cost of a link to '0' for either RSTP, MSTP, or MRSTP. For example: `spanning-tree <port-list> path-cost 0`. The Switch will use the auto path costs (depending on the auto path cost mode you set) as the link's path cost. See Table 223 on page 333 for the auto path cost values of each mode. `short`: The Switch uses 16-bit auto path costs. `long`: The Switch uses 32-bit auto path costs. `user-defined`: The Switch uses 32-bit auto path costs you define. Note: It is recommended to use the same auto path-cost mode on all switches within the spanning tree network system.	C	13
`spanning-tree auto-path-cost user-values <10M|100M|1G|2.5G|5G|10G> <1-200000000>`	Sets a user-defined auto path cost value for each link speed.	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

Table 227 spanning-tree Command Summary (continued)

COMMAND	DESCRIPTION	M	P
`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> edge-port`	Sets the specified ports as edge ports. This allows the port to transition to a forwarding state immediately without having to go through the listening and learning states. Note: An edge port becomes a non-edge port as soon as it receives a Bridge Protocol Data Units (BPDU).	C	13
`no spanning-tree <port-list> edge-port`	Sets the listed ports as non-edge ports.	C	13
`spanning-tree <port-list> path-cost <0–200000000>`	Specifies the cost of transmitting a frame to a LAN through the ports. It is assigned according to the speed of the bridge. Note: You can set the value to '0', the Switch will use the auto path cost you set using the `auto-path-cost` command. See Section 83.1 on page 333 for more information.	C	13
`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 <port-list> rootguard`	Enables root guard on the specified port in order to prevent the switches attached to the port from becoming the root bridge.	C	13
`no spanning-tree <port-list> rootguard`	Disables root guard on a port.	C	13
`spanning-tree help`	Provides more information about the specified command.	C	13

83.3 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 228 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.

Table 228 show spanning-tree config (continued)

LABEL	DESCRIPTION
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).

In this example, we enable RSTP on ports 21 – 24. Port 24 is connected to the host while ports 21 – 23 are connected to another switch.

```
sysname(config)# configure
sysname(config)# spanning-tree
sysname(config)# spanning-tree 21-24
sysname(config)# no spanning-tree 21-23 edge-port
```

The following example enables RSTP on ports 1–3. In this example, we want to use the User-defined auto path-cost mode, and set ports 1-3 to use the auto path costs we define.

1 Use the following commands to set the auto path-cost mode to User-defined mode. Here we set the path costs to 10000/1000/10 respectively for link speed of 10 M/100 M/5 G.

```
sysname# configure
sysname(config)# spanning-tree
sysname(config)# spanning-tree path-cost mode user-defined
sysname(config)# spanning-tree path-cost user-values 10M 10000 100M 1000 5G
10
```

2 Use the following commands to enable RSTP on ports 1–3, and set ports 1–3 to use auto path costs.

```
sysname# configure
sysname(config)# spanning-tree
sysname(config)# spanning-tree 1-3
sysname(config)# spanning-tree 1-3 path-cost 0
sysname(config)#
```

You can use the show spanning-tree command to display the current spanning tree configuration and examine your settings. The following shows a part of the result. The Switch automatically set the path cost of port 1 (link speed: 5 G) to 10, as we defined.

```
sysname(config)# exit
sysname# show spanning-tree
Port [1] Info:
    (a)Uptime:                  2891    (seconds)
    (b)State:                   FORWARDING
    (c)PortID:                  0x8014
    (d)PathCost:                10
    (e)DesignatedRoot:          8000-bc9999999999
    (f)DesignatedCost:          0
    (g)DesignatedBridge:        8000-bc9999999999
    (h)DesignatedPort:          0x8014
    (i)TopoChangeAck:           False
    (j)adminEdgePort:           False
    (k)operEdgePort:            False
    (m)MAC_Operational:         True
    (n)adminPointToPointMAC:    AUTO
    (o)operPointToPointMAC:     True
    rx_cfg_bpdu[   0]   rx_tcn_bpdu[   0]       rx_rstp_bpdu[   0]
...
sysname(config)#
```

CHAPTER 84
SSH Commands

84.1 Command Summary

Use these commands to configure SSH on the Switch.

The following section lists the commands for this feature.

Table 229 ssh Command Summary

COMMAND	DESCRIPTION	M	P
`show ssh`	Displays general SSH settings.	E	3
`show ssh session`	Displays current SSH sessions.	E	3
`show ssh known-hosts`	Displays known SSH computers information.	E	3
`ssh known-hosts <host-ip> <1024|ssh-rsa|ssh-dsa> <key>`	Adds a remote computer to which the Switch can access using SSH service.	C	13
`no ssh known-hosts <host-ip>`	Removes the specified remote computer from the list of all known computers.	C	13
`no ssh known-hosts <host-ip> <1024|ssh-rsa|ssh-dsa>`	Removes the specified remote computers 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
`show ssh authorized-keys`	Displays the actual encryption key's text string (up to 64 characters). Note: See Table 8 on page 13 for the product that supports this command.	E	14
`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
`import ssh <username> authorized-keys <key-string>`	Saves the authorized key file you want to import from your computer to the Switch. Note: See Table 8 on page 13 for the product that supports this command.	E	14
`clear ssh authorized-keys`	Removes the authorized key file from the Switch. The computer cannot authenticate without entering a password using an SSH connection. Note: See Table 8 on page 13 for the product that supports this command.	E	14

Table 229 ssh Command Summary (continued)

COMMAND	DESCRIPTION	M	P
clear ssh known-hosts	Removes all known computers which can access the Switch using SSH service. Note: See Table 8 on page 13 for the product that supports this command.	E	14
ssh regen-key rsa	Regenerates the Switch's default host key.	C	14

84.2 Command Examples

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

```
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 actual encryption key's text string (up to 64 characters).

```
sysname# show ssh authorized-keys
    ssh-rsa xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
UserA@ClientA
sysname#
```

This example saves the authorized key file you want to import from your computer to the Switch.

```
sysname# import ssh admin authorized-keys “ssh-rsa
dsafnjsdlkjgwxaxzasfsdkjhgfdshgdsj UserA@UbuntuClient”.

Import Successfully.

sysname#
```

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 230 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.

CHAPTER 85
Static Multicast Commands

85.1 Static Multicast Overview

Use these commands to set up static Multicast forwarding rules based on Multicast MAC addresses or Multicast IPv4 addresses. A Multicast MAC/IP address uniquely identifies a Multicast group in your network. The Switch forwards Multicast frames/packets of a Multicast group to specific ports within a VLAN based on the rules you set. For Layer 2 Multicast frames, the Switch forwards the frames based on the static Multicast forwarding by MAC rules you set. For Layer 3 Multicast packets, the Switch forwards the frames based on the static Multicast forwarding by IP rules you set.

If a Multicast group has no members, the Switch will either flood the Multicast frames to all ports (default) or drop them. Static (manual) Multicast forwarding allows you (the administrator) to forward Multicast frames to a member without the member having to join the group first. Use the `router igmp unknown-multicast-frame` command (see Table 94 on page 121) to configure which to do with unknown Multicast frames.

85.2 Command Summary

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

Table 231 Interface Command Values

COMMAND	DESCRIPTION
port-list	A list of one or more ports, separated by commas with no spaces. The list may also contain ranges of ports signified by a hyphen. For example: 1,3,5–8,10.

The following section lists the commands for this feature.

Table 232 multicast-forward Command Summary

COMMAND	DESCRIPTION	M	P
show mac address-table multicast	Displays the Multicast MAC address table.	E	3
multicast-forward name <*name*> mac <*mac-addr*> vlan <*vlan-id*> inactive	Creates a new static Multicast forwarding by MAC rule. The rule name can be up to 32 printable ASCII characters. Use the no multicast-forward mac <mac-addr> vlan <vlan-id> inactive command to activate a rule. *mac-addr*: Enter a Multicast MAC address which identifies the Multicast group. The last binary bit of the first octet pair in a Multicast MAC address must be 1. For example, the first octet pair 00000001 is 01 and 00000011 is 03 in hexadecimal, so 01:00:5e:00:00:0A and 03:00:5e:00:00:27 are valid Multicast MAC addresses. *vlan-id*: A VLAN identification number. Note: Static Multicast addresses do not age out.	C	13
multicast-forward name <*name*> mac <*mac-addr*> vlan <*vlan-id*> interface port-channel <*port-list*>	Creates and associates a static Multicast forwarding by MAC rule with specified ports within a specified VLAN.	C	13
multicast-forward-by-ip name <*name*> ip <*ip-addr*> vlan <*vlan-id*> interface port-channel <*port-list*>	Creates and associates a static Multicast forwarding by IP rule with specified ports within a specified VLAN. *ip-addr*: Enter a Multicast IP address (Class D IP address) which identifies the Multicast group. You can only use Class D IP addresses. Class D IP addresses are IP addresses reserved for Multicasting. Each Class D IP address uniquely identifies a Multicast group. The range is from 224.0.0.0 to 239.255.255.255.	C	13
no multicast-forward mac <*mac-addr*> vlan <*vlan-id*>	Removes a specified static Multicast forwarding by MAC rule.	C	13
no multicast-forward-by-ip ip <*ip-addr*> vlan <*vlan-id*>	Removes a specified static Multicast forwarding by IP rule.	C	13
no multicast-forward mac <*mac-addr*> vlan <*vlan-id*> inactive	Activates a specified static Multicast forwarding by MAC rule.	C	13

85.3 Command Examples

This example shows the current Multicast table. The **Type** field displays **User** for rules that were manually added through static Multicast forwarding or displays **System** for rules the Switch has automatically learned through IGMP snooping.

```
sysname# show mac address-table multicast
  MAC Address       VLAN ID   Type      Port
01:02:03:04:05:06   1         User      1-2
01:02:03:04:05:07   2         User      2-3
01:02:03:04:05:08   3         User      1-12
01:02:03:04:05:09   4         User      9-12
01:a0:c5:aa:aa:aa   1         System    1-12
```

This example removes a static Multicast forwarding rule with Multicast MAC address (01:00:5e:06:01:46) which belongs to VLAN 1.

```
sysname# no multicast-forward mac 01:00:5e:06:01:46 vlan 1
```

This example creates a static Multicast forwarding rule. The rule forwards frames with destination MAC address 01:00:5e:00:00:06 to ports 10~12 in VLAN 1.

```
sysname# configure
sysname(config)# multicast-forward name AAA mac 01:00:5e:00:00:06 vlan 1
interface port-channel 10-12
```

CHAPTER 86
Static Route Commands

86.1 Static Route Overview

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 through 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 through gateways other than those defined as the default gateway.

Route Failover

The Switch supports route failover for static routes. You can enable route failover and set up more than one route link with the same destination address as backup routes. The Switch sends ping requests to the link's next hop to determine if a route link has a reachable next hop. The Switch will check if the links have a reachable next hop, then sort these links by their metrics (the number of hops to the final destination). The link with the lowest metric will be the primary link. The link with the next lowest metric will be the secondary link. If route failover is enabled, when a primary route link is down, the Switch will use the secondary link. The secondary link will be set to down when the primary link is valid again. There will only be one active link at a time.

86.2 Command Summary

The following section lists the commands for this feature.

Table 233 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

Table 233 ip route Command Summary (continued)

COMMAND	DESCRIPTION	M	P
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. Note: You can set more than one route with the same destination as backup routes if you enable route failover using the ip route failover command.	C	13
ip route failover	Enables route failover for static routes.	C	13
no ip route <*ip*> <*mask*>	Removes a specified static route.	C	13
no ip route <*ip*> <*mask*> <*next-hop-ip*>	Removes a specified static route.	C	13
no ip route <*ip*> <*mask*> inactive	Enables a specified static route.	C	13
no ip route <*ip*> <*mask*> <*next-hop-ip*> inactive	Enables a specified static route.	C	13
no ip route failover	Disables route failover for static routes. If you disable route failover, the Switch will keep all the routes you set, but only use the primary route.	C	13

86.3 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 234 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
```

CHAPTER 87 Subnet-based VLAN Commands

87.1 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 71 on page 287 for protocol-based VLAN commands and Chapter 96 on page 371 for VLAN commands.

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

87.2 Command Summary

The following section lists the commands for this feature.

Table 235 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

Table 235 subnet-based-vlan Command Summary (continued)

COMMAND	DESCRIPTION	M	P
no subnet-based-vlan	Disables subnet-based VLAN on the Switch.	C	13
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 VLANs.	C	13

87.3 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
```

CHAPTER 88
Syslog Commands

88.1 Command Summary

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

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

Table 236 syslog User-input Values

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

The following section lists the commands for this feature.

Table 237 syslog Command Summary

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

Table 238 syslog server Command Summary

COMMAND	DESCRIPTION	M	P
`syslog server <ip-address> level <level> [udp <socket-number>]`	Sets the IPv4 or IPv6 address of the syslog server and the severity level. The default UDP port is 514. *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 239 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
`syslog type commands privilege <0-14>`	Sets a command privilege level. The Switch will only generate logs for commands that have a privilege level greater than or equal to the specified privilege level.	C	13
`no syslog type <type>`	Disables syslog logging for the specified log type.	C	13

PART V
Reference T-Z

CHAPTER 89
TACACS+ Commands

89.1 Command Summary

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

The following section lists the commands for this feature.

Table 240 tacacs-server Command Summary

COMMAND	DESCRIPTION	M	P
show tacacs-server	Displays TACACS+ server settings.	E	3
tacacs-server host <*index*> <*ip*> [auth-port <*socket-number*>] [key <*key-string*> | key-cipher <encrypted-*key-string*>]	Specifies the IP address of the specified TACACS+ server. The TCP port number and shared secret are optional. *index*: 1 or 2. cipher: inform the Switch that the string after the word "cipher" is an encrypted secret. This is only used when the Switch is restoring the encrypted key from a configuration file. To encrypt the key, use the aaa server key encryption command. *key-string*: 1 – 32 alphanumeric characters except [?], [|], ['], ["], [space], or [,].	C	14
tacacs-server mode <index-priority|round-robin>	Specifies how the Switch decides which TACACS server to select if you configure multiple servers. index-priority: The Switch tries to authenticate with the first configured TACACS server. If the TACACS server does not respond, then the Switch tries to authenticate with the second TACACS server. round-robin: The Switch alternates between TACACS servers that it sends authentication requests to.	C	14
tacacs-server timeout <1-1000>	Specify the amount of time (in seconds) that the Switch waits for an authentication request response from the TACACS server. 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	14
no tacacs-server <*index*>	Resets the specified TACACS+ server to its default values.	C	14

Table 241 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

Table 241 tacacs-accounting Command Summary (continued)

COMMAND	DESCRIPTION	M	P
tacacs-accounting host <*index*> <*ip*> [acct-port <*socket-number*>] [key <*key-string*> | key-cipher <encrypted-*key-string*>]	Specifies the IP address of the specified TACACS+ accounting server. The port number and key of the external TACACS+ accounting server are optional. *index*: 1 or 2. cipher: inform the Switch that the string after the word "cipher" is an encrypted secret. This is only used when the Switch is restoring the encrypted key from a configuration file. To encrypt the key, use the aaa server key encryption command. *key-string*: 1 – 32 alphanumeric characters except [?], [|], ['], ["], [space], or [,].	C	13
no tacacs-accounting <*index*>	Disables TACACS+ accounting on the specified server.	C	13

CHAPTER 90
Tech Support Commands

90.1 Tech-Support Overview

The Tech-Support feature is a log Enhancement tool that logs useful information such as CPU utilization history, memory and Mbuf (Memory Buffer) information and crash reports for issue analysis that is collected by customer support should you have difficulty with your Switch. The Tech Support Command Line Interface eases your effort in obtaining these reports. Type `show tech-support` command to see the log reports.

90.2 Command Summary

The following section lists the commands for this feature.

Table 242 Tech Support Command Summary

COMMAND	DESCRIPTION	M	P
`show tech-support`	Shows all tech-support log reports.	E	13
`show tech-support cpu`	Shows CPU history log. The log report holds 7 days of CPU log data and is stored in volatile memory (RAM). The data is lost if the Switch is turned off or in event of power outage. After 7 days, the logs wrap around and new log messages replace the earliest ones.	E	13
`show tech-support memory`	Shows the last memory session log before the Switch is turned off or in event of power outage.	E	13
`show tech-support mbuf`	Shows the mbuf that is higher than the threshold. Default mbuf value is 50.	E	13
`show tech-support crash`	Shows the last crash log before the Switch is turned off or in event of power outage.	E	13

Table 242 Tech Support Command Summary (continued)

COMMAND	DESCRIPTION	M	P
`tech-support cpu <threshold> keep <time>`	Sets the CPU threshold and time value for CPU utilization event logging. When CPU utilization is greater than or equal to the specified threshold for the specified time period, the Switch creates an event log message. *cpu threshold*: CPU utilization, as a percentage. The valid range is 50 – 100, and the default is 80. *time*: Time range, in seconds. The valid range is 5 – 60, and the default is 5.	C	13
`tech-support mbuf <threshold>`	Sets the Memory Buffer threshold for mbuf report. *mbuf threshold*: a number between and including 50 to 100.	C	13

90.3 Command Examples

This example sets the mbuf threshold to 60%, checks the mbuf threshold setting and generates the mbuf log report.

```
sysname# config <cr>
sysname(config)#
sysname(config)# tech-support mbuf 60 <cr>
sysname(config)#
sysname(config)# exit <cr>
sysname# show run <cr>
sysname# Building configuration...
  Current configuration:
tech-support mbuf 60
sysname#
sysname# show tech-support mbuf
Tech-support version: v1.1
Time :  1011:22:24 ==========   show system-information
================= msclock :-654018103

Product Model           : XGS2220-54FP
System Name             : XGS2220
System Mode             : Standalone
System Contact          :
System Location         :
System up Time          :  1011:22:24 (d90479ca ticks)
Ethernet Address        : b8:ec:a3:ff:f2:a2
Bootbase Version        : V1.00 | 06/13/2022
ZyNOS F/W Version       : V4.80(ACCE.0) | 08/03/2022
Hardware Version        : V1.0
Config Boot Image       : 1
Current Boot Image      : 1
Current Configuration   : 1
RomRasSize              : 6440206
Serial Number           : S222L18090003
Register MAC Address    : b8:ec:a3:ff:f2:a2

Time :  1011:22:24 ==========   show time
================= msclock :-654018001

Current Time  09:44:18 (UTC+00:00)
Current Date  2022-10-27

Time :  1011:22:24 ==========   mbuf log
================= msclock :-654017890

time: 1970-1-1 0:0:0
Pool ID: 0, Type: 0, used/max cnt: 0/400

Pool ID: 0, Type: 1, used/max cnt: 0/400

Pool ID: 0, Type: 2, used/max cnt: 0/400

Pool ID: 1, Type: 0, used/max cnt: 0/256

Pool ID: 1, Type: 1, used/max cnt: 0/2048

Pool ID: 1, Type: 2, used/max cnt: 0/2048
```

This example sets the CPU threshold to 80% and time to 5 seconds, and then uses the command show logging to display the log.

```
sysname# config <cr>
sysname(config)#
sysname(config)# tech-support cpu 80 keep 5 <cr>
sysname (config)#
sysname(config)# exit <cr>
sysname#
sysname# show logging
       1 2020-01-01T03:11:01Z IN authentication: SSH user admin login [IP address =
172.21.40.29]
     2 2020-01-01T03:02:53Z IN authentication: SSH user admin login [IP address =
172.21.40.29]
     3 2020-01-01T01:17:17Z IN authentication: HTTP(s) user admin login [IP address
= 172.21.40.27]
     4 2020-01-01T01:17:12Z IN authentication: HTTP(s) user admin logout [IP address
= 172.21.40.27]
     5 2020-01-01T01:16:40Z IN authentication: HTTP(s) user admin login [IP address
= 172.21.40.27]
     6 2020-01-01T01:15:20Z IN authentication: HTTP(s) user admin logout [IP address
= 192.168.0.13]
     7 2020-01-01T01:14:54Z IN authentication: HTTP(s) user admin login [IP address
= 192.168.0.13]
     8 2020-01-01T00:01:33Z ER system: Gets the time and date from a time server
failed
```

CHAPTER 91
TFTP Commands

91.1 Command Summary

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

The following section lists the commands for this feature.

Table 243 tftp Command Summary

COMMAND	DESCRIPTION	M	P
`copy tftp flash <ip> <remote-file>`	Restores firmware through TFTP.	E	13
`copy tftp config <index> <ip> <remote-file>`	Restores configuration with the specified filename from the specified TFTP server to the specified configuration file on the Switch. *index*: 1 or 2 Use `reload config <1|2>` to restart the Switch and use the restored configuration. Note: This overwrites the configuration on the Switch with the file from the TFTP server.	E	13
`copy tftp config merge <index> <ip> <remote-file>`	Merges configuration with the specified filename from the specified TFTP server with the specified configuration file on the Switch. *index*: 1 or 2 Use `reload config <1|2>` to restart the Switch and use the restored configuration. Note: This joins the configuration on the Switch with the one on the TFTP server, keeping the original configuration file and simply adding those parts that are different.	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

CHAPTER 92
Time Range Commands

92.1 Time Range Overview

You can set a time range for time-oriented features such as Classifier ACL (Access Control List) rule which categorizes data packets into different network traffic flows. The advantage of the time range feature is that it allows you to schedule the active time of configurations. Time range can be configured in two ways – Absolute and Periodic. Absolute is a fixed time range with a start and end time. Periodic is recurrence of a time range and does not have an end time.

92.2 Command Summary

The following section lists the commands for this feature.

Table 244 time-range Command Summary

COMMAND	DESCRIPTION	M	P
show time-range <*name*>	Displays details on the named rule.	C	3
time-range <*name*> [absolute start <hh:mm> <1-31> <jan-dec> <1970-2037> end <hh:mm> <1-31> <jan-dec> <1970-2037>]	Creates an absolute time-range rule that has a set start and end time and date (absolute). name is the name of the time-range rule.	E	13
time-range <*name*> [periodic <[<monday|tuesday|wednesday|thursday|friday|saturday|sunday><hh:mm> to monday|tuesday|wednesday|thursday|friday|saturday|sunday> <hh:mm>][<[monday][tuesday][wednesday][thursday][friday][saturday][sunday]|daily|weekdays|weekend> <hh:mm> to <hh:mm>]	Creates a periodic time-range rule that recurs at the specified time and day (periodic). name is the name of the time-range rule.	E	13
no time-range <*name*>	Removes the specified time-range rule.	C	13

92.3 Command Examples

The following are some examples of using the time-range commands.

```
sysname#
sysname# configure
sysname(config)# time-range work absolute start 08:00 1 jan 2015 end
17:30 31 dec 2015
sysname(config)# exit
sysname# show time-range work
  Time range work:
  Absolute start 08:00 1 January 2015 end 17:30 31 December 2015

sysname(config)# time-range work2 periodic monday 08:00 to friday 17:30
monday 08:00 to friday 17:30
sysname(config)# exit
sysname# show time-range work2
  Time range work2:
  Periodic Monday 08:00 to Friday 17:30
sysname#
```

CHAPTER 93
Traceroute Commands

93.1 Traceroute Overview

Traceroute is a tool to display the path a packet takes between two endpoints.

93.2 Command Summary

The following section lists the commands for this feature.

Table 245 traceroute Command Summary

COMMAND	DESCRIPTION	M	P
`traceroute <ip|host-name> [vlan <vlan-id>] [ttl <1-255>] [wait <1-60>] [queries <1-10>]`	Displays the path a packet takes to the specified Ethernet device with an IPv4 address. `vlan <vlan-id>`: Specifies the VLAN ID to which the Ethernet device belongs. `ttl <1-255>`: Specifies the Time To Live (TTL) period. This is to set the maximum number of the hops (routers) a packet can travel through. `wait <1-60>`: Specifies the time period to wait for a response to a probe before running another traceroute. `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
`traceroute6 <ipv6-addr|host-name> <[ttl <1-255>] [wait <1-60>] [queries <1-10> ]>`	Displays the route a packet takes to the specified Ethernet device with an IPv6 address. `vlan <vlan-id>`: Specifies the VLAN ID to which the Ethernet device belongs. `ttl <1-255>`: Specifies the Time To Live (TTL) period. This is to set the maximum number of the hops (routers) a packet can travel through. `wait <1-60>`: Specifies the time period to wait for a response to a probe before running another traceroute. `queries <1-10>`: Specifies how many times the Switch performs the traceroute function.	E	0
`traceroute6 help`	Provides more information about the specified command.	E	0

CHAPTER 94
Trunk Commands

94.1 Trunking Overview

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.

Note: Different models support different numbers of trunks (T1, T2, ...). This chapter uses a model that supports six trunks (from T1 to T6).

94.2 Command Summary

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

Table 246 Interface Command Values

COMMAND	DESCRIPTION
port-list	A list of one or more ports, separated by commas with no spaces. The list may also contain ranges of ports signified by a hyphen. For example: 1,3,5–8,10.

The following section lists the commands for this feature.

Table 247 trunk Command Summary

COMMAND	DESCRIPTION	M	P
`show trunk`	Displays link aggregation information.	E	3
`trunk <T1|T2|T3|T4|T5|T6>`	Activates a trunk group.	C	13
`no trunk <T1|T2|T3|T4|T5|T6>`	Disables the specified trunk group.	C	13

Table 247 trunk Command Summary (continued)

COMMAND	DESCRIPTION	M	P
`trunk <T1|T2|T3|T4|T5|T6> criteria <src-mac|dst-mac|src-dst-mac|src-ip|dst-ip|src-dst-ip>`	Sets the outgoing traffic distribution algorithm used in this trunk group for unicast traffic. Unicast traffic means traffic sent from one host to another host. Note: To set more than one criteria, run the command with multiple values separated by a space. **src-mac** means the Switch distributes traffic based on the source MAC address. **dst-mac** means the Switch distributes traffic based on the destination MAC address. **src-dst-mac** means the Switch distributes traffic based on a combination of the source and destination MAC addresses. **src-ip** means the Switch distributes traffic based on the source IP address. **dst-ip** means the Switch distributes traffic based on the destination IP address. **src-dst-ip** means the Switch distributes traffic based on a combination of the source and destination IP addresses.	C	13
`trunk non-unicast criteria <src|dst|port|src-mac|dst-mac|src-ip|dst-ip>`	Sets the outgoing traffic distribution algorithm used in all trunk groups for non-unicast traffic. Non-unicast traffic means Multicast traffic (one sender, multiple receivers) and broadcast traffic (packets send to all hosts on a network). Note: To set more than one criteria, run the command with multiple values separated by a space. Note: At the time of writing, this command only works on some models. Supported algorithms vary depending on the switch model. The non-unicast criteria follow the unicast criteria (GS1350). **src** means the Switch distributes traffic based on the source MAC address or source IP address. **dst** means the Switch distributes traffic based on the destination MAC address or destination IP address. **port** means the Switch distributes traffic based on the source or destination port. **src-mac** means the Switch distributes traffic based on the source MAC address. **dst-mac** means the Switch distributes traffic based on the destination MAC address. **src-ip** means the Switch distributes traffic based on the source IP address. **dst-ip** means the Switch distributes traffic based on the destination IP address.	C	13
`no trunk <T1|T2|T3|T4|T5|T6> criteria`	Returns the traffic distribution type used for the specified trunk group to the default (`src-dst-mac`).	C	13

Table 247 trunk Command Summary (continued)

COMMAND	DESCRIPTION	M	P
trunk <T1|T2|T3|T4|T5|T6> interface *<port-list>*	Adds a ports to the specified trunk group.	C	13
no trunk <T1|T2|T3|T4|T5|T6> interface *<port-list>*	Removes ports from the specified trunk group.	C	13
trunk <T1|T2|T3|T4|T5|T6> lacp	Enables LACP for a trunk group.	C	13
no trunk <T1|T2|T3|T4|T5|T6> 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 ports. *lacp-timeout*: 1 or 30	C	13

Table 248 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

94.3 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 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 249 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 through 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 ports 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 250 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	In some switches this displays the ports whose link state are up. In other switches this displays the ports which belong to this trunk group.
SYNCS	These are the ports that are currently transmitting data as one logical link in this trunk group.

This example configures the Switch for non-unicast trunking.

```
sysname# configure
sysname(config)# trunk T1
sysname(config)# trunk T1 interface 1
sysname(config)# trunk T1 interface 2
sysname(config)# trunk T1 interface 3
sysname(config)# trunk T1 interface 4
sysname(config)# trunk non-unicast criteria src dst port
```

CHAPTER 95
Vendor ID-based VLAN

95.1 Vendor ID-based VLAN Overview

The Vendor ID based VLAN feature assigns incoming untagged packets to a VLAN and classifies the traffic based on the source MAC address of the packet. When untagged packets arrive at the switch, the source MAC address of the packet is looked up in a Vendor ID to VLAN mapping table. If an entry is found, the corresponding VLAN ID is assigned to the packet. The assigned VLAN ID is verified against the VLAN table. If the VLAN is valid, ingress processing on the packet continues; otherwise, the packet is dropped.

This feature allows users to change ports without having to reconfigure the VLAN. You can assign a 802.1p priority to the vendor ID-based VLAN and define a vendor ID to VLAN mapping table by entering a specified source MAC address and mask.

For every vendor ID-based VLAN rule you set, you can specify a weight number to define the rule's priority level. As rules are processed one after the other, stating a priority order will let you choose which rule has to be applied first and which second.

Use these commands to bind a bunch of client source MAC addresses to a VLAN on the Switch.

95.2 Command Summary

The following section lists the commands for this feature.

Table 251 Vendor ID-based VLAN Command Summary

COMMAND	DESCRIPTION	M	P
vendor-id-based-vlan name <*name*> source-mac <*mac-addr*> mask <*mask*> <*vlan-id*> priority <*0-7*> [weight <0-255>]	Adds a new vendor ID-based VLAN entry. *name*: 1 – 32 alphanumeric characters *mask*: type the mask (from ff:ff:ff:00:00:00 to ff:ff:ff:ff:ff:ff) for the specified MAC address to determine which bits a packet's MAC address should match. Enter "f" for each bit of the specified MAC address that the traffic's MAC address should match. Enter "0" for the bits of the matched traffic's MAC address, which can be of any hexadecimal characters. For example, if you set the MAC address to 00:13:49:00:00:00 and the mask to ff:ff:ff:00:00:00, a packet with a MAC address of 00:13:49:12:34:56 matches this criteria. weight: Enter a number between 0 and 255 to specify the rule's weight. This is to decide the priority in which the rule is applied. The higher the number, the higher the rule's priority.	C	13
no vendor-id-based-vlan name <*name*> source-mac <*mac-addr*> mask <*mask*>	Removes an existing vendor ID-based VLAN entry.	C	13
show vendor-id-based-vlan	Show status of the vendor ID-based VLAN.	E	13

95.3 Command Example: add source MAC address

This example adds a binding source MAC address to a vendor ID-based VLAN with MAC address 00:a0:c5:01:23:45, mask ff:ff:ff:00:00:00, VLAN ID number 222, priority level 3 and weight 200.

```
sysname(config)# vendor-id-based-vlan name ex1 source-mac 00:a0:C5:01:23:45
mask ff:ff:ff:00:00:00 vlan 222 priority 3 weight 200
sysname(config)# exit
sysname# show vendor-id-based-vlan
  Index  Name         Source MAC               Mask  VLAN  Priority  Weight
  -----  ----  -----------------  -----------------  ----  --------  ------
      1   ex1  00:a0:c5:01:23:45  ff:ff:ff:00:00:00   222         3     200
sysname#
```

95.4 Command Example: remove source MAC address

This example deletes a binding source MAC address to a vendor ID-based VLAN with MAC address 00:a0:c5:01:23:45 and mask ff:ff:ff:00:00:00.

```
sysname(config)# no vendor-id-based-vlan source-mac 00:a0:c5:01:23:45 mask
ff:ff:ff:00:00:00
sysname(config)# exit
```

CHAPTER 96
VLAN Commands

96.1 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 groups; the traffic must first go through a router.

Use these commands to configure IEEE 802.1Q VLAN.

Note: See Chapter 97 on page 377 for VLAN IP commands.

Note: VLAN is unidirectional; it only governs outgoing traffic.

96.2 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
```

Note: See Chapter 36 on page 132 for `interface port-channel` commands.

96.3 Command Summary

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

Table 252 Interface Command Values

COMMAND	DESCRIPTION
port-list	A list of one or more ports, separated by commas with no spaces. The list may also contain ranges of ports signified by a hyphen. For example: 1,3,5–8,10.

The following section lists the commands for this feature.

Table 253 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
show vlan <*vlan-id*> counters	Displays concurrent incoming packet statistics of the specified VLAN and refreshes every 10 seconds until you press the [ESC] button.	E	3
show vlan <*vlan-id*> interface port-channel <*port-num*> counters	Displays concurrent incoming packet statistics of the specified port in the specified VLAN and refreshes every 10 seconds until you press the [ESC] button.	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 ports to be a permanent member of this VLAN group.	C	13
no fixed <*port-list*>	Sets fixed ports to normal ports.	C	13
forbidden <*port-list*>	Specifies the ports you want to prohibit from joining this VLAN group.	C	13
no forbidden <*port-list*>	Sets forbidden ports to normal ports.	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 ports to dynamically join this VLAN group using GVRP.	C	13
untagged <*port-list*>	Specifies the ports you do not want to tag all outgoing frames transmitted with this VLAN Group ID.	C	13
no untagged <*port-list*>	Specifies the ports you want to tag all outgoing frames transmitted with this VLAN Group ID.	C	13
exit	Leaves the VLAN configuration mode.	C	13
no vlan <*vlan-id*>	Deletes a VLAN.	C	13

The following section lists the commands for the ingress checking feature.

Note: 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 through the `ingress-check` command in the config-interface mode.

Table 254 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 255 ingress-check Command Summary

COMMAND	DESCRIPTION	M	P
`interface port-channel <port-list>`	Enters config-interface mode for the specified ports.	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

96.4 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 256 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 through 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
```

This example displays concurrent incoming packet statistics for VLAN 1.

```
MGS-3712# show vlan 1 counters
-------- Press ESC to finish -------
System up time:     0:59:02
  Vlan Info     Vlan Id.                :1
  Packet        KBs/s                   :0.0
                Packets                 :2
                Multicast               :0
                Broadcast               :2
                Tagged                  :0
  Distribution  64                      :2
                65 to 127               :0
                128 to 255              :0
                256 to 511              :0
                512 to 1023             :0
                1024 to 1518            :0
                Giant                   :0

-------- Press ESC to finish -------
System up time:     0:59:12
  Vlan Info     Vlan Id.                :1
  Packet        KBs/s                   :0.384
                Packets                 :10
                Multicast               :0
                Broadcast               :10
                Tagged                  :0
  Distribution  64                      :10
                65 to 127               :0
                128 to 255              :0
                256 to 511              :0
                512 to 1023             :0
                1024 to 1518            :0
                Giant                   :0
```

The following table describes the labels in this screen.

Table 257 show vlan counters

LABEL	DESCRIPTION
System up time	This field shows the total amount of time the connection has been up.
VLAN Info	This field displays the VLAN ID you are viewing.
Packet	
KBs/s	This field shows the number kilobytes per second flowing through this VLAN.
Packets	This field shows the number of good packets (unicast, Multicast and broadcast) flowing through this VLAN.
Multicast	This field shows the number of good Multicast packets flowing through this VLAN.
Broadcast	This field shows the number of good broadcast packets flowing through this VLAN.
Tagged	This field shows the number of VLAN-tagged packets flowing through this VLAN.
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.

Table 257 show vlan counters (continued)

LABEL	DESCRIPTION
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 (including bad packets) received that were between 1519 octets and the maximum frame size. The maximum frame size varies depending on your switch model.

CHAPTER 97
VLAN IP Commands

97.1 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.

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

97.2 Command Summary

The following section lists the commands for this feature.

Table 258 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 dhcp-bootp option-60	Enables DHCP option 60. When you enable DHCP option 60, make sure you set up a Vendor Class Identifier.	C	13
no ip address default-management dhcp-bootp option-60	Disables DHCP option 60.	C	13
ip address default-management dhcp-bootp option-60 class-id <*class-id*>	Defines a Vendor Class Identifier for DHCP option 60.	C	13
no ip address default-management dhcp-bootp option-60 class-id	Reset the Vendor Class Identifier for DHCP option 60 to default settings.	C	13
ip address default-management <*ip-address*> <*mask*>	Sets and enables the in-band management IP address and subnet mask.	C	13

Table 258 vlan ip address Command Summary (continued)

COMMAND	DESCRIPTION	M	P
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 through 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
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

97.3 Command Examples

See Section 4.5 on page 24 for an example of how to configure a VLAN management IP address using IPv4. See Chapter 42 on page 159 for IPv6 VLAN commands.

CHAPTER 98
VLAN Isolation Commands

98.1 VLAN Isolation Overview

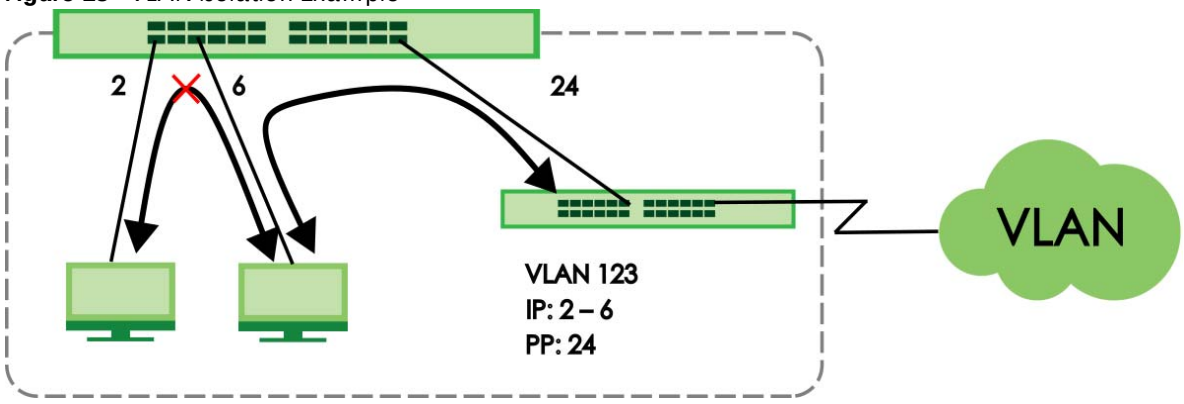
This chapter shows you how to configure the Switch to prevent communications between ports in the same VLAN.

VLAN Isolation allows you to prevent ports in the same VLAN from communicating with each other. Ports in the VLAN are separated into two groups:

- Promiscuous ports: These ports can communicate with any other port in the VLAN.
- Isolated ports: These ports can communicate only with promiscuous ports.

You specify which ports are in the promiscuous port list. The Switch automatically adds all other ports in the VLAN to the isolated port list and blocks traffic between the isolated ports.

Figure 13 VLAN Isolation Example



Note: If you change the VLAN settings, make sure you keep at least one port in the promiscuous port list for a VLAN with VLAN isolation enabled. Otherwise, this VLAN is blocked from the whole network.

Note: You can also prevent ports from communicating using Private VLANs. For details, see Chapter 70 on page 283. If Private VLAN and VLAN Isolation are both enabled, then the VLAN Isolation rules take priority.

98.1.1 VLAN Isolation Command Summary

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

Table 259 VLAN isolation Command Values

COMMAND	DESCRIPTION
port-list	A list of one or more ports, separated by commas with no spaces. The list may also contain ranges of ports signified by a hyphen. For example: 1,3,5–8,10.

The following section lists the commands for this feature.

Table 260 VLAN isolation Command Summary

COMMAND	DESCRIPTION	M	P
no vlan-isolation <*vlan-id*>	Removes the specified VLAN Isolation rule.	C	13
no vlan-isolation <*vlan-id*> inactive	Enables the specified VLAN Isolation rule.	C	13
vlan-isolation name <*name*> vlan <*vlan-id*> promiscuous-port <*port-list*>	Specifies which ports in the VLAN are not isolated by adding them to the promiscuous port list. The Switch automatically adds other ports in this VLAN to the isolated port list and block traffic between the isolated ports. Enter a rule name, VLAN ID and the promiscuous ports.	C	13
vlan-isolation name <*name*> vlan <*vlan-id*> promiscuous-port <*port-list*> inactive	Disables the specified VLAN Isolation rule.	C	13
vlan-isolation name <*name*> vlan <*vlan-id*>	Sets a VLAN Isolation rule for the specified VLAN. The Switch automatically adds all ports except uplink ports in this VLAN to the isolated port list and blocks traffic between the isolated ports. The uplink ports in the VLAN are always in the promiscuous port list.	C	13
vlan-isolation name <*name*> vlan <*vlan-id*> inactive	Disables the specified VLAN Isolation rule.	C	13
show vlan-isolation	Displays the settings and status of all VLAN Isolation rules on the Switch.	E	3
show vlan-isolation <*vlan-id*>	Displays the settings and status of the specified VLAN Isolation rule on the Switch.	E	3

98.1.2 Command Examples

This example sets a VLAN Isolation rule (pvlan-123) that applies to VLAN 123. Ports 7 and 8 are the promiscuous ports in VLAN 123. Other ports in this VLAN are added to the isolated port list automatically and cannot communicate with each other. The isolated ports in VLAN 123 can send and receive traffic from ports 7 and 8. This example also shows all VLAN Isolation rules configured on the Switch.

```
sysname# configure
sysname(config)# vlan-isolation name pvlan-123 vlan 123 promiscuous-port 7-8
sysname(config)# exit
sysname# show vlan-isolation
  VLAN: 123    Active: Yes
  Name    Promiscuous Port
  ------------ --------------------------
  pvlan-123  7-8
sysname#
```

This example sets a VLAN Isolation rule (pvlan-111) that applies to VLAN 111. Ports 1, 2 and 24 belong to VLAN 111. Ports 1 and 2 are added to the isolated port list automatically and cannot communicate with each other. Port 24 is the uplink port and also the promiscuous port in this VLAN. The isolated ports in VLAN 111 can send and receive traffic from the uplink port 24. This example also shows all VLAN Isolation rules configured on the Switch.

```
sysname# configure
sysname(config)# vlan-isolation name pvlan-111 vlan 111
sysname(config)# exit
sysname# show vlan-isolation
  VLAN: 111    Active: Yes
  Name    Promiscuous Port
  ----------- -------------------------
  pvlan-111  24
sysname#
```

CHAPTER 99
VLAN Mapping Commands

99.1 VLAN Mapping Overview

Use these commands to configure VLAN mapping on the Switch. With VLAN mapping enabled, the Switch can map the VLAN ID and priority level of packets received from a private network to those used in the service provider's network. The Switch discards the tagged packets that do not match an entry in the VLAN mapping table.

Note: You can not enable VLAN mapping and VLAN stacking at the same time.

99.2 Command Summary

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

Table 261 Interface Command Values

COMMAND	DESCRIPTION
port-list	A list of one or more ports, separated by commas with no spaces. The list may also contain ranges of ports signified by a hyphen. For example: 1,3,5–8,10.

The following section lists the commands for this feature.

Table 262 vlan mapping Command Summary

COMMAND	DESCRIPTION	M	P
`no vlan-mapping`	Disables VLAN mapping on the Switch.	C	13
`no vlan-mapping interface port-channel <port> vlan <1-4094>`	Removes the specified VLAN mapping rule.	C	13
`no vlan-mapping interface port-channel <port> vlan <1-4094> inactive`	Enables the specified VLAN mapping rule.	C	13
`vlan-mapping`	Enables VLAN mapping on the Switch.	C	13
`vlan-mapping name <name> interface port-channel <port> vlan <1-4094> translated-vlan <1-4094> priority <0-7>`	Creates a VLAN mapping rule.	C	13
`vlan-mapping name <name> interface port-channel <port> vlan <1-4094> translated-vlan <1-4094> priority <0-7> inactive`	Disables the specified VLAN mapping rule.	C	13

Table 262 vlan mapping Command Summary (continued)

COMMAND	DESCRIPTION	M	P
interface port-channel <*port-list*>	Enters config-interface mode for the specified ports.	C	13
vlan-mapping	Enables VLAN mapping on the ports.	C	13
no vlan-mapping	Disables VLAN mapping on the ports.	C	13

99.3 Command Examples

This example enables VLAN mapping on the Switch and creates a VLAN mapping rule to translate the VLAN ID from 123 to 234 in the packets received on port 4.

```
sysname# configure
sysname(config)# vlan-mapping
sysname(config)# vlan-mapping name test interface port-channel 4 vlan 123
translated-vlan 234 priority 3
sysname(config)#
```

This example enables VLAN mapping on port 4.

```
sysname# configure
sysname(config)# interface port-channel 4
sysname(config-interface)# vlan-mapping
sysname(config-interface)# exit
sysname(config)#
```

CHAPTER 100
VLAN Port Isolation Commands

100.1 Port Isolation Overview

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.

100.2 Command Summary

The following section lists the commands for this feature.

Table 263 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
`interface port-channel <port-list>`	Enters config-interface mode for the specified ports. The port list must consist of one or more ports, separated by commas with no spaces. The list may also contain ranges of ports signified by a hyphen. For example: 1,3,5–8,10.	C	13
`no vlan1q port-isolation`	Enables VLAN port isolation on the ports.	C	13
`vlan1q port-isolation`	Disables VLAN port isolation on the ports.	C	13

CHAPTER 101
VLAN Stacking Commands

101.1 VLAN Stacking Overview

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

101.2 Command Summary

The following section lists the commands for this feature.

Table 264 vlan-stacking Command Summary

COMMAND	DESCRIPTION	M	P
`interface port-channel <port-list>`	Enters config-interface mode for the specified ports. The port list must consist of one or more ports, separated by commas with no spaces. The list may also contain ranges of ports signified by a hyphen. For example: 1,3,5–8,10.	C	13
`vlan-stacking priority <0-7>`	Sets the priority of the specified ports in port-based VLAN stacking.	C	13
`vlan-stacking role <normal|access|tunnel>`	Sets the VLAN stacking port roles of the specified ports. `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 ports.	C	13
`vlan-stacking tunnel-tpid <tpid>`	Sets a four-digit hexadecimal number from 0000 to FFFF that the Switch adds in the outer VLAN tag of the outgoing frames sent on the tunnel ports.	C	13
`no vlan-stacking`	Disables VLAN stacking on the Switch.	C	13
`no vlan-stacking selective-qinq interface port-channel <port> cvid <vlan-id>`	Removes the specified selective VLAN stacking rule.	C	13

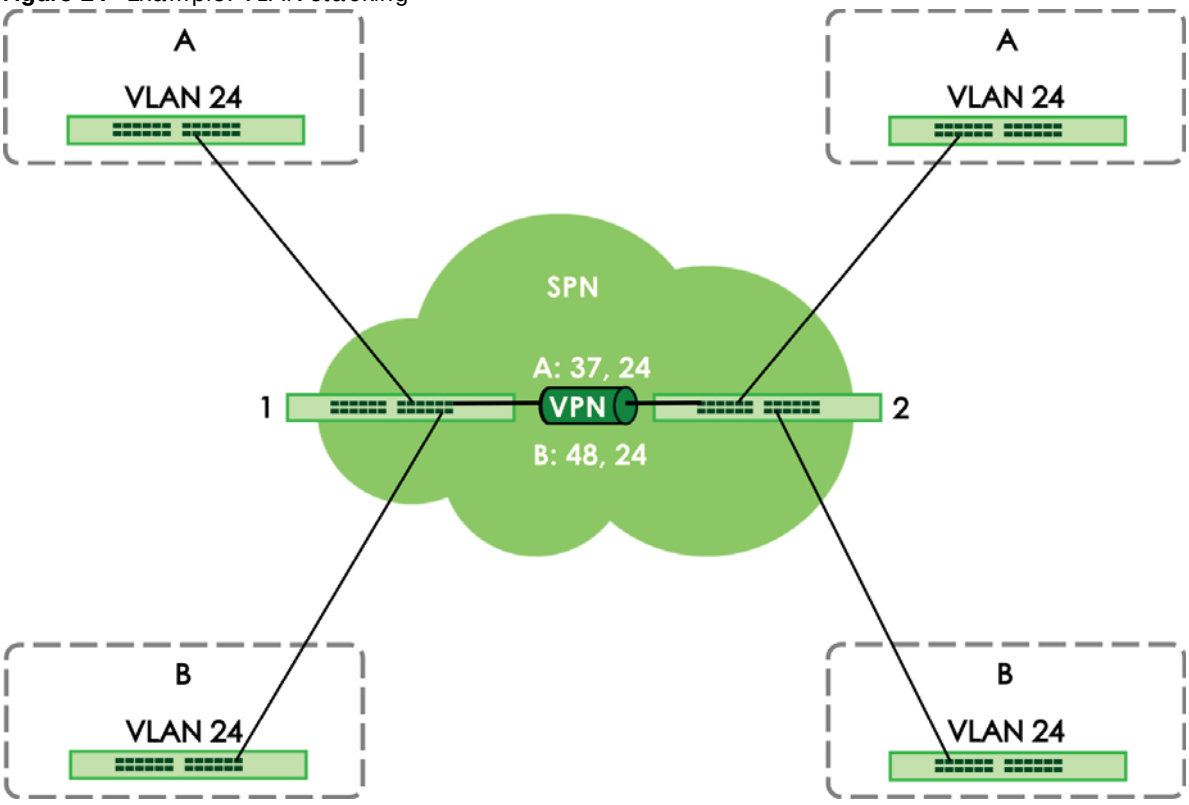
Table 264 vlan-stacking Command Summary (continued)

COMMAND	DESCRIPTION	M	P
`no vlan-stacking selective-qinq interface port-channel <port> cvid <vlan-id> inactive`	Enables the specified selective VLAN stacking rule.	C	13
`show vlan-stacking`	Displays VLAN stacking settings.	E	3
`vlan-stacking`	Enables 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
`vlan-stacking selective-qinq name <name> interface port-channel <port> cvid <cvid> spvid <spvid> priority <0-7>`	Creates a selective VLAN stacking rule. *cvid*: 1 – 4094. This is the VLAN tag carried in the packets from the subscribers. *spvid*: 1 – 4094: This is the service provider's VLAN ID (the outer VLAN tag).	C	13
`vlan-stacking selective-qinq name <name> interface port-channel <port> cvid <cvid> spvid <spvid> priority <0-7> inactive`	Disables the specified selective VLAN stacking rule.	C	13

101.3 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 **x** and then stripping those tags at edge device **y** as the data frames leave the network.

Figure 14 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)# 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
06              access          1               0
07              access          1               0
08              access          1               0
....
```

CHAPTER 102
VLAN Trunking Commands

102.1 Command Summary

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

The following section lists the commands for this feature.

Table 265 vlan-trunking Command Summary

COMMAND	DESCRIPTION	M	P
`interface port-channel <port-list>`	Enters config-interface mode for the specified ports. The port list may consist of one or more ports, separated by commas with no spaces. The list may also contain ranges of ports signified by a hyphen. For example: 1,3,5–8,10.	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 through the VLAN-trunking port.	C	13
`no vlan-trunking`	Disables VLAN trunking on the ports.	C	13

CHAPTER 103
Voice VLAN Commands

103.1 Voice VLAN Overview

Voice VLAN ensures that the sound quality of an IP phone is preserved from deteriorating when the data traffic on the Switch ports is high. It groups the voice traffic with defined priority into an assigned VLAN which enables the separation of voice and data traffic coming onto the Switch port.

You can set priority level to the Voice VLAN and add MAC address of IP phones from specific manufacturers by using its ID from the Organizationally Unique Identifiers (OUI).

See below commands and examples to set up the Voice VLAN.

103.2 Command Summary

The following section lists the commands for this feature.

Table 266 Voice VLAN Command Summary

COMMAND	DESCRIPTION	M	P
voice-vlan <*vlan-id*>	Sets the Voice VLAN ID.	C	13
voice-vlan priority <*0-7*>	Sets the Voice VLAN priority level.	C	13
voice-vlan oui <*mac-addr*> mask <*mask-addr*> description <*description*>	Sets the Voice VLAN device's OUI address, mask address and device manufacturer description.	C	13
no voice-vlan	Disables Voice VLAN configuration.	C	13
no voice-vlan oui <mac-addr> mask <mask-addr>	Removes the OUI from the Voice VLAN.	C	13
show voice-vlan	Show Voice VLAN status.	E	3

103.3 Command Example

This example configures Voice VLAN to port number 5, priority level number 6 and displays Voice VLAN session.

```
sysname# configure
sysname(config)# voice-vlan 5
sysname(config)# voice-vlan priority 6
sysname(config)# exit
sysname# show voice-vlan
  Voice VLAN    : enable
  VLAN ID       : 5
  Priority      : 6
  Port      Mode      Tagging      VLAN Membership
    1    normal      tagged           no
    2    normal      tagged           no
    3    normal      tagged           no
    4    normal      tagged           no
    5    normal      tagged           no
    6    normal      tagged           no
    7    normal      tagged           no
    8    normal      tagged           no
    9    normal      tagged           no
   10    normal      tagged           no
   11     fixed      tagged          yes
   12     fixed      tagged          yes
   13     fixed      tagged          yes
   14     fixed      tagged          yes
   15     fixed      tagged          yes
   16     fixed      tagged          yes
   17     fixed      tagged          yes
   18     fixed      tagged          yes
   19     fixed      tagged          yes
   20     fixed      tagged          yes
   21 forbidden      tagged           no
   22 forbidden      tagged           no
   23 forbidden      tagged           no
   24 forbidden      tagged           no
   25 forbidden      tagged           no
   26 forbidden      tagged           no
   27 forbidden      tagged           no
   28 forbidden      tagged           no
```

This example sets the VLAN ports for Voice VLAN as seen in the above example. Normal port is 5 to 10, Fixed port is 11 to 20 and forbidden port is 21 to 28. Port numbers can be higher if the Switch model has 48 ports.

```
sysname# configure
sysname(config)# vlan 5
sysname(config-vlan)# normal 5-10
sysname(config-vlan)# fixed 11-20
sysname(config-vlan)# forbidden 21-28
sysname(config-vlan)# exit
sysname# show voice-vlan
  Voice VLAN    : enable
  VLAN ID       : 5
  Priority      : 6
  Port      Mode      Tagging      VLAN Membership
    1    normal      tagged           no
    2    normal      tagged           no
    3    normal      tagged           no
    4    normal      tagged           no
    5    normal      tagged           no
    6    normal      tagged           no
    7    normal      tagged           no
    8    normal      tagged           no
    9    normal      tagged           no
   10    normal      tagged           no
   11     fixed      tagged          yes
   12     fixed      tagged          yes
   13     fixed      tagged          yes
   14     fixed      tagged          yes
   15     fixed      tagged          yes
   16     fixed      tagged          yes
   17     fixed      tagged          yes
   18     fixed      tagged          yes
   19     fixed      tagged          yes
   20     fixed      tagged          yes
   21 forbidden      tagged           no
   22 forbidden      tagged           no
   23 forbidden      tagged           no
   24 forbidden      tagged           no
   25 forbidden      tagged           no
   26 forbidden      tagged           no
   27 forbidden      tagged           no
   28 forbidden      tagged           no
```

CHAPTER 104
VRRP Commands

104.1 VRRP Overview

Virtual Router Redundancy Protocol (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.

104.2 Command Summary

The following section lists the commands for this feature.

Table 267 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
no preempt	Disables VRRP preemption mode.	C	13
preempt	Enables preemption mode.	C	13
exit	Exits from the VRRP command mode.	C	13

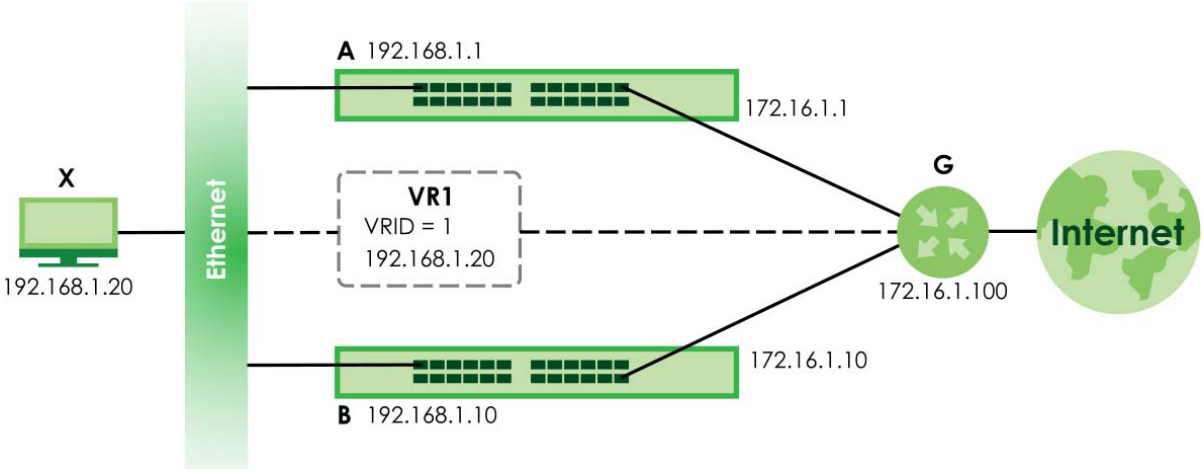
Table 267 VRRP Command Summary (continued)

COMMAND	DESCRIPTION	M	P
`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

104.3 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 15 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 15 on page 393.

```
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 15 on page 393.

```
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)#
```

CHAPTER 105
WoL Relay Commands

105.1 WoL Relay Overview

Wake On LAN (WoL) is a feature to remotely turn on a device on the LAN network. A device is turned on by receiving a magic packet. To use this feature the remote hardware (for example the network adapter on a computer) must support Wake On LAN using the "Magic Packet" method.

A magic packet is a UDP broadcast packet. The device that you want to turn on is off, so it cannot respond to a TCP packet. Therefore, It has to be a UDP broadcast packet to turn on a device.

Broadcast packets are generally not routed. A magic packet cannot be routed. This prevents DDoS attacks, but also prohibits you from sending magic packets to other devices in different subnets. The Switch's Wake On LAN relay feature allows you to send magic packets to devices across different subnets.

105.2 Command Summary

The following section lists the commands for this feature.

Table 268 Wol Relay Command Summary

COMMAND	DESCRIPTION	M	P
`wol relay udp <destination-socket> source-vlan <vlan-list> destination-vlan <vlan-list>`	Configure settings on Wake On LAN relay. <destination-socket>: Enters a UDP port number that magic packets are sent through. The most common port for transmission is UDP port 9. <vlan-list>: Enter the source VLAN ID where the magic packet originates from. Enter the destination VLAN ID where the magic packet will be sent to.	C	13
`no wol relay udp <destination-socket>`	Removes the specified Wake on LAN relay rule. <destination-socket>: Enters a UDP port number that magic packets are sent through.	C	13

CHAPTER 106
ZULD Commands

106.1 ZULD Overview

A unidirectional link is a connection where the link is up on both ends, but only one end can receive packets. This may happen if OAM was initially enabled but then disabled, there are mis-configured transmitting or receiving lines or the hardware is malfunctioning. Zyxel Unidirectional Link Detection (ZULD) is a layer-2 protocol that can detect and disable these physical one-way links before they cause loops or communication malfunction.

ZULD must be enabled on the Switch and the ports in order to detect unidirectional links by monitoring OAMPDUs.

Note: Ports advertise their unidirectional link detection capability using OAMPDUs, so all connected devices must support OAM as well as ZULD.

Note: OAM must be enabled on other connected devices too. If OAM is not enabled initially, ZULD will not work.

106.2 Command Summary

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

Table 269 Interface Command Values

COMMAND	DESCRIPTION
port-list	A list of one or more ports, separated by commas with no spaces. The list may also contain ranges of ports signified by a hyphen. For example: 1,3,5–8,10.

The following section lists the commands for this feature.

Table 270 zuld Command Summary

COMMAND	DESCRIPTION	M	P
zuld	Enables ZULD on the Switch.	C	13
no zuld	Disables ZULD on the Switch.	C	13
interface port-channel <*port-list*>	Enters config-interface mode for the specified ports.	C	13
zuld	Enables ZULD on the specified ports.	C	13
no zuld	Disables ZULD on the specified ports.	C	13

Table 270 zuld Command Summary (continued)

COMMAND	DESCRIPTION	M	P
zuld mode <normal|aggressive>	Configures the ZULD mode. normal: ZULD only sends a syslog and trap when it detects a unidirectional link. aggressive: ZULD shuts down the port (puts it into an ErrDisable state) as well as sends a syslog and trap when it detects a unidirectional link.	C	13
zuld probe-time <5-65535>	Sets the length of time that ZULD waits before declaring that a link is unidirectional. When the probe time expires, and one port (either on the Switch or the connected device) still has not received an OAMPDU, then ZULD declares that the link is unidirectional.	C	13
show zuld [*<port-list>*]	Displays ZULD details and link state for all ports or the specified ports.	E	3
show zuld summary	Displays ZULD details of each port in a summary table.	E	3

106.3 Command Example

This example enables Ethernet OAM on the Switch and ports 1 – 3 first, then enables ZULD on the Switch and ports 1 – 3. It also sets a ZULD mode and displays the configuration details.

```
sysname# configure
sysname(config)# ethernet oam
sysname(config)# interface port-channel 1-3
sysname(config-interface)# ethernet oam
sysname(config-interface)# exit
sysname(config)# zuld
sysname(config)# interface port-channel 1-3
sysname(config-interface)# zuld
sysname(config-interface)# zuld mode aggressive
sysname(config-interface)# exit
sysname(config)# exit
sysname# show zuld 1-3
  Port 1
    Active            : Yes
    Mode              : Aggressive
    Probe Time        : -
    Link State        : Linkdown
  Port 2
    Active            : Yes
    Mode              : Aggressive
    Probe Time        : -
    Link State        : Linkdown
  Port 3
    Active            : Yes
    Mode              : Aggressive
    Probe Time        : -
    Link State        : Linkdown
sysname#
```

CHAPTER 107 Miscellaneous Commands

107.1 Command Summary

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

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

Table 271 Interface Command Values

COMMAND	DESCRIPTION
port-list	A list of one or more ports, separated by commas with no spaces. The list may also contain ranges of ports signified by a hyphen. For example: 1,3,5–8,10.

The following section lists the commands for this feature.

Table 272 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 3.2.3.1 on page 19.	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 3.2.3.2 on page 20.	E	0
`disable`	Changes the session's priority level to 0 and changes the mode to user mode. See Section 3.2.3.3 on page 20.	E	13
`configure`	Changes the mode to config mode.	E	13
`exit`	Returns to the previous mode.	C	13
`logout`	Logs out of the CLI.	E	0

Table 273 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 <index>`	Restarts the Switch (cold reboot) with the specified configuration file.	E	13

Table 273 Command Summary: Additional Enable Mode (continued)

COMMAND	DESCRIPTION	M	P
boot image <1|2>	The Switch supports dual firmware images, ras-0 and ras-1. Run this command, where <index> is 1 (ras-0) or 2 (ras-1) to specify which image is updated when firmware is loaded using the Web Configurator and to specify which image is loaded when the Switch starts up.	E	13
cable-diagnostics <*port-list*>	Performs a physical wire-pair test of the Ethernet connections on the specified ports.	E	13
ping <*ip*|*host-name*> [vlan <*vlan-id*>] [size <0-1472>] [-t]	Sends Ping packets to the specified Ethernet device. *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 [1|2]	Restarts the system (warm reboot) with the specified configuration file. 1: config-1 2: config-2	E	13
reset slot <*slot-list*>	Restarts the card in the selected slot. The card restarts using the last-saved configuration. Any unsaved changes are lost.	E	13
show alarm-status	Displays alarm status.	E	0
show cpu-utilization	Displays the CPU utilization statistics on the Switch.	E	0
show cpu-utilization process	Displays the CPU and memory usage of each process.	E	0
show except-smac	Displays whether the Switch is to drop the packets with an all-zero source MAC address (00:00:00:00:00:00).	E	13
show interfaces status	Displays the summary status of interfaces for all ports on the Switch.	E	3
show interfaces transceiver <*port-list*>	Displays real-time SFP (Small Form Factor Pluggable) transceiver information and operating parameters on specified SFP ports. The parameters include, for example, module temperature, module voltage, transmitting and receiving power.	E	3
show memory	Displays the memory utilization statistics on the Switch.	E	3
show power-source-status	Displays the status of each power module in the system.	E	0
show rootguard	Displays STP mode and root guard information.	E	3
show stacking slot <*slot number*>	Displays general status information for each slot in the stack.	E	13
show stacking slot status	Displays what type of card is installed for each slot in the stack and its current operational status.	E	13
show slot config <*slot-list*>	Displays detailed information about the specified slots in the stack.	E	13
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 versions of the currently installed firmware images on the flash memory.	E	0

Table 273 Command Summary: Additional Enable Mode (continued)

COMMAND	DESCRIPTION	M	P
`test interface port-channel <port-list>`	Performs an internal loopback test on the specified ports. The test returns `Passed!` or `Failed!`.	E	13
`write memory [<index>]`	Saves current configuration in volatile memory to the configuration file the Switch is currently using or the specified configuration file.	E	13

Table 274 Command Summary: Additional Configure Mode

COMMAND	DESCRIPTION	M	P
`admin-username <name>`	Sets the login user name. Up to 32 printable ASCII characters except ? | ' " or , . Note: "admin" is the default administrator login user name. Note: See Table 8 on page 13 for the product that supports this command.	C	14
`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 originating from itself (such as SNMP traps) or packets with unknown source.	C	13
`except-smac zero-smac-drop`	Sets the Switch to filter and drop the packets with an all-zero source MAC address (00:00:00:00:00:00).	C	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
`install help`	Displays command help information.	C	13
`install slot <slot-list> type <card-type>`	Changes what type of card is in the slot without restarting the system.	C	13
`locator-led`	Turns on the **LOCATOR** LED on the Switch. By default, the LED blinks and automatically turns off after 30 minutes. This helps to locate the Switch that you are managing when multiple switches are installed in a rack or placed in the same room.	C	13
`locator-led <1-1440>`	Changes how long (in minutes) the **LOCATOR** LED blinks for.	C	13
`mode zynos`	Changes the CLI mode to the ZyNOS format.	C	13
`no except-smac zero-smac-drop`	Sets the Switch to allow and forward the packets with an all-zero source MAC address (00:00:00:00:00:00).	C	13
`no install slot <slot>`	Uninstalls the card in the slot.	C	13
`no locator-led`	Stops the **LOCATOR** LED from blinking immediately.	C	13
`no shutdown slot <slot-list>`	Turns on the power to the slot.	C	13
`shutdown slot <slot-list>`	Turns off the power to the slot.	C	13

Table 274 Command Summary: Additional Configure Mode (continued)

COMMAND	DESCRIPTION	M	P
`transceiver-ddm timer <1 - 4294967>`	Sets the duration of the digital diagnostic monitoring (DDM) timer. This defines how often (in milliseconds) the Switch sends the digital diagnostic monitoring (DDM) information through the installed transceivers.	C	13
`reset sfp <port-list>`	Restarts the specified SFP ports. This Fiber Module Rescue function allows you to restart a fiber SFP transceiver that is in error state without having to remove and reinsert the transceiver. The Switch stops then re-supplies power on the specified SFP ports to restart it. Use the command when your SFP port encounters connection errors. After restarting an SFP port, use the show `interface <port-list>` command to check the port status. You can also check the port LED on the Switch panel or port status on the Web Configurator to see if the connection has recovered. Note: Make sure the transceiver is correctly inserted into the SFP port. Note: See Table 8 on page 13 for the products that support this command.	E	13

107.2 Command Examples

This example checks the cable pairs on ports 1 and 4.

```
sysname# cable-diagnostics 1
Port   Channel   Pair status   Cable length (m)   Distance to fault (m)
----   -------   -----------   ----------------   ---------------------
   1     pairA          Open                N/A                   0.00
         pairB          Open                N/A                   0.00
         pairC          Open                N/A                   0.00
         pairD          Open                N/A                   0.00
sysname# cable-diagnostics 4
Port   Channel   Pair status   Cable length (m)   Distance to fault (m)
----   -------   -----------   ----------------   ---------------------
  4      pairA            Ok               5.55                   N/A
         pairB            Ok               5.55                   N/A
         pairC            Ok               5.55                   N/A
         pairD            Ok               5.55                   N/A
```

The following table describes the labels in this screen.

Table 275 Cable-diagnostics

LABEL	DESCRIPTION
Port	This is the number of the physical Ethernet port on the Switch.
Channel	An Ethernet cable usually has four pairs of wires. A 10BASE-T or 100BASE-TX port only use and test two pairs, while a 1000BASE-T port requires all four pairs. This displays the descriptive name of the wire-pair in the cable.
Pair status	**Ok**: The physical connection between the wire-pair is okay. **Open**: There is no physical connection (an open circuit detected) between the wire-pair. **Short**: There is an short circuit detected between the wire-pair. **Unknown**: The Switch failed to run cable diagnostics on the cable connected this port. **Unsupported**: The port is a fiber port or it is not active.
Cable length	This displays the total length of the Ethernet cable that is connected to the port when the **Pair status** is **Ok** and the Switch chipset supports this feature. This shows **N/A** if the **Pair status** is **Open** or **Short**. Check the **Distance to fault**. This shows **Unsupported** if the Switch chipset does not support to show the cable length.
Distance to fault	This displays the distance between the port and the location where the cable is open or shorted. This shows **N/A** if the **Pair status** is **Ok**. This shows **Unsupported** if the Switch chipset does not support to show the distance.

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 276 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 277 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 278 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 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 279 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 through IGMP snooping VLAN in fixed mode. **Dynamic**: This VLAN is learned dynamically in auto mode. See Chapter 35 on page 124 for more information about IGMP snooping VLAN and IGMP modes.

This example shows general system information of the Switch.

```
sysname# show system-information

Product Model           : XGS2220-54FP
System Name             : XGS2220
System Mode             : Standalone
System Contact          :
System Location         :
System up Time          :  1011:30:18 (d90bb588 ticks)
Ethernet Address        : b8:ec:a3:ff:f2:a2
Bootbase Version        : V1.00 | 06/13/2022
ZyNOS F/W Version       : V4.80(ACCE.0) | 08/03/2022
Hardware Version        : V1.0
Config Boot Image       : 1
Current Boot Image      : 1
Current Configuration   : 1
RomRasSize              : 6440206
Serial Number           : S222L18090003
Register MAC Address    : b8:ec:a3:ff:f2:a2
XGS2220# show system-information

Product Model           : XGS2220-54FP
System Name             : XGS2220
System Mode             : Standalone
System Contact          :
System Location         :
System up Time          :  1011:33:19 (d90e7bb6 ticks)
Ethernet Address        : b8:ec:a3:ff:f2:a2
Bootbase Version        : V1.00 | 06/13/2022
ZyNOS F/W Version       : V4.80(ACCE.0) | 08/03/2022
Hardware Version        : V1.0
Config Boot Image       : 1
Current Boot Image      : 1
Current Configuration   : 1
RomRasSize              : 6440206
Serial Number           : S222L18090003
Register MAC Address    : b8:ec:a3:ff:f2:a2
sysname#
```

The following table describes the labels in this screen.

Table 280 show system-information

LABEL	DESCRIPTION
Product Model	This field displays the model name.
System Name	This field displays the system name (or hostname) of the Switch.
System Mode	This field displays standalone or stacking mode
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 81 on page 321.
System Location	This field displays the geographic location of this Switch. Use the snmp-server command to configure this. See Chapter 81 on page 321.
System up Time	This field displays how long the Switch has been running since it last started up.
Ethernet Address	This field displays the MAC address of the Switch.
Bootbase Version	This field displays the bootbase version the Switch is running.

Table 280 show system-information (continued)

LABEL	DESCRIPTION
ZyNOS F/W Version	This field displays the firmware version the Switch is running.
Hardware Version	This field displays the hardware version number of the Switch. The integer is the generation number of the Switch series, and the decimal is the version of the hardware change. For example, V1.0 is a hardware version for the Switch where 1 identifies the first generation of the Switch series, and .0 is the first hardware change.
Config Boot Image	This field displays whether the Switch is configured to run firmware 1 or 2 when it next starts.
Current Boot Image	This field displays whether the Switch is running firmware 1 or 2.
Config Boot Image	This field displays which firmware image (1 or 2) is loaded when the Switch starts up.
Current Boot Image	This field displays the firmware image (1 or 2) the Switch is currently using.
RomRasSize	This field displays how much ROM is used.
Service Status	This field displays the service name (**Advance Routing** for example) if a service license is enabled at myZyxel or **Not Licensed** if the service license is not enabled. It also shows the amount of time that remains if you enabled a trial license (**Advance Routing | Trial 30 day(s) 0 hour(s)** for example). This field is available when you can enable service licenses and manage subscription services for your Switch.
Serial Number	This field displays the serial number of this Switch. The serial number is used for device tracking and control.
Register MAC address	This field displays the MAC address of the Switch that you must use to register at myZyxel.com or the NCC (Nebula Control Center).

This example displays run-time SFP (Small Form Factor Pluggable) parameters on ports 9 (the first SFP port 0, with an SFP transceiver installed) and 10 (the second SFP port 1, no SFP transceiver installed) on the Switch. You can also see the alarm and warning thresholds for temperature, voltage, transmission bias, transmission and receiving power as shown.

```
sysname# show sfp 9-10

SFP                     : 0
Part Number             : SFP-SX-DDM
Series Number           : S081113001132
Revision                : V1.0
Transceiver             : 1000BASE-SX
Temperature(C) Alarm(80.00 ~ 0.00), Warning(75.00 ~ 5.00), Current(38.00)
Voltage(V) Alarm(3.50 ~ 3.10), Warning(3.45 ~ 3.15), Current(3.37)
Tx Bias(mA) Alarm(100.05 ~ 1.00), Warning(90.04 ~ 2.00), Current(5.25)
Tx Power(dBm) Alarm(-2.99 ~ -8.98), Warning(-3.49 ~ -8.48), Current(-6.05)
Rx Power(dBm) Alarm(-2.99 ~ -18.01), Warning(-3.49 ~ -17.39), Current(-4.24)

SFP                     : 1
Not Available
```

This example displays run-time SFP (Small Form Factor Pluggable) parameters on port 21 on the Switch. You can also see the alarm and warning thresholds for temperature, voltage, transmission bias, transmission and receiving power as shown.

```
sysname# show interface transceiver 21
  Transceiver Information

Port                    : 21 (SFP)
Vendor                  : Zyxel
Part Number             : SFP-LX-10-D
Series Number           : S081133000074
Revision                : V1.0
Date Code               : 2008-08-11
Transceiver             : 1000BASE-LX

++ : high alarm, + : high warn, - : low warn, -- : low alarm.

                   Current   High Alarm   High Warn    Low Warn   Low Alarm
                             Threshold   Threshold   Threshold   Threshold
-------------- ----------- ------------ ----------- ----------- -----------
Temperature(C) ++    38.00        -1.00       75.00        5.00        0.00
Voltage(V)            3.36         3.50        3.45        3.15        3.10
Tx Bias(mA)          14.53       100.05       90.04        7.00        6.00
Tx Power(dBm)        -5.80        -2.99       -3.49       -8.96       -9.50
Rx Power(dBm)  +     -3.36        -2.99       -3.49      -20.50      -21.02
sysname#
```

This example displays the firmware version the Switch is currently using.

```
sysname# show version
  Current ZyNOS version : V4.80(ACCE.0) | 08/03/2022
  Image 1 ZyNOS version : V4.80(ACCE.0) | 08/03/2022
  Image 2 ZyNOS version : V4.80(ACCE.0) | 08/03/2022
```

This example displays the firmware versions of the dual firmware images.

```
sysname# show version flash
  Flash 1 ZyNOS version : V4.80(ACCE.0) | 08/03/2022
  Flash 2 ZyNOS version : V4.80(ACCE.0) | 08/03/2022
```

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 VII Appendices and Index of Commands

Index of Commands

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

APPENDIX 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 281 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